kyndryl

Navigating CPS 230: The impact on Australian banks and insurance companies and their compliance strategies

Understanding the likely impact of CPS 230 and preparing for ongoing compliance

Contents

Executive summary

CPS 230 is a new standard from the Australian Prudential Regulation Authority (APRA) that aims to transform how banks and insurance companies manage risks. The regulation emphasises risk management practices, third-party risk, and business continuity to bolster financial institutions' resilience to operational disruptions. Compliance with CPS 230 — in force from July 1st, 2025 — presents both challenges and opportunities for APRA-regulated companies.

This white paper examines the likely impacts of CPS 230 and proposes strategies for organisations to reduce their risks and create robust compliance frameworks. The paper underscores the board-level responsibility for ensuring that any APRA-regulated entity is resilient, ready for business disruptions, and able to manage risks effectively to deliver essential services to customers.

Understanding CPS 230

CPS 230 is part of APRA's broader initiative to strengthen the resilience of the financial system in Australia, focusing on operational risk management. The regulation mandates that financial institutions develop, implement and maintain comprehensive risk management frameworks that address various operational risks, including those posed by third-party service providers. The standard applies to all APRA-regulated entities, including banks, insurers and superannuation funds. It emphasises the importance of:

- Operational and third-party risk management
- Business continuity planning
- Board-level (C-Suite) oversight

Business impacts of CPS 230

An informal survey of tier-one financial organisations in Australia reveals the following top five likely business impacts of the revised standard:

1. Enhanced accountability for operational risk boards.

Senior management will be held more accountable for ensuring robust operational risk management frameworks. This will require improved oversight and reporting structures, driving a stronger focus on risk culture and governance across the organisation.

2. Increased compliance and administrative burden.

Firms need to enhance risk management processes, documentation and reporting, which may increase compliance costs. Firms must maintain comprehensive risk management frameworks, perform regular audits and adhere to stricter operational requirements.

3. Greater focus on outsourcing and third-party risk management.

CPS 230 imposes stricter guidelines on outsourcing, requiring firms to maintain more rigorous oversight of their service providers. This will likely result in restructuring vendor contracts, increasing due diligence and emphasising third-party risk management.

4. Increased operational resilience requirements.

APRA-regulated businesses must now ensure they are more resilient to disruptions; the revised regulation sets out specific requirements on managing operational incidents and recovery. This could necessitate investments in IT infrastructure, business continuity planning and cybersecurity to meet the expectations of the new standard.

5. Financial and reputational implications of non-compliance.

Non-compliance with CPS 230 could result in regulatory action or fines, damaging a company's financial standing and reputation. Increased scrutiny from regulators and stakeholders may also lead to a loss of investor confidence or market position.

Key actions for compliance

CPS 230 raises the bar on risk management practices, requiring stronger operational resilience and governance from APRA-regulated businesses while adding new layers of accountability and scrutiny.

To address the business impacts associated with the revised CPS 230 regulation, organisations can implement several key actions to help achieve compliance, mitigate risks and maintain operational resilience.

1. Strengthen governance and accountability structures.

Organisations should ensure that their board and senior management are fully engaged in operational risk management. They can achieve this by:

- Establishing clear governance frameworks with defined roles and responsibilities for overseeing risk.
- Enhancing board-level reporting to provide insight into operational risks, incident management and risk appetite.
- Conducting regular training and awareness sessions to ensure that leaders understand their obligations under CPS 230.

2. Enhance risk management frameworks.

A robust operational risk management framework is essential. Businesses should:

- Conduct a comprehensive review and refresh of their existing risk management policies and procedures.
- Develop a clear risk appetite statement that aligns with the requirements of CPS 230.
- Implement continuous monitoring and improvement mechanisms for operational risks, including cybersecurity, fraud and business continuity.

3. Improve third-party risk management.

The revised CPS 230 increases the focus on outsourcing and third-party risks. Organisations should:

- Perform a thorough assessment of all third-party providers, especially those involved in critical services.
- Strengthen due diligence processes, renegotiate contracts, and ensure vendors meet higher resilience and compliance standards.
- Develop contingency plans for third-party failures and maintain regular communication with vendors on risk issues.

4. Invest in operational resilience and incident management.

Organisations must bolster their ability to withstand and recover from disruptions. To do this, they should:

- Invest in business continuity and disaster recovery plans. Here, the gamification of testing using war games scenarios has proven invaluable in helping to ensure that all plans are regularly tested and updated.
- Implement a strong incident management process that includes detailed reporting, root cause analysis and timely remediation.
- Focus on improving IT infrastructure, cybersecurity measures and data recovery systems to meet resilience requirements.

5. Embed a culture of compliance and risk awareness.

Compliance with CPS 230 requires a cultural shift that promotes risk awareness across all levels of the organisation. To foster this culture, organisations should:

- Conduct mandatory, organisation-wide cyber training to increase awareness of operational risk and compliance requirements.
- Establish a transparent communication channel for reporting risks and incidents, ensuring that all employees understand the importance of timely reporting.
- Align performance incentives with risk management goals, encouraging proactive risk identification and mitigation efforts.

Risks of non-compliance

By taking the actions mentioned previously, organisations can not only address the business impacts of the revised CPS 230 but also strengthen their overall operational resilience and governance frameworks.

Conversely, ignoring or failing to address the business and technical imperatives outlined in the revised CPS 230 can pose significant risks to organisations in the financial services sector.

Five key risks associated with non-compliance are as follows:

1. **Regulatory penalties and sanctions.**
   Non-compliance with the revised CPS 230 can lead to severe financial penalties, enforcement actions or sanctions imposed by APRA. These could include fines, restrictions on business activities or even revocation of banking licenses. These actions would result in immediate financial losses and could severely disrupt business operations.

2. **Reputational damage.**
   Any failure to meet CPS 230 requirements, particularly in managing operational risks or responding to incidents, could harm an organisation's reputation. Customers, investors, and stakeholders may lose confidence in the organisation's ability to safeguard their interests, leading to loss of business, negative media coverage and long-term brand damage.

3. **Increased vulnerability to operational failures.**
   Ignoring the technical imperatives around operational resilience — such as incident management, IT security, and business continuity — can leave organisations vulnerable to disruptions such as cyberattacks, system failures and supply chain breakdowns. Without a robust framework in place, these incidents could result in prolonged downtime, financial losses and damage to critical infrastructure.

4. **Weak third-party risk management.**
   The revised CPS 230 emphasises the importance of managing outsourcing risks. Failure to address third-party risk management could expose organisations to service provider failures or breaches that affect critical operations. This lack of oversight could lead to non-compliance, data breaches or operational disruptions due to vendor mismanagement, which could negatively affect the entire business ecosystem.

5. **Deterioration in operational governance and risk culture.**
   Not prioritising operational risk management and governance could lead to an organisation-wide decline in risk awareness and accountability. This could result in poor decision-making, failure to identify risks and an inability to respond effectively to crises. A weak risk culture often leads to systemic issues that could escalate, ultimately affecting the organisation's long-term stability and performance.

Key leaders in CPS 230 compliance

Ensuring ongoing compliance with CPS 230 will typically require the involvement of several key leadership roles:

1. **Board of directors:**
   Tasked with establishing a strong organisational culture and ensuring the presence of an effective risk management framework, the board must oversee compliance with CPS 230 and hold senior management accountable for their actions.

2. **CEO and executive leadership:**
   Ultimately responsible for implementing CPS 230 throughout the organisation, the CEO and other executive leaders should ensure that the strategic direction integrates operational risk management effectively.

3. **Chief Risk Officer (CRO):**
   This role — critical under CPS 230 — involves direct oversight and management of operational risks, ensuring that risk management frameworks, policies and practices meet CPS 230 standards.

4. **Chief Compliance Officer (CCO):**
   Responsible for organisational adherence to all regulatory requirements, including CPS 230, the CCO manages and reports on compliance risks and collaborates with other leaders to ensure adequate controls are in place.

5. **Chief Operating Officer (COO):**
   Ensures that daily operational processes align with CPS 230 through appropriate controls and risk management practices.

6. **Chief Information Security Officer (CISO):**
   Given the focus on risk in CPS 230, particularly cyber and operational risks, the CISO is essential for maintaining the resilience of IT systems and robust cybersecurity measures.

7. **Internal audit:**
   Although not directly accountable for implementation, the internal audit function is crucial for reviewing and evaluating adherence to CPS 230, reporting findings to the board and senior management.

Maintaining compliance

The extended deadline of July 1st, 2025 has passed and APRA-regulated business should now be in compliance with CPS 230. Any organisations that have yet to achieve full compliance should prioritise the following steps:

1. Develop a compliance plan.

As soon as possible, create a strategy to meet the requirements of CPS 230, addressing operational risk, third-party risk management, and business continuity.

2. Engage with APRA.

Be prepared to show progress on risk management frameworks through updates or meetings with APRA.

3. Deliver organisational change.

Put in place the appropriate structures and controls to achieve full compliance, including governance, risk management, and operational resilience.

Compliance with CPS 230 is by no means a one-and-done exercise. Organisations will need to stay on top of their own changing businesses and any future modifications to the regulation. The key actions and key leaders sections in this white paper may provide useful guidance on maintaining compliance.

Conclusion

Non-compliance with CPS 230 poses significant risks to financial institutions, including regulatory penalties, reputational damage and operational disruptions. To ensure robust operational resilience and maintain regulatory confidence, prioritising adherence to CPS 230 is essential. Many organisations achieved full compliance ahead of the July 2025 deadline, mitigating risks and strengthening their risk management frameworks. Any remaining non-compliant organisations must move quickly to avoid penalties. Ultimately, all APRA-regulated entities must set up the appropriate organisational structures and controls to promote long-term compliance.

Why Kyndryl?

Kyndryl has deep experience in consulting and operations for financial services organisations. Many of the world's leading banks and insurance companies trust Kyndryl consultants to advise them on compliance with industry regulations. Combining industry experience with expertise in transformation and change management, Kyndryl helps organisations achieve and maintain compliance with regulations such as CPS 230.

For more information

To learn more about how Kyndryl can help you achieve and maintain CPS 230 compliance, please contact your Kyndryl representative or Kyndryl Business Partner, or visit kyndryl.com.

Author

Anandh Maistry is a Managing Partner Banking, Financial Services and Insurance, Growth and Telco Industry at Kyndryl, Australia and New Zealand.

kyndryl