Strengthening CPS 230 Resilience Through Internal Audit

Since 1 July 2025, APRA's Prudential Standard CPS 230 Operational Risk Management has been fully enforceable. The standard now shifts the focus from readiness to demonstrating resilience, requiring entities to prove that operational risk frameworks, business continuity plans and service provider arrangements operate effectively in practice.

Under CPS 230, Internal Audit has two mandated responsibilities:

- Periodically review the Business Continuity Plan (BCP) to assure the Board of its credibility and adequacy of testing (para 46), and
- Reviewing proposed material outsourcing arrangements relating to a Critical Operation (CO) and regularly report to the Board on compliance with the entity's service provider management policy (para 60).

Beyond these mandated responsibilities, Internal Audit plays a critical role in providing assurance that operational risk frameworks are not only in place but operate effectively under real conditions. It must go beyond confirming design, and challenge whether management decisions and controls operate effectively, adapt to emerging risks, and remain aligned to strategic objectives.

Our team brings hands-on experience implementing CPS 230 across multiple entities. This perspective gives us practical insight into where gaps typically emerge and what APRA expects as entities transition from implementation to ongoing compliance. Internal Audit must now provide assurance that operational risk frameworks can withstand real disruption and regulatory scrutiny.

Operational Risk Management

CPS 230 Sections 24 to 33

These sections require APRA-regulated entities to identify and manage a full range of operational risks, including legal and regulatory compliance, technology, data, supplier and change management. It also requires these processes to be embedded into governance, controls, monitoring, incident management and issue management. Our audits focus on whether these frameworks operate effectively under stress and regulatory scrutiny. We look for evidence that governance supports timely escalation, risk profiles drive informed decisions, and integrated risk data enables accurate reporting.

Key Audit Themes

- **Critical Operations:** Confirm that identified COs reflect actual business dependencies and tolerance levels, and that governance supports timely escalation during disruption.
- **Risk Profiles & Appetite:** Evaluate if operational risk profiles and KRIs drive timely decisions and Board reporting and confirm alignment with risk appetite and strategy.
- **Risk in Change:** Evaluate processes for managing risk during change initiatives and whether scenario analysis anticipates resilience risks.
- **Integrated Risk Data:** Verify that risk information is complete, timely and accurate across systems, enabling timely insights and escalation.
- **Governance:** Validate clarity of roles across management and the Board and confirm that responsibilities for operational risk management are embedded and traceable.

Artefacts Typically Reviewed

We review governance artefacts such as the Risk Appetite Statement, Risk Management Strategy, Risk Taxonomy and operational risk profiles to confirm risk informed decisions and align with resilience objectives.

Business Continuity Management

CPS 230 Sections 34 to 46

These sections require APRA-regulated entities to maintain the ability to continue COs during disruptions within defined tolerance levels. COs are processes that have a material impact on an entity's customers if a disruption occurs. Our reviews assess whether BCPs are credible in practice, including whether critical dependencies are understood, tolerances are realistic and recovery strategies are actionable under severe scenarios. We also examine whether continuity planning is embedded across operational risk and service provider frameworks, avoiding siloed recovery strategies, and whether testing programs validate resilience under varied scenarios and drive meaningful lessons learned.

Key Audit Themes

- **Business Impact Analysis:** Assess whether CO identification and tolerance metrics such as Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Recovery Level Objective (RLO), are realistic and actionable under severe disruption.
- **Business Continuity Plans:** Evaluate whether BCPs include activation triggers and escalation pathways that enable timely response, and whether execution risks and dependencies have been addressed.
- **Board Oversight:** Confirm that governance goes beyond sign-off and provides meaningful insights from testing and incident reviews to challenge resilience.
- **Integration:** Test whether continuity planning is embedded across operational risk and service provider frameworks, avoiding siloed recovery strategies.
- **Testing Program:** Review whether multi-year testing validates resilience under varied scenarios, including material service provider failures, and whether lessons learned drive continuous improvement.

Artefacts Typically Reviewed

Business Impact Analysis, BCPs, Disaster Recovery Plans, BCP test results and Board reporting packs are assessed to validate readiness under severe disruption.

Service Provider Management

CPS 230 Sections 47 to 60

These sections require APRA-regulated entities to govern material service providers, those relied upon for COs or that expose the entity to material operational risk, through robust frameworks, contractual provisions and ongoing oversight. Our audits assess whether oversight extends beyond direct providers to critical fourth-party dependencies and whether monitoring delivers actionable insights to senior management. We also review the enforceability of resilience-related contractual provisions and whether governance processes give Internal Audit adequate visibility of proposed material outsourcing arrangements. We further consider whether reporting mechanisms enable clear escalation of compliance issues to senior management and the Board.

Key Audit Themes

- **Governance Frameworks:** Assess whether service provider management policies are embedded into procurement and renewal processes.
- **Materiality Assessment:** Evaluate if risk and materiality assessments capture real dependencies and escalation triggers, and whether legacy arrangements have been uplifted to meet CPS 230 standards.
- **Contractual Provisions:** Review whether agreements include enforceable resilience obligations such as service levels, incident reporting, and termination clauses.
- **Monitoring and Reporting:** Test whether ongoing monitoring provides actionable insights to senior management, and whether performance failures trigger timely remediation.
- **Fourth-Party Risk:** Confirm that oversight extends beyond third-party providers to fourth-party dependencies that could compromise resilience.

Artefacts Typically Reviewed

Service Provider Management Policy, Material Service Provider Register, contractual agreements, exit plans and monitoring reports are reviewed to ensure resilience obligations are enforceable and monitored.

Conclusion

Looking ahead, APRA-regulated entities must maintain CPS 230 compliance on an ongoing basis. Certain areas will require continued attention and investment, particularly business continuity, scenario analysis and material service provider management, as reflected in the 12-month extension for non-SFI entities.

CPS 230 reinforces the need for disciplined operational risk ownership across all lines of defence. Internal Audit plays a critical role in providing independent assurance over the operating effectiveness of resilience frameworks, the maturity of governance and third-party oversight, and the entity's ability to apply CPS 230 principles to new and ongoing activities. By identifying improvement opportunities and validating how effectively risks are managed in practice, Internal Audit supports stronger decision-making and sustained operational resilience.

If your internal audit plan for 2026 includes CPS 230, we can work with your audit team to provide assurance where it matters most. Contact us to discuss how we can support your approach and help address APRA's expectations.

Our Authors

Katherina Sau
Director

Katherina is a risk and assurance practitioner experienced in internal audit and risk transformation, aligned to CPS 230 and broader risk frameworks across public and private sector clients. She has supported APRA-regulated entities with CPS 230 implementation, leading initiatives across Critical Operations identification, business continuity management reviews, and material service provider management uplift. She is CA, CIA and CRISC certified and serves as a member of the Audit, Finance and Risk Committee of Squash Australia.

Branden Lee
Senior Consultant

Branden is a risk practitioner with deep experience in internal audit and controls assurance, specialising in CPS 230, CPS 234, and broader operational risk frameworks across private-sector clients. His recent work includes supporting CPS 230 readiness for a global financial services provider through service-provider risk assessments, as well as leading internal audits over operational and financial processes for a major life insurer and a national energy provider.

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand.