

APRA CPS 230 — Operational Risk Management

CPS 230 is an APRA standard requiring banks, insurers, and superannuation funds to manage operational risks and ensure resilience.



Australian Government

What it is

Australia Prudential Standard CPS 230 – Operational Risk Management is a regulatory standard that assists financial institutions in identifying, assessing, and managing operational risks to support organizational resilience and regulatory compliance. It establishes systematic approaches to minimize disruptions from technology failures, internal process breakdowns, and external events.

Published by the Australian Prudential Regulation Authority (APRA), CPS 230 applies to entities regulated under the Banking, Insurance, and Superannuation Acts in Australia. The standard covers areas such as risk assessment, business continuity, incident management, internal controls, and third-party risk oversight, with a focus on operational resilience across critical business services.

At a glance

PUBLISHER

Australian Prudential Regulation
Authority (APRA)

TYPE

Framework

VERSION

CPS 230 — Operational Risk
Management

EFFECTIVE

July 2018

DOMAIN

Risk Management

FAMILY

Other

REGION

Australia

INDUSTRY

Financial Services

ADOPTION MODEL

Regulatory Compliance

IMPLEMENTATION COMPLEXITY

High

Source: <https://www.apra.gov.au/consultations/operational-risk-management>

Why it matters

- **Enhance operational resilience** Strengthen the ability to maintain critical services during technology failures, internal errors, or external disruptions.
- **Support regulatory compliance** Facilitate adherence to APRA requirements, reducing the likelihood of compliance breaches and associated penalties.
- **Improve incident response effectiveness** Enable rapid identification, management, and communication of incidents to limit business impact and support swift recovery.
- **Strengthen oversight of third-party risks** Establish consistent processes to monitor and mitigate risks arising from outsourced services and supply chain partners.

How SmartSuite supports APRA CPS 230

Operational Risk and Control Framework Structure operational risk categories, controls, and ownership aligned to CPS 230 requirements.	Critical Operations and Service Mapping Identify critical services, dependencies, and third-party providers with full traceability.	Business Continuity and Disruption Planning Manage continuity plans, recovery objectives, and disruption scenarios across operations.
Third-Party Risk and Outsourcing Oversight Track vendor risks, contracts, and performance monitoring for outsourced services.	Incident and Disruption Management Workflows Manage incident detection, response, escalation, and regulatory reporting obligations.	CPS 230 Compliance and Resilience Reporting Provide dashboards showing risk exposure, resilience posture, and CPS 230 compliance readiness.

Common framework mappings

APRA CPS 234

EU DORA

ISO 22301

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

Official resources

Australia Prudential Standard CPS 230 – Operational Risk Management Defines requirements for operational risk management for financial institutions in Australia. apra.gov.au/consultations/operational-risk-management	Operational Risk Management Guidance Provides implementation guidance supporting CPS 230 requirements for managing operational risks. apra.gov.au/consultations/operational-risk-management
Operational Resilience Overview Outlines APRA's approach to enhancing resilience across critical business services. apra.gov.au/consultations/operational-risk-management	Risk Management Framework Guidance Describes how organizations can integrate CPS 230 into their risk management frameworks. apra.gov.au/consultations/operational-risk-management

Frequently asked questions

- What is CPS 230 used for?**
CPS 230 is used to establish minimum standards for operational risk management and business continuity for entities regulated by the Australian Prudential Regulation Authority (APRA). It aims to ensure organizations identify, assess, and manage operational risks to achieve resilience against disruptions, internal failures, and external threats.
- Is CPS 230 mandatory?**
Yes, compliance with CPS 230 is mandatory for APRA-regulated entities in the banking, insurance, and superannuation sectors. Organizations are required to demonstrate alignment with the standard to maintain their regulatory standing and avoid potential enforcement actions.
- Who must comply with CPS 230?**
CPS 230 applies to financial institutions regulated by APRA, including authorized deposit-taking institutions (ADIs), general and life insurers, and superannuation trustees. Its coverage includes all business units, operations, and critical business services within these regulated entities.

What are the key operational risk concepts required by CPS 230?

Key concepts within CPS 230 include operational risk identification, risk assessment, governance structures, internal controls, incident management, business continuity planning, and third-party risk management. Entities must maintain documented artifacts such as risk registers, incident logs, and business continuity plans.

How should organizations implement CPS 230?

Organizations implement CPS 230 by integrating its requirements with their existing risk management frameworks, assigning clear accountabilities, and embedding operational controls. This includes conducting regular risk assessments, testing business continuity plans, and managing third-party arrangements in line with the standard.

How does CPS 230 relate to other risk management frameworks?

While CPS 230 has specific APRA requirements, it aligns with international standards such as ISO 27001 (information security) and the NIST Cybersecurity Framework. Integrating CPS 230 requirements with these frameworks can streamline operational risk management and enhance overall regulatory compliance.

What ongoing compliance activities are needed under CPS 230?

Ongoing compliance requires organizations to regularly review and test risk controls, update risk assessments, maintain current business continuity and incident management plans, and continuously monitor third-party arrangements. Evidence of compliance should be documented and made available for APRA review.

How would SmartSuite support CPS 230 (Operational Risk Management)?

SmartSuite helps organizations manage CPS 230 compliance through centralized risk and control registers, workflow-enabled policy governance, and scheduled compliance testing. It enables collection and storage of audit-ready evidence, tracks remediation tasks, and provides reporting dashboards for continuous operational risk monitoring and regulatory readiness.

License included / downloadable: Yes APRA Prudential Standard CPS 230 is publicly available through the Australian Prudential Regulation Authority.

Full framework page and mappings: smartsuite.com/frameworks/apra-cps-230-operational-risk-management