SmartSuite

Framework / Cybersecurity / Other

APRA CPS 234

APRA CPS 234 is the prudential standard that requires APRA-regulated entities to maintain information security capability, test controls, and notify APRA of incidents within 72 hours.



What it is

Prudential Standard CPS 234 Information Security is the Australian Prudential Regulation Authority's binding standard on information security. It commenced on 1 July 2019 and applies to authorized deposit-taking institutions, general insurers, life companies, private health insurers, and RSE licensees (superannuation trustees). Its aim is for each entity to be resilient to information security incidents, including cyber-attacks, by maintaining an information security capability that matches the size and extent of the threats to its information assets.

At a glance

PUBLISHER
Australian Prudential Regulation Authority (APRA)

TYPE
Framework

VERSION
CPS 234 Information Security (July 2019 version)

EFFECTIVE
July 1, 2019

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Australia

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: apra.gov.au/system/files/cps_234_july_2019_for_public_release.pdf

Why it matters

- **Board accountability** The Board of an APRA-regulated entity is ultimately responsible for information security and must ensure it is maintained in line with the size and extent of threats (paragraph 13).
- **Third-party coverage** Capability assessment, control design evaluation, testing assurance, and internal audit apply to assets managed by related parties and third parties, not only those under outsourcing agreements (paragraphs 16, 22, 28, and 34).
- **Tested response** Entities keep plans for incidents that could plausibly occur, covering every stage from detection to post-incident review, and review and test them annually (paragraphs 24 to 26).
- **Independent testing** A systematic testing program scaled to threats and asset criticality, run by skilled and functionally independent specialists, with its sufficiency reviewed at least annually (paragraphs 27 to 31).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports APRA CPS 234

Paragraph-level control map

Map CPS 234 paragraphs 13 to 36 to controls, owners, and evidence, with the CPG 234 practices alongside.

Asset classification

Record information assets, including third-party assets, with criticality and sensitivity ratings and an accountable owner.

Incident response plans

Hold response plans for plausible incidents with their annual review and test dates and Board escalation paths.

Testing program and internal audit

Plan systematic testing and internal audit reviews, record results, and escalate deficiencies that cannot be remediated in time.

Third-party assurance

Assess related-party and third-party capability and controls, and record the assurance reports relied on, using Third Party Risk Management.

Notification clocks

Track the 72-hour incident and 10-business-day control weakness notification deadlines to completion with Workflow Orchestration.

Common framework mappings

ASD Essential Eight | CIS Controls v8.1 | EU DORA | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

Australia Prudential Standard CPS 234 — Information Security

Defines minimum information security requirements for Australian financial institutions.

apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

Frequently asked questions

Who must comply with CPS 234?

All APRA-regulated entities: authorized deposit-taking institutions (including foreign ADIs for their Australian branch operations), general insurers, life companies, private health insurers, and RSE licensees in respect of their business operations. It commenced on 1 July 2019.

When must APRA be notified under CPS 234?

As soon as possible and no later than 72 hours after becoming aware of an information security incident that materially affected, or had the potential to materially affect, the entity or its customers, or that has been notified to other regulators. A material control weakness that will not be remediated in time must be notified within 10 business days.

What does CPS 234 require for third parties?

Entities must assess the capability of related and third parties managing information assets, evaluate the design of their controls, assess whether their control testing is adequate where the entity relies on it, and have internal audit assess third-party assurance it relies on. This covers all information assets managed by related and third parties, not only outsourcing arrangements.

How often must response plans and testing be reviewed?

Information security response plans must be reviewed and tested at least annually. The sufficiency of the testing program must be reviewed at least annually or when there is a material change to information assets or the business environment.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How do CPS 234, CPG 234, and CPS 230 fit together?

CPS 234 sets the binding information security requirements. CPG 234 is APRA's non-enforceable guide to sound practice for them. CPS 230 Operational Risk Management, applying since 1 July 2025, requires entities to meet CPS 234, and an incident reported under CPS 234 need not be reported again under CPS 230.

License included / downloadable: Yes APRA publishes CPS 234 on apra.gov.au and it is free to read and download. The text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/australia-prudential-standard-cps-234-information-security

 © 2026 SmartSuite Inc. All rights reserved.