SmartSuite

Framework / Cybersecurity / Other

APRA CPG 234: Information Security

APRA CPG 234 is APRA's non-enforceable practice guide to CPS 234, describing sound information security practice for Australian banks, insurers, and superannuation trustees.



What it is

APRA Prudential Practice Guide CPG 234 Information Security (June 2019) is the Australian Prudential Regulation Authority's guidance on sound practice for meeting Prudential Standard CPS 234, which has applied to APRA-regulated entities since 1 July 2019. Those entities are authorized deposit-taking institutions, general insurers, life companies, private health insurers, and RSE licensees (CPS 234, paragraph 2). The guide does not itself create enforceable requirements; the obligations sit in CPS 234.

CPG 234 is written for boards, senior management, and risk and information security specialists. It covers roles and responsibilities, information security capability, the policy framework, information asset identification and classification, implementation of controls, incident management, testing control effectiveness, internal audit, and notification, with Attachments A to H on security principles, training, identity and access, software security, cryptography, customer security, testing techniques, and reporting.

At a glance

PUBLISHER
Australian Prudential Regulation Authority (APRA)

TYPE
Guidance

VERSION
CPG 234 Information Security (June 2019)

EFFECTIVE
June 2019

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Australia

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: apra.gov.au/practice-guides/cpg-234

Why it matters

- **Board-ready oversight** The Considerations for the Board section lists six areas for a Board to challenge management on: roles and responsibilities, capability, policy framework, controls, testing, and internal audit.
- **Controls across the asset life-cycle** Controls are expected at every stage from planning and design to decommissioning, with responsibility allocated to a named information asset owner.
- **Third-party reach** CPS 234 extends capability, control design, testing, and internal audit assurance to information assets managed by related parties and third parties (paragraphs 16, 22, 28, and 34).
- **Clear notification triggers** CPS 234 requires notice to APRA within 72 hours of a material incident and within 10 business days of a material control weakness that will not be remediated in time (paragraphs 35 and 36).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports APRA CPG 234

CPS 234 requirement map

Map CPS 234 paragraphs 13 to 36 and the matching CPG 234 practices to controls and owners.

Asset classification

Record information assets with criticality and sensitivity ratings and an accountable information asset owner.

Incident and notification workflow

Run incidents from detection to post-incident review with Workflow Orchestration, tracking the 72-hour and 10-business-day notification clocks.

Testing and internal audit

Plan the systematic testing program 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 internal audit relies on, using Third Party Risk Management.

Board reporting

Use Enterprise Reporting to show control health, testing coverage, incidents, and open weaknesses to the Board.

Common framework mappings

APRA CPS 234 | ASD Essential Eight | CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

APRA CPG 234 Information Security Prudential Practice Guide

Defines guidance for Australian financial institutions on managing information security risks.

apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf

Frequently asked questions

Is APRA CPG 234 mandatory?

No. A prudential practice guide describes APRA's view of sound practice and does not itself create enforceable requirements. The enforceable obligations are in Prudential Standard CPS 234 Information Security, which CPG 234 helps entities implement.

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. CPS 234 commenced on 1 July 2019.

When must APRA be notified of an information security incident?

CPS 234 requires notice as soon as possible and no later than 72 hours after an entity becomes aware of an incident that materially affected, or could 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. CPG 234 says to notify even without complete information.

How does CPG 234 relate to CPS 230?

CPS 230 Operational Risk Management has applied since 1 July 2025. It requires entities to meet CPS 234 and says an information security incident reported under CPS 234 does not need to be reported separately under CPS 230. CPG 234 dates from June 2019 and predates CPS 230.

Does CPG 234 require ISO/IEC 27001 or the ASD Essential Eight?

No. The guide says it is not intended to replace or endorse existing industry standards, and that an entity would typically use discretion in adopting the standards it considers fit for purpose in specific control areas.

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

License included / downloadable: Yes APRA licenses CPG 234 under Creative Commons Attribution 3.0 Australia, which allows the text to be copied, distributed, and adapted with attribution and without implying APRA endorsement. The text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/apra-cpg-234-information-security-prudential-practice-guide