SmartSuite

Framework / Cybersecurity / Other

# APRA CPG 234: Information Security

APRA CPG 234 guides APRA-regulated financial institutions to manage information security risks and protect critical data assets.

## What it is

APRA CPG 234 — Information Security Prudential Practice Guide is a supervisory framework that provides guidance to Australian financial institutions on managing information security risks and protecting critical data assets. The guide outlines principles and expected practices for establishing and maintaining effective cybersecurity and information security capabilities.

Published by the Australian Prudential Regulation Authority (APRA), CPG 234 is primarily intended for banks, insurers, and superannuation entities regulated under APRA's remit. The guide addresses a range of areas, including cybersecurity controls, risk management, incident response, third-party security, and ongoing assurance, all within the context of regulatory compliance.

## At a glance

| | | |
|---|---|---|
| PUBLISHER<br>Australian Prudential Regulation Authority (APRA) | TYPE<br>Guidance | VERSION<br>CPG 234 |
| EFFECTIVE<br>June 2019 | DOMAIN<br>Cybersecurity | FAMILY<br>Other |
| REGION<br>Australia | INDUSTRY<br>Financial Services | ADOPTION MODEL<br>Regulatory Compliance |
| IMPLEMENTATION COMPLEXITY<br>High | | |

Source: https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf

## Why it matters

- **Strengthen information security management** Enable organizations to build robust information security frameworks that address evolving risks and regulatory demands.
- **Enhance regulatory compliance** Support ongoing adherence to APRA standards while facilitating alignment with industry-recognized information security frameworks and expectations.
- **Improve oversight of third-party risk** Guide institutions in managing risks associated with service providers, ensuring consistent security controls across outsourced arrangements.
- **Promote proactive incident response** Enable timely detection, escalation, and resolution of security incidents to minimize disruption and financial loss.


Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

## How SmartSuite supports APRA CPG 234

### Sound Practice Mapping to Controls

Translate CPG guidance into operational controls with clear ownership.

### Governance and Accountability Evidence

Track board/management oversight, decisions, and reporting artifacts.

### Risk Assessments and Treatment Plans

Run security risk assessments and manage mitigations with approvals.

### Assurance and Testing Cadence

Schedule testing, capture results, and track remediation through closure.

### Vendor Due Diligence and Monitoring

Manage due diligence, contract safeguards, and monitoring evidence for vendors.

### Regulator-Ready Reporting

Provide clear reporting on posture, gaps, and continuous improvement.

## 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

### What is APRA CPG 234 used for?

APRA CPG 234 is designed to guide Australian financial institutions in effectively managing information security risks and protecting critical data assets. It provides principles and recommended practices to meet APRA's expectations for information security capability and governance.

### Is compliance with APRA CPG 234 mandatory?

While CPG 234 is a prudential practice guide and not a legally enforceable standard, APRA-regulated entities are expected to align their practices with its recommendations. Non-compliance may signal inadequate risk management and can result in heightened supervisory attention.

### Who does APRA CPG 234 apply to?

CPG 234 applies to all financial institutions regulated by APRA, including banks, insurers, and superannuation entities. Its scope covers both internal information security arrangements and those involving third-party service providers.

### What are the key requirements of APRA CPG 234?

The guide emphasizes information security governance, risk identification and management, implementation of security controls, ongoing monitoring, and incident response. Organizations must regularly review their information security posture and ensure controls are appropriately designed and operating effectively.

### How should organizations implement APRA CPG 234?

Implementation involves establishing robust security policies, conducting regular risk assessments, and aligning controls with the guide's principles. Financial institutions must assign clear roles and responsibilities, maintain supporting documentation, and ensure continuous improvement through review and testing.


Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

### How does APRA CPG 234 relate to other security frameworks?

APRA CPG 234 can be integrated with internationally recognized standards, such as ISO 27001, to ensure comprehensive information security management. Organizations often map controls and processes across frameworks to streamline compliance and demonstrate alignment to multiple standards.

### What ongoing compliance activities are required by APRA CPG 234?

Ongoing compliance requires regular testing and review of controls, continuous risk monitoring, periodic staff training, and timely updates to policies and procedures. Accurate documentation and evidence collection are also essential to demonstrate compliance during audits.

### How would SmartSuite support APRA CPG 234?

SmartSuite enables organizations to operationalize APRA CPG 234 by providing centralized risk registers, control libraries aligned with regulatory expectations, and policy governance tools. It facilitates evidence collection, tracks remediation tasks, and supports audit readiness with reporting dashboards, streamlining ongoing compliance management.

License included / downloadable: Yes APRA CPG 234 is publicly available through the Australian Prudential Regulation Authority and can be accessed without a commercial license.

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