

APRA CPS 234

CPS 234 sets minimum information security requirements for APRA-regulated entities to manage cyber risk and protect sensitive data.



What it is

Australia Prudential Standard CPS 234 — Information Security is a regulatory framework that establishes minimum information security requirements to help organizations manage cybersecurity risks and protect sensitive data. It aims to strengthen the information security posture of regulated entities and ensure the resilience of critical financial systems.

Issued by the Australian Prudential Regulation Authority (APRA), CPS 234 applies to banks, insurers, superannuation trustees, and other APRA-regulated institutions. The standard mandates requirements for information security controls, risk assessments, incident response, and ongoing oversight of third-party service providers, focusing on both compliance and operational resilience.

At a glance

<div>PUBLISHER</div> <div>Australian Prudential Regulation Authority (APRA)</div>	<div>TYPE</div> <div>Framework</div>	<div>VERSION</div> <div>CPS 234</div>
<div>EFFECTIVE</div> <div>July 1, 2019</div>	<div>DOMAIN</div> <div>Cybersecurity</div>	<div>FAMILY</div> <div>Other</div>
<div>REGION</div> <div>Australia</div>	<div>INDUSTRY</div> <div>Financial Services</div>	<div>ADOPTION MODEL</div> <div>Regulatory Compliance</div>
<div>IMPLEMENTATION COMPLEXITY</div> <div>High</div>		

Source: https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

Why it matters

- **Strengthen cybersecurity governance** Enable effective oversight and accountability for information security risks across regulated entities and third-party service providers.
- **Enhance regulatory compliance** Support adherence to APRA's requirements and demonstrate organizational diligence through well-documented controls and risk assessments.
- **Improve incident response readiness** Require robust processes for timely detection, reporting, and management of security incidents affecting critical business operations.
- **Protect sensitive data assets** Reduce the risk of data breaches by enforcing stricter controls over the confidentiality, integrity, and availability of information.

How SmartSuite supports APRA CPS 234

Information Asset Inventory and Classification Track information assets, criticality, and owners with clear classification rules.	Control Implementation and Evidence Manage required security controls with implementation evidence and cadence.	Testing and Assurance Program Schedule control testing, capture results, and manage remediation to closure.
Incident Response and APRA Notification Readiness Track incidents, escalation decisions, and reporting evidence for APRA expectations.	Third-Party Service Provider Oversight Manage vendor due diligence, contracts, and ongoing monitoring evidence.	Leadership Reporting on Posture and Actions Provide leadership reporting on posture, gaps, testing status, and actions.

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

What is CPS 234 used for?

CPS 234 is designed to establish minimum information security requirements for APRA-regulated entities, such as banks, insurers, and superannuation trustees. It aims to strengthen the protection of sensitive data and ensure the resilience of critical Australian financial systems against cybersecurity threats.

Is CPS 234 mandatory for organizations?

Yes, CPS 234 is a mandatory prudential standard issued by APRA. All entities regulated by APRA must comply with its information security requirements or risk regulatory sanction.

Who does CPS 234 apply to?

CPS 234 applies to all APRA-regulated entities, including banks, credit unions, building societies, insurers, and superannuation trustees. It also extends to third-party service providers that manage or store information assets on behalf of these organizations.

What are the key artifacts required under CPS 234?

Key artifacts include documented security policies, risk assessment reports, information asset inventories, security control records, incident response procedures, and evidence of security testing and oversight. Entities must formalize governance and assign clear accountability for information security.

How is CPS 234 implemented within organizations?

Organizations must identify and classify information assets, assess associated security risks, implement appropriate controls, and ensure ongoing effectiveness through regular testing and reviews. Governance structures must clearly define roles and responsibilities for information security at the board and senior management levels.

How does CPS 234 relate to other information security frameworks?

CPS 234 can be aligned with international frameworks such as ISO 27001 and NIST SP 800-53, but it specifically addresses APRA's local regulatory requirements. Integration with broader cybersecurity programs helps organizations meet both local and global standards.

What ongoing compliance requirements does CPS 234 impose?

Entities must regularly review and update risk assessments, test security controls, monitor third-party performance, and promptly notify APRA of material security incidents. Compliance is demonstrated through audit trails, regulatory reporting, and evidence of continuous improvement.

How would SmartSuite support CPS 234?

SmartSuite enables organizations to manage CPS 234 compliance by mapping regulatory controls, tracking risk assessments, and documenting information asset classifications. It facilitates evidence collection for audits, supports control effectiveness monitoring, and streamlines regulatory reporting and incident management.

License included / downloadable: Yes APRA Prudential Standard CPS 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/australia-prudential-standard-cps-234-information-security