# Australia: APRA's CPS 234



OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

# Australia: APRA's CPS 234

The CPS 234 Information Security ('CPS 234') is a mandatory Prudential Standard issued by the Australian Prudential Regulation Authority ('APRA'). In particular, the CPS 234 applies to all APRA-regulated entities in banking, insurance and superannuation industries, and aims to ensure that regulated entities take appropriate measures to prevent, respond and notify information security incidents, including cyber threats, to the APRA.

## When Do The Requirements Take Effect?

The CPS 234 entered into effect on 1 July 2019. Where an APRA-regulated entity's information assets are managed by a third party, the CPS 234 will apply in relation to those assets from the earlier of the next renewal date of the contract with the third party or from 1 July 2020.

Furthermore, APRA published, on 25 June 2019, an updated version of the Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology to assist regulated entities in complying with the CPS 234 and includes guidance on classification and notification requirements.

**Key definitions**

**Information security capability:** Refers to the totality of resources, skills and controls which provide the ability and capacity to maintain information security.

**Information security control:** Refers to a prevention, detection or response measure to reduce the likelihood or impact of an information security incident;

**Information security incident:** Refers to an actual or potential compromise of information security.

**Information security policy framework:** Refers to the totality of policies, standards, guidelines and procedures pertaining to information security.

## Key Requirements

### Information Security Capabilities

The CPS 234 outlines that an APRA-regulated entity must maintain an information security capability which is proportionate to the size and extent of potential threats and which can be adapted to manage any changes in vulnerabilities and threats. The APRA-regulated entity must also assess the information security capability of a related or third party to ensure proportionality with any potential consequences of an information security incident.

### Policy Framework

An APRA-regulated entity must maintain an information security policy framework which takes into consideration any potential threats and vulnerabilities and outlines the role and responsibilities of all governing bodies, individuals and related parties that have an obligation to maintain information security.

### Asset Identification and Classification

Information assets must be classified by APRA-regulated entities based on the the degree to which an information security incident has the potential to affect, financially or non-financially, the entity or other interested parties.

### Implementation of Controls

The CPS 234 requires APRA-regulated entities to have information security controls in place to protect its information assets and considers, the criticality and sensitivity of the information assets the life-cycle stage of information assets, and any potential consequences of an information security incident. Where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party’s information security controls.

### Incident Management

The CPS 234 outlines requirements for APRA-regulated entities to put in place mechanisms to detect and respond to information security incidents in a timely manner. In particular, an APRA-regulated entity must maintain an information security response plan, which should be tested annually.

### Testing Control Effectiveness

An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing programme conducted by a skilled, independent specialist. The programme should be reviewed annually or in response to a material change. APRA-regulated entities should also assess the testing controls adopted by a related or third party. In addition, any testing results that identify information security control deficiencies that cannot be remediated in a timely manner must be reported to the Board or senior management.

### Internal Audit

An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties.

### Notification

Similar to the notification requirements under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), the CPS 234 introduces specific reporting obligations outlining that a regulated entity must notify the APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that:

- materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or
- have been notified to other regulators, either in Australia or other jurisdictions, such as the Office of the Australian Information Commissioner or a supervisory authority under the GDPR.

An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.