# Prudential Standard CPS 234

# Information Security

## Objectives and key requirements of this Prudential Standard

This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats.

A key objective is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.

The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security.

The key requirements of this Prudential Standard are that an APRA-regulated entity must:

- clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals;
- maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity;
- implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and
- notify APRA of material information security incidents.

## Authority

1. This Prudential Standard is made under:

   (a) section 11AF of the *Banking Act 1959* (**Banking Act**);

   (b) section 32 of the *Insurance Act 1973* (Insurance Act);

   (c) section 230A of the *Life Insurance Act 1995* (Life Insurance Act);

   (d) section 92 of the *Private Health Insurance (Prudential Supervision) Act 2015* (PHIPS Act); and

   (e) section 34C of the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

## Application

2. This Prudential Standard applies to all 'APRA-regulated entities' defined as:

   (a) **authorised deposit-taking institutions** (**ADIs**), including **foreign ADIs**, and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);

   (b) **general insurers**, including **Category C insurers**, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs), and **parent entities** of **Level 2 insurance groups**;

   (c) **life companies**, including **friendly societies**, **eligible foreign life insurance companies** (EFLICs) and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs);

   (d) **private health insurers** registered under the PHIPS Act; and

   (e) RSE licensees under the SIS Act in respect of their business operations.[1]

3. The obligations imposed by this Prudential Standard on, or in relation to, a foreign ADI, a Category C insurer or an EFLIC apply only in relation to the Australian branch operations of that entity.

4. Where an APRA-regulated entity is the 'Head of a group',[2] it must comply with a requirement of this Prudential Standard:

   (a) in its capacity as an APRA-regulated entity;

---

1 For the purposes of this Prudential Standard, an 'RSE licensee's business operations' includes all activities of an RSE licensee (including the activities of each RSE of which it is the licensee), and all other activities of the RSE licensee to the extent that they are relevant to, or may impact on, its activities as an RSE licensee.

2 Where a Level 2 group operates within a Level 3 group, a requirement expressed as applying to a Head of a group is to be read as applying to the Level 3 Head.

(b) by ensuring that the requirement is applied appropriately throughout the group, including in relation to entities that are not APRA-regulated; and

(c) on a group basis.

In applying the requirements of this Prudential Standard on a group basis, references in paragraphs 13 to 36 to an 'APRA-regulated entity' are to be read as 'Head of a group' and references to 'entity' are to be read as 'group'.

5. This Prudential Standard commences on 1 July 2019, subject to paragraph 6.

6. Where an APRA-regulated entity's information assets are managed by a third party, the requirements in this Prudential Standard will apply in relation to those information assets from the earlier of the next renewal date of the contract with the third party or 1 July 2020.

## Interpretation

7. Terms that are defined in *Prudential Standard APS 001 Definitions* (APS 001), *Prudential Standard GPS 001 Definitions* (GPS 001), *Prudential Standard LPS 001 Definitions*, *Prudential Standard HPS 001 Definitions* or *Prudential Standard 3PS 001 Definitions* appear in bold the first time they are used in this Prudential Standard.

8. In this Prudential Standard, unless the contrary intention appears, a reference to an Act, Regulation or Prudential Standard is a reference to the Act, Regulation or Prudential Standard as in force from time to time.

9. Where this Prudential Standard provides for APRA to exercise a power or discretion, the power or discretion is to be exercised in writing.

10. For the purposes of this Prudential Standard:

'group' means a Level 2 group or a **Level 3 group**, as relevant;

'Head of a group' means a Level 2 Head or **Level 3 Head**, as relevant;

'Level 2 group' means the entities that comprise:

(a) **Level 2** as defined in APS 001; or

(b) a Level 2 insurance group as defined in GPS 001;

'Level 2 Head' means:

(a) where an ADI that is a member of a Level 2 group is not a subsidiary of an authorised banking NOHC or another ADI, that ADI;

(b) where an ADI that is a member of a Level 2 group is a subsidiary of an authorised banking NOHC, that authorised banking NOHC; or

(c) the parent entity of a Level 2 insurance group as defined in GPS 001.

## Adjustments and exclusions

11. APRA may adjust or exclude a specific prudential requirement in this Prudential Standard in relation to an APRA-regulated entity.[3]

## Definitions

12. The following definitions are used in this Prudential Standard:

    (a) *availability* refers to accessibility and usability when required;

    (b) *confidentiality* refers to access being restricted only to those authorised;

    (c) *criticality* refers to the potential impact of a loss of availability;

    (d) *information asset* means information and information technology, including software, hardware and data (both soft and hard copy);

    (e) *information security* means the preservation of an information asset's confidentiality, integrity and availability;

    (f) *information security capability* means the totality of resources, skills and controls which provide the ability and capacity to maintain information security;

    (g) *information security control* means a prevention, detection or response measure to reduce the likelihood or impact of an information security incident;

    (h) *information security incident* means an actual or potential compromise of information security;

    (i) *information security policy framework* means the totality of policies, standards, guidelines and procedures pertaining to information security;

    (j) *information security threat* (threat) is a circumstance or event that has the potential to exploit an information security vulnerability;

    (k) *information security vulnerability* (vulnerability) is a weakness in an information asset or information security control that could be exploited to compromise information security;

    (l) *integrity* refers to completeness, accuracy and freedom from unauthorised change or usage; and

    (m) *sensitivity* means the potential impact of a loss of confidentiality or integrity.

---

[3] Refer to subsection 11AF(2) of the Banking Act, subsection 32(3D) of the Insurance Act, subsection 230A(4) of the Life Insurance Act, subsection 92(4) of the PHIPS Act and subsection 34C(5) of the SIS Act.

## Roles and responsibilities

13. The Board[4] of an APRA-regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must **ensure** that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.[5]

14. An APRA-regulated entity must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions.[6]

## Information security capability

15. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.

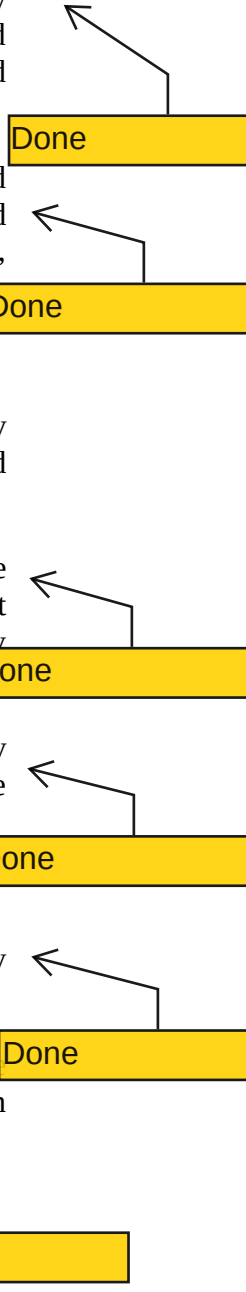
16. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.[7]

17. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.

## Policy framework

18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.

19. An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.[8]




4 For an RSE licensee, a reference to the Board is to be read as a reference to the Board of directors or group of individual trustees of an RSE licensee, as applicable. 'Group of individual trustees' has the meaning given in subsection 10(1) of the SIS Act.

5 A reference to the Board in the case of a foreign ADI, is a reference to the **senior officer outside Australia.**

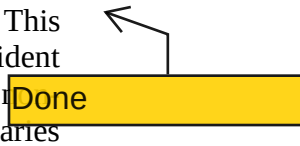
6 For the purposes of this Prudential Standard, governing bodies and individuals includes committees, working groups and forums.

7 For the avoidance of doubt, paragraph 16 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

8 For the purpose of paragraph 19 of this Prudential Standard, parties includes governing bodies and individuals with responsibilities referred to in paragraph 14, as well as all other staff, contractors, consultants, related parties, third parties and customers.

## Information asset identification and classification

20. An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.




## Implementation of controls

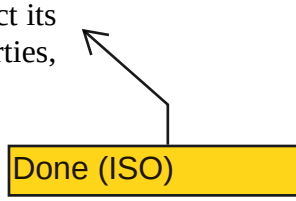
21. An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with:

    (a) vulnerabilities and threats to the information assets;

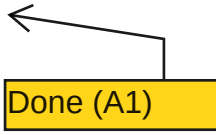
    (b) the criticality and sensitivity of the information assets;

    (c) the stage at which the information assets are within their life-cycle;[9] and

    (d) the potential consequences of an information security incident.



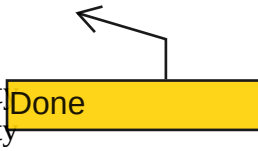

22. Where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity.[10]




## Incident management

23. An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.

24. An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).




25. An APRA-regulated entity's information security response plans must include the mechanisms in place for:

    (a) managing all relevant stages of an incident, from detection to post-incident review; and

---

9 The use of the term 'life-cycle' in this context refers to the process from planning and design through to decommissioning and disposal of an information asset.

10 For the avoidance of doubt, paragraph 22 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

(b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate.

26. An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.

ISO 27001

## Testing control effectiveness

27. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:

Annual ISO 27001 Test

(a) the rate at which the vulnerabilities and threats change;

(b) the criticality and sensitivity of the information asset;

(c) the consequences of an information security incident;

(d) the risks associated with exposure to environments where the APRA-regulated entity is unable to enforce its information security policies;[11] and

(e) the materiality and frequency of change to information assets.

28. Where an APRA-regulated entity's information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of this Prudential Standard.[12]

29. An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.

30. An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.

31. An APRA-regulated entity must review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment.

## Internal audit

32. An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including

ISO 27001 - August

[11] Also referred to as an 'untrusted' environment.

[12] For the avoidance of doubt, paragraph 28 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

those maintained by related parties and third parties (information security control assurance).

33. An APRA-regulated entity must ensure that the information security control assurance is provided by personnel appropriately skilled in providing such assurance.

34. An APRA-regulated entity's internal audit function must assess the information security control assurance provided by a related party or third party where:

    (a) an information security incident affecting the information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and

    (b) internal audit intends to rely on the information security control assurance provided by the related party or third party.[13]

## APRA notification

35. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that:

    (a) 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

    (b) has been notified to other regulators, either in Australia or other jurisdictions.[14]

Will do when In
occurs

36. 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.

---

13 For the avoidance of doubt, paragraph 34 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

14 For the avoidance of doubt, paragraph 35 of this Prudential Standard applies to notifications of information security incidents not already captured as notifications under *Prudential Standard CPS 231 Outsourcing, Prudential Standard SPS 231 Outsourcing, Prudential Standard CPS 232 Business Continuity Management* or *Prudential Standard SPS 232 Business Continuity Management*. Other regulators include domestic government agencies and international regulators.