PRO-26: CPS 234 - SUMMARY REPORT

PROGRAM SUMMARY

2021/04/21

Effective From 2019-12-31 16:00:00
Effective To N/A
Report Date 2021-04-21 13:14:08

Standards CPS Summary

Description

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 minimize 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: a)classify its information assets by criticality and sensitivity to determine the potential impact of an information security incident on the entity and the interests of beneficiaries and other customers; b)clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals; c)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 d)notify APRA of material information security incidents.

Scope

This Prudential Standard applies to all 'APRA-regulated entities' defined and 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.

Notes

xMatters continuous its commitment to compliance and transparency!

In our continuous efforts to improve and implement controls and safeguards for our clients, xMatters has undergone self-assessment to affirm our compliance with the latest Prudential Standard CPS 234 Information Security introduced by the Australian Prudential Regulation Authority (APRA).

The Prudential Standard CPS 234 Information Security is a federal law for APRA-regulated entities and came into effect on 1 July 2019. The CPS 234 will help the APRA-regulated entities' resilience against information security incidents, and their ability to respond swiftly and effectively in the event of a breach. CPS 234 requires APRA-regulated entities and suppliers to:

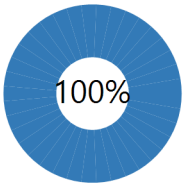
Clearly define information-security related roles and responsibilities;

Maintain an information security capability commensurate with the size and extent of threats to their information assets;

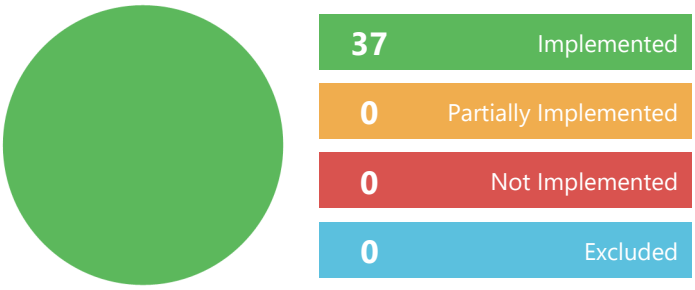
Implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls; and

Promptly notify APRA of material information security incidents.

Overall Progress



Implementation Status



Total Controls/Policies

18

Number of Requirements

37

Requirements Per Standard

Requirement	Status	Owner
CPS SUMMARY		
(No Category)		
1.1	Implemented	Information Assurance Department
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.		
1.2	Implemented	Information Assurance Department
Information security capability 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.		
1.3	Implemented	Information Assurance Department
Information security capability 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.		
2.1	Implemented	Information Assurance Department
Policy framework 18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.		
2.2	Implemented	Information Assurance Department
Policy framework 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.		
3	Implemented	Information Assurance Department
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.		
4.1	Implemented	Information Assurance Department
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:		
04.1.1	Implemented	Information Assurance Department
Implementation of controls (a) vulnerabilities and threats to the information assets;		
04.1.2	Implemented	Information Assurance Department
Implementation of controls (b) the criticality and sensitivity of the information assets;		

04.1.3	**Implemented**	Information Assurance Department

Implementation of controls
(c) the stage at which the information assets are within their life cycle; and

04.1.4	**Implemented**	Information Assurance Department

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

4.2	**Implemented**	Information Assurance Department

Implementation of controls
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.

5.1	**Implemented**	Information Assurance Department

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.

5.2	**Implemented**	Information Assurance Department

Incident management
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).

5.3	**Implemented**	Information Assurance Department

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

05.3.1	**Implemented**	Information Assurance Department

Incident management
(a) managingall relevant stages of an incident, from detection to post-incident review; and

05.3.2	**Implemented**	Information Assurance Department

Incident management
(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.

5.4	**Implemented**	Information Assurance Department

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

6.1	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
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:

06.1.1	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
(a) the rate at which the vulnerabilities and threats change;

06.1.2	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
(b) the criticality and sensitivity of the information asset;

06.1.3	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
(c) the consequences of an information security incident; and

06.1.4	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
(d) the risks associated with exposure to environments where the APRA-regulated entity is unable to enforce its information security policies; and

06.1.5	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
(e) the materiality and frequency of change to information assets.

6.2	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
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.

6.3	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
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.

6.4	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
30. An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.

6.5	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
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.

6.6	**Implemented**	Information Assurance Department

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

6.7	**Implemented**	Information Assurance Department

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

6.8	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
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:

06.8.1	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
(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

06.8.2	**Implemented**	Information Assurance Department

Testing control effectiveness&Internal Audit
(b) internal audit intends to rely on the information security control assurance provided by the related party or third party.

7.1	**Implemented**	Information Assurance Department

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:

07.1.1	**Implemented**	Information Assurance Department

APRA notification
(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

07.1.2	**Implemented**	Information Assurance Department

APRA notification
(b) has been notified to other regulators, either in Australia or other jurisdictions.

7.2	**Implemented**	Information Assurance Department

APRA notification
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.