Connect › Support › Advance

The Institute of Internal Auditors Australia

Whitepaper

APRA CPS 234 Information Security

March 2023

Level 5, 580 George Street, Sydney NSW 2000 | PO Box A2311, Sydney South NSW 1235
T +61 2 9267 9155 **F** +61 2 9264 9240 **E** enquiry@iia.org.au **www.iia.org.au**

APRA CPS 234 Information Security

Contents

Background

Purpose

The purpose of this White Paper is to capture suggested information security auditing techniques within the financial services and insurance sectors. It does not explore every element but focuses on high-level expectations.

Background

The Australian financial services and insurance industry is regulated by the Australian Prudential Regulation Authority (APRA) which has recognised the importance of financial institutions having strong information security.

Prudential Standard CPS 234 'Information Security' is a regulation issued by APRA that took effect on 1 July 2019. It requires organisations in the financial services and insurance sectors to strengthen their information security framework to protect their organisation and their customers from threat of cyber attacks.

CPS 234 contains specific requirements in relation to information security for internal audit in the financial services and insurance sectors. CPS 234 is supported by a Prudential Practice Guide (CPG 234).

The Institute of Internal Auditors-Australia (IIA-Australia) has also issued CPS 234 guidance in its 20 Critical Questions Series publication 'What Directors Should Ask About Prudential Standard CPS 234 Information Security' (2023).

Discussion

Issue

Information security is is concerned with protecting information and ICT systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Information security has become vital to most organisations in today's connected world. Well-publicised information security breaches at Australian companies Optus (Office of the Australian Information Commissioner, 2022a) and Medibank (Office of the Australian Information Information Commissioner, 2022b) in 2022 highlight how important information security is to an organisation. Internal audit assurance activities are vital to protecting information in every organisation, whether mandated by CPS 234 or not.

Internal audit plays role in confirming an organisation's information security capability with the board and its audit committee and risk committee. There are many interconnected parties involved with information security including an organisation's customers, third party suppliers, internal stakeholders, external stakeholders and regulators.

The APRA-mandated internal audit role is to assess compliance with CPS 234 for regulated organisations.

History

The Three Lines Model has been long established in the financial services sector. It was mentioned by the Basel Committee on Banking Supervision in 'Sound Practices for the Management and Supervision of Operational Risk' (2011) and in 'Corporate Governance Principles for Banks' (2015). Therefore, It is not unreasonable to assert that the 2019 Australian regulations were written with the expectation that regulated financial services institutions would adopt the three lines model for assurance.

CPS 234 came into force on 1 July 2019. The standard applies to all APRA regulated entities which includes banks, general insurers, life insurers, private health insurers and superannuation funds – registrable

APRA CPS 234 Information Security

superannuation entity (RSE) licensees under the 'Superannuation Industry (Supervision) Act 1993'.

The APRA 2020–2024 'Cyber Security Strategy' made it clear for the 680 entities it supervises that it is establishing a baseline of cyber controls with 'non-negotiable' cyber practices (Australian Prudential Regulation Authority, 2020).

The APRA 'Cyber Security Strategy' aims to increase board and executive management focus on information security risks, with internal audit seen as the 'eyes and ears' of a board into their organisation's information security operations and practices. APRA also aims to rectify weak links in the broader financial services ecosystem and supply chain which is estimated to cover around 17,000 inter-connected businesses and markets.

Discussion

APRA Requirements

CPS 234 Component	What It Means
Roles and Responsibilities	› The board of directors is ultimately responsible. › The board must ensure information security is maintained. › Information security-related roles and responsibilities must be defined.
Information Security Capability	› Information security capability must be maintained – this includes for third parties. › Capability must be maintained with respect to changes in vulnerabilities and threats.
Policy Framework	› Information security policy framework must be maintained. › Policy framework must provide direction on responsibilities of all parties with information security obligations.
Information Asset Identification and Classification	› Information assets must be classified including those managed by third parties.
Implementation of Controls	› There must be information security controls to protect information assets. › Design of information security controls of third parties must be evaluated.
Incident Management	› There must be robust mechanisms to detect and respond to information security incidents in a timely manner. › There must be plans to respond to plausible information security incidents that could occur. › Information security response plans must be reviewed and tested annually.
Testing Control Effectiveness	› Information security controls must have their effectiveness tested through a systematic testing program – this includes third parties. › Information security control deficiencies identified by testing must be escalated to the board or senior management. › Testing must be performed by appropriately skilled and functionally independent specialists.
Internal Audit	› Internal audit must review design and operating effectiveness of information security controls – this includes for third parties. › Information security control assurance must be provided by personnel appropriately skilled in providing such assurance. › Internal audit must assess information security control assurance provided by a related party or third party where (a) an information security incident affecting information assets has potential to have a material effect (b) internal audit intends to rely on such assurance.
APRA notification	› APRA must be advised no later than 72 hours after a material information security incident occurs. › APRA must be advised no later than 10 business days after a material information security control weakness is identified.

APRA CPS 234 Information Security

CPS 234 Internal Audit Related Requirements

CPS 234 contains internal audit related requirements in relation to information security in the financial services and insurance sectors:

Internal audit

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

CPS 234 Assurance Methods

If your organisation is covered by CPS 234, is your internal audit function adequately skilled to independently critique CPS 234 requirements versus the level of information security controls established within the organisation?

It is worthwhile noting that in an October 2022 presentation to the Customer Owned Banking Association, APRA noted there is "Lack of / inconsistent involvement from Lines 2 and 3 in control testing".

Internal audit is required to evaluate information security controls, whether a service is provided in-house or by a related party or third party supplier. Internal audit must assess information security control assurance provided by a related party or third party if it intends to rely upon it (para 34b). A related party or third party includes all suppliers and not just those captured by APRA Prudential Standard CPS 231 'Outsourcing'.

In providing its assurance, internal audit is expected to achieve comprehensive assurance over time. It will consider the extent to which it can rely on other assurance providers and changes in risk triggered by new threats or other changes to the IT context (Australian Prudential Regulation Authority, 2019a, para 84).

For example, an insurer engages a supplier to manage and produce its customer statements and a file containing confidential customer data is shared between the organisations for this purpose. Internal audit may rely on third party assurance over the supplier generating the customer statements, provided it is satisfied the level of assurance covers all controls of the primary organisation being audited.

Assurance can be obtained through:

- Internal audit.
- External consulting firms.
- Reliance upon third party reviews.

Tripartite independent information security reviews across APRA regulated entities are required. In a tripartite review, boards are required to engage an external consulting firm approved by APRA to conduct a thorough review of their CPS 234 compliance and report back to both the board and APRA. (Australian Prudential Regulation Authority, 2021)

CPS 234 Audit Steps

Information security audit practices with a focus on CPS 234 are suggested on the following page.

APRA CPS 234 Information Security

Audit Step	CPS 234 Reference	Good Practice
Roles and Responsibilities	Para 13 para 14	› Is the board of directors aware of its responsibility for information security? › Is this clearly stated in the board charter? › Does the board ensure information security is maintained through regular meeting agenda items and oversight? › Are information security and related metrics standing agenda items and reviewed at board and executive meetings? › Are all information security-related roles and responsibilities clearly defined in policy and job descriptions? › Is there an organisation awareness program to ensure understanding of what this means?
Information Security Capability	para 15 para 16 para 17	› Does the organisation maintain information security capability? › Does this include related party and third party information security capability? › Is there a strong due diligence process for assessing business partner and third party information security capability? › Is information security capability maintained with respect to changes in vulnerabilities and threats? › Are vulnerabilities and threats routinely re-assessed? › Is there a cybersecurity strategy identifying adversaries, threats and vulnerabilities? › Does this include mitigation plans?
Policy Framework	para 18 para 19	› Is there a comprehensive information security policy framework? › Is it approved by the board? › Is it regularly reviewed and kept up-to-date? › Does the information security policy framework provide direction on responsibilities of all parties with information security obligations? › Does this include related parties and third parties?
Information Asset Identification and Classification	para 20	› Are responsibilities related to information assets clearly defined? › Are information assets identified? › Are information assets classified by criticality and sensitivity? › Do assigned classifications affect the degree of importance and therefore the amount of oversight and assurance activities? › Are information assets protected based on their classification? › Is there a process in place to regularly review the information security asset register and relevant controls? › Does this include information assets managed by related parties and third parties?
Implementation of Controls	para 21 para 22	› Is information security risk periodically re-assessed to consider changes in vulnerabilities, threats and information asset holdings? › Is design of information security controls of related parties and third parties periodically evaluated to ensure their adequacy to address identified risks?
Incident Management	para 23 para 24 para 25 para 26	› Does the organisation have an information security / data breach / cyber incident response plan in place to manage such things as APRA notification, third party management and incident management? › Is the plan regularly reviewed and updated by relevant stakeholders and approved by the board? › Are there robust mechanisms to detect and respond to information security incidents in a timely manner? › Does the board monitor the level of incidents? › Are there plans to respond to plausible information security incidents that could occur? › Are information security response plans reviewed and tested at least annually?

APRA CPS 234 Information Security

Testing Control Effectiveness	para 27 para 28 para 29 para 30 para 31	› Do information security controls have their effectiveness tested through a systematic testing program? › Does this include related party and third party information security controls? › Is testing performed by appropriately skilled and functionally independent Line 2 technical specialists? › Is sufficiency of the testing program reviewed at least annually or when material change to information assets or the business environment occurs? › Are information security control deficiencies identified by testing escalated to senior management and the board / audit committee? › Are information security control deficiencies recorded and diligently followed-up to ensure remediation is implemented in a timely manner according to risk exposure?
Internal Audit	para 32 para 33 para 34	› Has the internal audit function worked with the cybersecurity function to ensure internal audit services review the most critical cyber controls? › Does internal audit review design and operating effectiveness of information security controls? › Does this encompass operation of the systematic Line 2 testing program? › Does this include for related party and third party design and operating effectiveness of information security controls? › Is information security control assurance provided by appropriate technical specialists skilled in providing such assurance? › Does internal audit assess information security control assurance provided by a related party or a third party where (a) an information security incident affecting information assets has potential to have a material effect (b) internal audit intends to rely on such assurance?
APRA notification	para 35 para 36	› Is there a formal APRA notification policy approved by the board? › Is APRA advised no later than 72 hours after a material information security incident occurs? › Is APRA advised no later than 10 business days after a material information security control weakness is identified? › Has the board developed a policy on the meaning of 'material'? Has this been discussed with APRA?

Conclusion

Summary

As we continue to live in an even more interconnected electronic word, protection of information from the perspective of both organisations and customers is paramount.

APRA has flagged their intentions in this area, and it's time for financial service and insurance entities to critically analyse their people, systems and processes with respect to information security.

Conclusion

It is critical for internal auditors to diligently follow the requirements of CPS 234 including guidance within APRA Prudential Practice Guide CPG 234 'Information Security'.

Demonstrated information security skills and experience on the internal audit team will go a long way to an effective CPS 234 audit regime and a sound outcome for stakeholders.

APRA CPS 234 Information Security

Bibliography and References

Australian Prudential Regulation Authority, 2019a. Prudential Practice Guide CPG 234 Information Security. [Online] Available at: https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf

Australian Prudential Regulation Authority, 2019b. Prudential Standard CPS 234 Information Security. [Online] Available at: https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

Australian Prudential Regulation Authority, 2020. Executive Board Member Geoff Summerhayes - speech to Financial Services Assurance Forum. [Online] Available at: https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

Australian Prudential Regulation Authority, 2021. Improving cyber resilience: the role boards have to play. [Online] Available at: https://www.apra.gov.au/news-and-publications/improving-cyber-resilience-role-boards-have-to-play

Basel Committee on Banking Supervision, 2011. Principles for the Sound Management of Operational Risk. [Online] Available at: https://www.bis.org/publ/bcbs96.pdf

Basel Committee on Banking Supervision, 2015. Guidelines: Corporate governance principles for banks. [Online] Available at: https://www.bis.org/bcbs/publ/d328.pdf

Office of the Australian Information Commissioner, 2022a. OAIC opens investigation into Optus over data breach. [Online] Available at: https://www.oaic.gov.au/updates/news-and-media/oaic-opens-investigation-into-optus-over-data-breach

Office of the Australian Information Information Commissioner, 2022b. OAIC opens investigation into Medibank over data breach. [Online] Available at: https://www.oaic.gov.au/updates/news-and-media/oaic-opens-investigation-into-medibank-over-data-breach

The Institute of Internal Auditors - Australia, 2023. The 20 Critical Questions Series: What Directors should ask about Prudential Standard CPS 234 Information Security. [Online].

Purpose of White Papers

A White Paper is a report authored and peer reviewed by experienced practitioners to provide guidance on a particular subject related to governance, risk management or control. It seeks to inform readers about an issue and present ideas and options on how it might be managed. It does not necessarily represent the position or philosophy of the Institute of Internal Auditors-Global and the Institute of Internal Auditors–Australia.

Author's Biography

This White Paper written by:
Malcolm Webster BComm(Mgmt), GradDip(CIT), DipFP, GradCert (Cyber Security)
Mal Webster is Chief Risk Officer of financial services institution Australian Mutual Bank Limited (AMBL). During his career, Mal has worked in a variety of risk and audit roles. At the Commonwealth Bank of Australia, he worked on retail network audits, analytics and ICT audits. Mal has exposure to Information technology practices, including direct exposure to APRA's tripartite reviews against CPS 234, and has formal qualifications in Information Technology and Cyber Security. Prior to that, Mal worked for ASX Top 50 companies ANZ, TabCorp and Westfield in a variety of roles.

This White Paper edited by:

Michael Parkinson BSc(Hons), GradDipComp, PFIIA, CIA, CISA, CRMA, CRISC

Andrew Cox MBA, MEC, GradDipSc, GradCertPA, DipBusAdmin, DipPubAdmin, AssDipAcctg, CertSQM, PFIIA, CIA, CISA, CFE, CGAP, CSQA, MACS Snr, MRMIA

Fred Taweel BBus (BusAdmin), GradDipAppCorpGov, CIA, CFE, PFIIA, FGIA, FCGI(CS,CGP)

APRA CPS 234 Information Security

About the Institute of Internal Auditors–Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

The IIA-Australia ensures its members and the profession are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

The IIA was established in 1941 and now has more than 200,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

Copyright

Disclaimer