The Institute of Internal Auditors Australia

The 20 Critical Questions Series

What Directors should ask about Prudential Standard CPS 234 Information Security

Prudential Standard CPS 234 Information Security applies to all Australian Prudential Regulation Authority (APRA) regulated entities which includes banks, general insurers, life insurers, private health insurers and registrable superannuation entity (RSE) licensees under the Superannuation Industry (Supervision) Act. It came into force on 1 July 2019.

Information Security – Is concerned with protecting information and ICT systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Information Security Capability – The totality of resources, skills and controls which provide the ability and capacity to maintain information security.

Cybersecurity – Protection of internet-connected systems and data from cyber threats to protect against unauthorised access.

ICT – A term used to holistically include information, communication and technology (ICT) related matters within an organisation – used interchangeably with the simpler abbreviation IT (information technology).

Roles and Responsibilities

1. 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?
2. 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

3. 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?
4. 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

5. Is there a comprehensive information security policy framework? Is it approved by the board? Is it regularly reviewed and kept up-to-date?
6. 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

7. 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

8. Is information security risk periodically re-assessed to consider changes in vulnerabilities, threats and information asset holdings?
9. Is design of information security controls of related parties and third parties periodically evaluated to ensure their adequacy to address identified risks?

What Directors should ask about Prudential Standard CPS 234 Information Security

Incident Management

10. 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?
11. 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?
12. Are information security response plans reviewed and tested at least annually?

Testing Control Effectiveness

13. 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?
14. Is sufficiency of the testing program reviewed at least annually or when material change to information assets or the business environment occurs?
15. Are information security control deficiencies identified by testing escalated to senior management and the board / audit committee?
16. 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

17. 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?
18. Is information security control assurance provided by appropriate technical specialists skilled in providing such assurance?
19. 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

20. 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?

The Big Question

How does the board and senior management know it has strong information security processes in place that are operating effectively, and that the organisation is compliant with APRA Prudential Standard 234 Information Security