

Prudential Standard CPS 234 and ISO/IEC 27001



APRA CPS 234 Requirement	ISO 27001:2013 Requirement	Requirement Overview	ISO 27001:2013 Annex A Reference Control	Control Overview
<p>security ate with threats ts, and tinued e entity;</p> <p>CI 6.1; CI 6.2; CI 8.1</p>	<p>IR/IS/ IR/RO/IR/ IR/IR/ RPP/</p>	<p>When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed. The organization shall define and apply an information security risk assessment process.</p>	<p>A.8.1.1; A.12.6.1</p>	<p>All IS roles & re be defined and</p> <p>Inventory of ass associated with information pro shall be identifi of these assets</p> <p>about technical information syst shall be obtaine the organization such vulnerabilit appropriate mea address the ass</p>

<p>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</p>	<p>CI 8.1; CI 8.2; CI 8.3</p>	<p>The organization shall plan, implement and control the processes needed to meet information security requirements. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.</p>	<p>A.8.1.1 ; A.8.1.2; A.8.1.3; A.8.1.4</p>	<p>Inventory of assets - Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.</p> <p>Assets maintained in the inventory shall be owned.</p> <p>Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.</p> <p>All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.</p>
<p>Notify APRA of material information security incidents.</p>	<p>CI 10.1; CI 10.2</p>	<p>When a nonconformity occurs, the organization shall:</p> <p>a) react to the nonconformity, and as applicable:</p> <p>1) take action to control and correct it; and</p> <p>2) deal with the consequences.</p>	<p>A.16.1.1 ; A.16.1.2; A.16.1.3</p>	<p>Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents. Information security events shall be reported through appropriate management channels as quickly as possible. Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.</p>

Information security capability

An APRA-regulated entity must establish an information security capability that meets the requirements of paragraph 12 (i.e. Board is responsible for maintaining IS).

CI 4.4 ; CI 5.2

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard. Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this International Standard; and

b) reporting on the performance of the information security management system to top management.

A.5.1.1; A.5.1.2;
A.6.1.1

Set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

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.

CI 6.1 ; 8.1

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall ensure that outsourced processes are determined and controlled.

A.15.1.1;
A.16.1.4;
A.16.1.5;
A.16.1.7

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. Information security events shall be assessed and it shall be ensured that the organization's information security requirements are met.

o

<p>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.</p>	<p>CI 5.1 , 5.2, 5.3</p>	<p>d) includes a commitment to continual improvement of the information security management system.</p> <p>The information security policy shall:</p> <p>e) be available as documented information;</p> <p>f) be communicated within the organization; and</p> <p>g) be available to interested parties, as appropriate.</p>	<p>A.14.2.1; A.15.1.1</p>	<p>Rules for the development of software and systems shall be established and applied to developments within the organization. Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.</p>
--	--------------------------	--	-------------------------------	--

Information asset identification and classification

<p>An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. Criticality and sensitivity is the degree to which an information security incident affecting that information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.</p>	<p>CI 6.1, 8.1,8.2</p>	<p>The organization shall define and apply an information security risk assessment process that:</p> <p>c) identifies the information security risks:</p> <ol style="list-style-type: none"> 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners; 	<p>A.8.1.1;A.8.1.3; A.8.2.1;A.8.2.2</p>	<p>Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.</p>
--	------------------------	---	---	--

Implementation of controls

<p>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:</p> <p>(a) vulnerabilities and threats to the information assets;</p> <p>(b) the criticality and sensitivity of the information assets;</p> <p>(c) the stage at which the information assets are within their life cycle; and</p> <p>(d) the potential consequences of an information security incident.</p>	<p>CI 6.1; CI 8.1; CI 8.2; CI 8.3</p>	<p>The organization shall define and apply an information security risk treatment process to:</p> <p>a) select appropriate information security risk treatment options, taking account of the risk assessment results;</p> <p>b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen. Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.</p>	<p>Annex A ; A.8.1 (Asset Management) ; A.8.2 (Information classification w.r.t value & criticality); A.16 (IS Incident Management)</p>	<p>The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.</p>
<p>Where information assets are managed by a related party or third party, an APRA-regulated entity must evaluate the design and operating effectiveness of that party's information security controls.</p>	<p>CI 9.1; CI 9.3</p>	<p>The organization shall evaluate the information security performance and the effectiveness of the information security management system. Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.</p>	<p>A. 15.1.1; A.15.1.2; A.15.1.3 ; A.15.2.1</p>	<p>Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be</p>

Incident management

An APRA-regulated entity must

<p>An APRA-regulated entity's information security response plans must include the mechanisms in place for:</p> <p>(a) managing all relevant stages of an incident, from detection to post-incident review; and</p> <p>(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.</p>	<p>CI 9.1; CI 10.1</p>	<p>The organization shall evaluate the information security performance and the effectiveness of the information security management system.</p>	<p>A.16.1.5; A.16.1.6; A.17.1.2</p>	<p>Information security incidents shall be responded to in accordance with the documented procedures. Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.</p>
<p>An APRA-regulated entity must annually confirm that its information security response plans are effective.</p>	<p>CI 9.3; CI 10.1</p>	<p>The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.</p>	<p>A.17.1.1; A.17.1.3</p>	<p>The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse.</p>



managed, taking account of the
criticality of business information,

<p>An APRA-regulated entity must review the sufficiency of the testing program at least annually or on material change to information assets or the business environment.</p>	<p>CI 8.1</p>	<p>The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.</p>	<p>A.18.1.2</p>	<p>The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes.</p>
---	---------------	---	-----------------	---

Internal Audits

<p>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).</p>	<p>CI 9.2</p>	<p>The organization shall conduct internal audits at planned intervals. The organization shall:</p> <p>c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;</p>	<p>A.18.1.1; A.18.1.2; A.18.2.1</p>	<p>All relevant legislative, statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.</p>
---	---------------	--	---	--

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).

CI 7.1; CI 7.2 ; CI 9.2

The organization shall:
e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

A.12

Where information assets are managed by a related party or third party, internal audit must assess the information security control assurance provided by that party, where an information security incident affecting those information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.

CI 9.2

The organization shall:

c) plan and