Draft Prudential Standard CPS 234 & ISO/IEC 27001

APRA CPS 234 Requirement	ISO 27001:2013 Requirement	Requirement Overview	ISO 27001:2013 Annex A Reference Control	Control Overview
Objectives and key requirements				
Clearly define the information security related roles and responsibilities of the Board, and of senior management, governing bodies and individuals;	Cl 5.1 ; Cl 5.3	Top management shall demonstrate leadership and commitment with respect to the information security management system. Management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	A.6.1.1	All IS roles & responsibilities shall be defined and allocated.
Maintain 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;	Cl 6.1; Cl 6.2 ; Cl 8.1	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.	A.8.1.1;A.12.6.1	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. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

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	Cl 8.1; Cl 8.2; Cl 8.3	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.	A.8.1.1 ; A.8.1.2; A.8.1.3; A.8.1.4	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. Assets maintained in the inventory shall be owned. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
Notify APRA of material information security incidents.	Cl 10.1; Cl 10.2	When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences.	A.16.1.1 ; A.16.1.2; A.16.1.3	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.

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).	Cl 4.4 ; Cl 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.	Cl 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 decided if they are to be classified as information security incidents. Information security incidents shall be responded to in accordance with the documented procedures. The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

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.	Cl 8.1 ; Cl 8.2	The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur,	A.15.2.2; A.18.2.1	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. 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.

Policy framework

An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.	Cl 5.2	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	A.9.1.1; A.9.4.1; A.10.1.2	An access control policy shall be established, documented and reviewed based on business and information security requirements. Access to information and application system functions shall be restricted in accordance with the access control policy. A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

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.	Cl 5.1 , 5.2, 5.3	The information security policy shall: e) be available as documented information; f) be communicated within the organization; and g) be available to interested parties, as appropriate.	A.14.2.1; A.15.1.1	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.

Information asset identification and classification

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.	Cl 6.1, 8.1,8.2	The organization shall define and apply an information security risk assessment process that: c) identifies the information security risks: 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;	A.8.1.1;A.8.1.3; A.8.2.1;A.8.2.2	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.

Implementation of controls				
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; and (d) the potential consequences of an information security incident.	Cl 6.1; Cl 8.1; Cl 8.2; Cl 8.3	The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; 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.	Annex A ; A.8.1 (Asset Management) ; A.8.2 (Information classification w.r.t value & criticality); A.16 (IS Incident Management)	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.
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.	Cl 9.1; Cl 9.3	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.	A. 15.1.1; A.15.1.2; A.15.1.3 ; A.15.2.1	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. All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. Organizations shall regularly monitor, review and audit supplier service delivery.

Incident management

An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.	Cl 9.3; Cl 10.1; Cl 10.2	When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences;	A.16.1.1; A.16.1.2; A.16.1.3	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.
An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).	Cl 6.1; Cl 8.1	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 The organization shall implement the information security risk treatment plan.	A.16.1.5; A.16.1.6; A.17.1.2	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.

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 (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.	Cl 9.1; Cl 10.1	The organization shall evaluate the information security performance and the effectiveness of the information security management system.	A.16.1.5; A.16.1.6; A.17.1.2	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.
An APRA-regulated entity must annually confirm that its information security response plans are effective.	Cl 9.3; Cl 10.1	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.	A.17.1.1; A.17.1.3	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.

Testing control effectiveness

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: (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; and (d) the risks associated with exposure to untrusted environments, where an entity's ability to enforce its information security policy is impeded.	Cl 6.1; Cl 8.1	The organization shall plan actions to address these risks and opportunities; and how to: 1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	A.18.2.1; A.18.2.2; A.18.2.3	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. Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.
Where 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, an entity must assess whether that testing is commensurate with paragraph 26 (a)-(d)	Cl 6.1; Cl 8.1	The organization shall define and apply an information security risk treatment process to: determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE :Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;	A.15.1.1; A.15.1.3; A.15.2.2	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. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

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, to enable an assessment and potential response by the Board or senior management to mitigate the exposure, as appropriate.	Cl 9.3 ; Cl 10.1	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.	A.18.2.1; A.18.2.2; A.18.2.3	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes. Information security events shall be reported through appropriate management channels as quickly as possible.
Testing must be conducted by appropriately skilled and functionally independent specialists.	Cl 7.1; Cl 7.2	The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	A.18.1.2	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.

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.	Cl 8.1	The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	A.18.1.2	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.

Internal Audits

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).	Cl 9.2	The organization shall conduct internal audits at planned intervals. The organization shall: 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;	A.18.1.1; A.18.1.2; A.18.2.1	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.

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).	Cl 7.1; Cl 7.2 ; Cl 9.2	The organization shall: e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	A.12.7.1	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.
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.	Cl 9.2	The organization shall: 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; d) define the audit criteria and scope for each audit; f) ensure that the results of the audits are reported to relevant management; and g) retain documented information as evidence of the audit programme(s) and the audit results.	A.15.1.1; A.15.1.3; A.15.2.1; A.18.1.3; A.18.1.4	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. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. Organizations shall regularly monitor, review and audit supplier service delivery. Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.