Prudential Standard CPS 232 and ISO 22301:2019

APRA CPS 232 Paragraph	APRA CPS 232 Requirement	ISO 22301:2019 Requirement	Requirement overview
Objectives and key requirements			
	Maintain a business continuity management policy for the institution or group, approved by the Board;	Cl 5.2.1	Top management shall establish a business continuity policy that: a) is appropriate to the purpose of the organization; b) provides a framework for setting business continuity objectives; c) includes a commitment to satisfy applicable requirements; d) includes a commitment to continual improvement of the BCMS.
	Identify, assess and manage potential business continuity risks to ensure that it is able to meet its financial and service obligations to its depositors, policyholders and other stakeholders;	Cl 8.2.3	The organization shall implement and maintain a risk assessment process. NOTE The process for risk assessment is addressed in ISO 31000. The organization shall: a) identify the risks of disruption to the organization's prioritized activities and to their required resources; b) analyse and evaluate the identified risks; c) determine which risks require treatment.
	Consider business continuity risks and controls as part of its risk management framework;	Cl 8.2.1	The organization shall: a) implement and maintain systematic processes for analysing the business impact and assessing the risks of disruption; b) review the business impact analysis and risk assessment at planned intervals and when there are significant changes within the organization or the context in which it operates.

	Maintain a business continuity plan that documents procedures and information which enable the institution to manage business disruptions;	Cl 8.4.4	The organization shall document and maintain business continuity plans and procedures. The business continuity plans shall provide guidance and information to assist teams to respond to a disruption and to assist the organization with response and recovery.
	Review the business continuity plan annually and periodically arrange for its review by the internal audit function or an appropriate external expert; and	Cl 8.6	The organization shall: a) evaluate the suitability, adequacy and effectiveness of its business impact analysis, risk assessment, strategies, solutions, plans and procedures; b) undertake evaluations through reviews, analysis, exercises, tests, post-incident reports and performance evaluations; c) conduct evaluations of the business continuity capabilities of relevant partners and suppliers; d) evaluate compliance with applicable legal and regulatory requirements, industry best practices, and conformity with its own business continuity policy and objectives; e) update documentation and procedures in a timely manner. These evaluations shall be conducted at planned intervals, after an incident or activation, and when significant changes occur. These evaluations shall be conducted at planned intervals, after an incident or activation, and when significant changes occur.
	Notify APRA in the event of certain disruptions.	Cl 8.4.3.1	The organization shall document and maintain procedures for: a) communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate; NOTE The organization can document and maintain procedures for how, and under what circumstances, the organization communicates with employees and their emergency contacts. b) receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent; c) ensuring the availability of the means of communication during a disruption; d) facilitating structured communication with emergency responders;

			e) providing details of the organization's media response following an incident, including a communications strategy; f) recording the details of the disruption, the actions taken and the decisions made.
		Cl 8.4.3.2	Where applicable, the following shall also be considered and implemented: a) alerting interested parties potentially impacted by an actual or impending disruption; b) ensuring appropriate coordination and communication between multiple responding organizations. The warning and communication procedures shall be exercised as part of the organization's exercise programme described in 8.5.

Business continuity management

20	BCM is a whole-of-business approach that includes policies, standards and procedures for ensuring that critical business operations can be maintained or recovered in a timely fashion, in the event of a disruption. Its purpose is to minimise the financial, legal, regulatory, reputational and other material consequences arising from a disruption.	Cl 1.0 and Cl 4	The standard specifies the structure and requirements for implementing and maintaining a business continuity management system (BCMS) that develops business continuity appropriate to the amount and type of impact that the organization may or may not accept following a disruption. The outcomes of maintaining a BCMS are shaped by the organization's legal, regulatory, organizational and industry requirements, products and services provided, processes employed, size and structure of the organization, and the requirements of its interested parties. A BCMS emphasizes the importance of: — understanding the organization's needs and the necessity for establishing business continuity policies and objectives;

		Cl 4.2.2	— operating and maintaining processes, capabilities and response structures for ensuring the organization will survive disruptions; — monitoring and reviewing the performance and effectiveness of the BCMS; — continual improvement based on qualitative and quantitative measures. A BCMS, like any other management system, includes the following components: a) a policy; b) competent people with defined responsibilities; c) management processes relating to: 1) policy; 2) planning; 3) implementation and operation; 4) performance assessment; 5) management review; 6) continual improvement; d) documented information supporting operational control and enabling performance evaluation. The organization shall: a) implement and maintain a process to identify, have access to, and assess the applicable legal and regulatory requirements related to the continuity of its products and services, activities and resources; b) ensure that these applicable legal, regulatory and other requirements are taken into account in implementing and maintaining its BCMS; c) document this information and keep it up to date.

21	Critical business operations are the business functions, resources and infrastructure that may, if disrupted, have a material impact on the institution's business functions, reputation, profitability, depositors and/or policyholders.	Cl 8.2.2	The organization shall use the process for analysing business impacts to determine business continuity priorities and requirements. The process shall: a) define the impact types and criteria relevant to the organization's context; b) identify the activities that support the provision of products and services.
22	BCM must, at a minimum, include: a) a BCM policy in accordance with paragraphs 23 to 25; b) a business impact analysis (BIA) including risk assessment in accordance with paragraphs 26 and 27; c) recovery objectives and strategies; in accordance with paragraphs 28 and 29; d) a BCP in accordance with paragraphs 30 to 33; and e) programs for: (i) review and testing of the BCP in accordance with paragraphs 34 and 35; and (ii) training and ensuring awareness of staff in relation to BCM.	Cl 4.4	The organization shall establish, implement, maintain and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of this document.

Business continuity management policy

23	The Board must approve the institution's BCM policy.	Cl 5.1	Top management shall demonstrate leadership and commitment with respect to the BCMS by: a) ensuring that the business continuity policy and business continuity objectives are established and are compatible with the strategic direction of the organization.

		Cl 5.2.1	Top management shall establish a business continuity policy that: a) is appropriate to the purpose of the organization; b) provides a framework for setting business continuity objectives; c) includes a commitment to satisfy applicable requirements; d) includes a commitment to continual improvement of the BCMS.
24	The BCM policy must be up-to-date, documented and must set out the objectives and approach in relation to BCM.	Cl 5.2.2	The business continuity policy shall: a) be available as documented information; b) be communicated within the organization; c) be available to interested parties, as appropriate.
25	The BCM policy must clearly state the roles, responsibilities and authorities to act in relation to the BCM policy.	Cl 5.3	Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization. Top management shall assign the responsibility and authority for: a) ensuring that the BCMS conforms to the requirements of this document; b) reporting on the performance of the BCMS to top management.

Business impact analysis

26	A BIA involves identifying all critical business functions, resources and infrastructure of the institution and assessing the impact of a disruption on these.	Cl 8.2.2	The organization shall use the process for analysing business impacts to determine business continuity priorities and requirements. The process shall: a) define the impact types and criteria relevant to the organization's context; b) identify the activities that support the provision of products and services; c) use the impact types and criteria for assessing the impacts over time resulting from the disruption of these activities;

27	When conducting the BIA, the APRA-regulated institution must consider: a) plausible disruption scenarios over varying periods of time; b) the period of time for which the institution could not operate without each of its critical business operations; c) the extent to which a disruption to the critical business operations might have a material impact on the interests of depositors and/or policyholders of the institution; and d) the financial, legal, regulatory and reputational impact of a disruption to the institution's critical business operations over varying periods of time.		d) identify the time frame within which the impacts of not resuming activities would become unacceptable to the organization; NOTE 1 This time frame can be referred to as the "maximum tolerable period of disruption (MTPD)". e) set prioritized time frames within the time identified in d) for resuming disrupted activities at a specified minimum acceptable capacity; NOTE 2 This time frame can be referred to as the "recovery time objective (RTO)". f) use this analysis to identify prioritized activities; g) determine which resources are needed to support prioritized activities; h) determine the dependencies, including partners and suppliers, and interdependencies of prioritized activities.
		Cl 8.2.3	The organization shall implement and maintain a risk assessment process. The organization shall: a) identify the risks of disruption to the organization's prioritized activities and to their required resources; b) analyse and evaluate the identified risks; c) determine which risks require treatment.

Recovery objectives and strategies

28	Recovery objectives are pre-defined goals for recovering critical business operations to a specified level of service (recovery level) within a defined period (recovery time) following a disruption.	Cl 8.2.2 d) and e)	d) identify the time frame within which the impacts of not resuming activities would become unacceptable to the organization; NOTE 1 This time frame can be referred to as the "maximum tolerable period of disruption (MTPD)". e) set prioritized time frames within the time identified in d) for resuming disrupted activities at a specified minimum acceptable capacity; NOTE 2 This time frame can be referred to as the "recovery time objective (RTO)".

29	An APRA-regulated institution must identify and document appropriate recovery objectives and implementation strategies based on the results of the BIA and the size and complexity of the institution.	Cl 8.4.5	The organization shall have documented processes to restore and return business activities from the temporary measures adopted during and after a disruption.

Business continuity planning

30	An APRA-regulated institution must maintain at all times a documented BCP for the institution that meets the objectives of the institution's BCM policy.	Cl 8.4.1	The organization shall implement and maintain a response structure that will enable timely warning and communication to relevant interested parties. It shall provide plans and procedures to manage the organization during a disruption. The plans and procedures shall be used when required to activate business continuity solutions. NOTE There are different types of procedures that comprise business continuity plans. The organization shall identify and document business continuity plans and procedures based on the output of the selected strategies and solutions. The procedures shall: a) be specific regarding the immediate steps that are to be taken during a disruption; b) be flexible to respond to the changing internal and external conditions of a disruption; c) focus on the impact of incidents that potentially lead to disruption; d) be effective in minimizing the impact through the implementation of appropriate solutions; e) assign roles and responsibilities for tasks within them.
31	The BCP must document procedures and information that enable the institution to: a) manage an initial business disruption (crisis management); and b) recover critical business operations.	Cl 8.4.4.1	The organization shall document and maintain business continuity plans and procedures. The business continuity plans shall provide guidance and information to assist teams to respond to a disruption and to assist the organization with response and recovery.

32	The BCP must document procedures and information that enable the institution to: a) manage an initial business disruption (crisis management); and b) recover critical business operations. c) recovery strategies for each critical business operation; d) infrastructure and resources required to implement the BCP; e) roles, responsibilities and authorities to act in relation to the BCP; and f) communication plans with staff and external stakeholders.	Cl 8.4.4.2	Collectively, the business continuity plans shall contain: a) details of the actions that the teams will take in order to: 1) continue or recover prioritized activities within predetermined time frames; 2) monitor the impact of the disruption and the organisation's response to it; b) reference to the pre-defined threshold(s) and process for activating the response; c) procedures to enable the delivery of products and services at agreed capacity; d) details to manage the immediate consequences of a disruption giving due regard to: 1) the welfare of individuals; 2) the prevention of further loss or unavailability of prioritized activities; 3) the impact on the environment.
		Cl 8.4.4.3	Each plan shall include: a) the purpose, scope and objectives; b) the roles and responsibilities of the team that will implement the plan; c) actions to implement the solutions; d) supporting information needed to activate (including activation criteria), operate, coordinate and communicate the team's actions; e) internal and external interdependencies; f) the resource requirements; g) the reporting requirements; h) a process for standing down. Each plan shall be usable and available at the time and place at which it is required.

33	Where material business activities are outsourced, an APRA-regulated institution must satisfy itself as to the adequacy of the outsourced service provider's BCP and must consider any dependencies between the two BCPs.	Cl 8.1 Cl 8.2.2 h)	The organization shall ensure that outsourced processes and the supply chain are controlled. The organization shall use the process for analysing business impacts to determine business continuity priorities and requirements. The process shall determine the dependencies, including partners and suppliers, and interdependencies of prioritized activities.

Review and testing of business continiuity plan

35	An APRA-regulated institution must review and test the institution's BCP at least annually, or more frequently if there are material changes to business operations, to ensure that the BCP can meet the BCM objectives. The results of the testing must be formally reported to the Board or to delegated management.	Cl 8.6	The organization shall implement and maintain a programme of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions. The organization shall conduct exercises and tests that: a) are consistent with its business continuity objectives; b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives; c) develop teamwork, competence, confidence and knowledge for those who have roles to perform in relation to disruptions; d) taken together over time, validate its business continuity strategies and solutions; e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements; f) are reviewed within the context of promoting continual improvement; g) are performed at planned intervals and when there are significant changes within the organization or the context in which it operates. The organization shall act on the results of its exercising and testing to implement changes and improvements. 8.6 Evaluation of business continuity documentation and capabilities
36	The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 34.		

		Cl 8.6	The organization shall: a) evaluate the suitability, adequacy and effectiveness of its business impact analysis, risk assessment, strategies, solutions, plans and procedures; b) undertake evaluations through reviews, analysis, exercises, tests, post-incident reports and performance evaluations; c) conduct evaluations of the business continuity capabilities of relevant partners and suppliers; d) evaluate compliance with applicable legal and regulatory requirements, industry best practices, and conformity with its own business continuity policy and objectives; e) update documentation and procedures in a timely manner. These evaluations shall be conducted at planned intervals, after an incident or activation, and when significant changes occur.

Notification requirements

36	An APRA-regulated institution must notify APRA as soon as possible and no later than 24 hours after the institution experiences a major disruption that has the potential to have a material impact on the institution's risk profile, or affect its financial soundness. The APRA-regulated institution must explain to APRA the nature of the disruption, the action being taken, the likely effect and the timeframe for returning to normal operations. The APRA-regulated institution must notify APRA when normal operations resume.	Cl 7.4	The organization shall determine the internal and external communications relevant to the BCMS, including: a) on what it will communicate; b) when to communicate; c) with whom to communicate; d) how to communicate; e) who will communicate.

37	The information or notifications required by this Prudential Standard must be given in such form, if any, and by such procedures, if any, as APRA determines and publishes on its website from time to time.		

Internal audit

38	An institution's internal audit function, or an appropriate external expert, must periodically review the BCP and provide an assurance to the Board or to delegated management that: (a) the BCP is in accordance with the institution's BCM policy and addresses the risks it is designed to control; and (b) testing procedures are adequate and have been conducted satisfactorily.	Cl 9.2.1	The organization shall conduct internal audits at planned intervals to provide information on whether the BCMS: a) conforms to: 1) the organization's own requirements for its BCMS; 2) the requirements of this document; b) is effectively implemented and maintained.