APRA CPS 232 Paragraph	APRA CPS 232 Requirement	ISO 22301:2019 Requirement	Requirement overview
	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;

			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.

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 ýnancial, legal, regulatory, reputational and other material consequences arising from a disruption.	Cl 1.0 and Cl 4	The standard speciýes 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 e ectiveness 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 deýned 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.

23	The Board must approve the institution's

		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.

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) deýne 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 tof Ce prf C00530equir

28	Recovery objectives are pre-deýned goals for recovering critical business operations to a speciýed level of service (recovery level) within a deýned 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 identiýed in d) for resuming disrupted activities at a speciýed minimum acceptable capacity; NOTE 2 This time frame can be referred to as the

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.
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 e ectiveness 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 deýned aims and objectives; c) develop teamwork, competence, conýdence 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 signiýcant 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 identiýed as a result of the review and testing required under paragraph 34.		

		Cl 8.6	The organization shall: a) evaluate the suitability, adequacy and e ectiveness 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 signiýcant 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 institutionîs risk proýle, or a ect its ýnancial soundness. The APRA-regulated institution must explain to APRA the nature of the disruption, the action being taken, the likely e ect 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 notiýcations 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.		

Audit arrangement

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) th(1B00440052C05100491 10.6 6.1 6300EE4003004560