

DRAFT

# Prudential Standard XPS XXX

## Business Continuity Management for [Insert Specific Institution]

### Objective and Key Requirements of this Standard

This Prudential Standard aims to ensure that an [institution – this would be specified as an ADI, insurer or life company] implements a whole of business approach to business continuity management ('BCM') appropriate to the nature and scale of its operations. BCM increases an [institution's] resilience to business disruption arising from internal and external events and reduces the impact on the [institution's] business operations, reputation or profitability, its [depositors/policyholders] and other stakeholders.

The prime responsibility for the business continuity of the [institution] rests with the Board of that [institution], or with the Country Head in Australia for a foreign branch [ADI] or foreign GI.

The key requirements of this Prudential Standard are:

- the Board and senior management of the [institution] or, in the case of a foreign branch [ADI] or foreign GI the Country Head in Australia, must consider the [institution's] business continuity risks and controls as part of its overall risk management framework and to this end must attest to a formal policy covering BCM arrangements in the risk management declaration provided to APRA on an annual basis;
- each [institution] must identify, on a whole of business basis, critical business functions, resources and infrastructure that would have a material impact if subject to disruption. The Board must establish thresholds for assessing materiality;
- each [institution] must assess the impact of plausible disruption scenarios on all critical business functions, resources and infrastructure, and have in place appropriate recovery strategies to ensure that all appropriate resources are readily available to withstand the impact of the disruption;
- each [institution] must develop, implement and maintain a Business Continuity Plan ('BCP') that documents procedures and information which enable the institution to respond to disruptions, recover critical business functions and return to normal operations in an orderly manner. The BCP must be reviewed at least annually by senior management and periodically

**DRAFT**

reviewed by the [institution's] internal audit function or an external expert; and

- an [institution] must notify APRA as soon as possible and no later than 24 hours after experiencing a major disruption that has the potential to materially impact [depositors/policyholders].

Details on these requirements are contained below, and in Guidance Note XGN XXX.1 which forms part of this Standard.

The requirements relating to annual risk management declarations are contained in XPS XXX [this will be tailored for each industry – APS 310 for ADI's, GPS 220 for GIs]. Additional requirements relating to Outsourcing are set out in *XPS XXX Outsourcing*.

**DRAFT****Prudential Standard**

1. This Prudential Standard, made under section X of the *X Act 19XX* ('the Act'), applies to all [institutions] [authorised/registered] under the Act.

**Business Continuity Management**

2. Business Continuity Management ('BCM') describes a whole of business approach to ensure critical business functions can be maintained, or restored in a timely fashion, in the event of material disruptions arising from internal or external events. Its purpose is to minimise the financial, legal, reputational and other consequences arising from the disruption.
3. To this end, APRA requires [institutions] to identify, assess and manage potential business continuity risks to ensure the [institution] is able to meet its financial and service obligations to its [depositors/policyholders] and other creditors.
4. BCM involves an integrated process of Risk assessment (see paragraph 14), Business Impact Analysis (see paragraphs 15 to 19), Recovery strategy (see paragraphs 20 to 22), Business Continuity Plan (see paragraphs 23 to 28), and Crisis management (see paragraph 29).
5. BCM should also be considered in the preliminary planning phase for new business acquisitions, joint ventures, outsourcing arrangements and major projects involving the introduction of new business processes and systems.

**The role of the board and senior management**

6. The Board, or in the case of a [foreign branch [ADI], or foreign GI], the Country Head in Australia, is ultimately responsible for the business continuity of the [institution].
7. The Board or Country Head may delegate operational responsibility for BCM to a responsible committee ('the Committee') and/or senior management of the [institution]. The operational responsibility must be clearly expressed in the charter of the responsible committee and in the performance objectives of senior management.
8. Senior management must similarly establish clear lines of accountability and reporting for individuals with BCM responsibility.
9. Procedures must be in place to ensure that all business units are fully aware of, and comply with, the BCM policy.

**DRAFT**

10. In larger institutions, consideration should also be given to establishing a centralised business continuity function to ensure that common standards and practices are in place across the institution.

**Materiality**

11. This standard is applicable on a whole of business basis to critical business functions, resources and infrastructure that would have a material impact if subject to disruption.
12. The thresholds of what constitutes materiality must be set by the Board or Country Head of an [institution]. The assessment of what constitutes a material business activity or a material support function is often a subjective one and depends on the circumstances faced by individual institutions. Generally, however, a material activity or function is defined as one that has the potential, if disrupted, to impact significantly on the [institution's] business operations, reputation or profitability.
13. Factors that APRA would expect to be considered by the Board when making this assessment include:
  - (a) the extent to which the interests of [depositors/policyholders] may be adversely impacted by disruption to the normal services and operations of the institution;
  - (b) the financial and reputational impact of a failure of the [institution] to perform over a given period of time (depending on the importance of the business activity, this may be measured in hours);
  - (c) the revenue lost as a share of total revenue;
  - (d) the degree of difficulty, including the time taken, in restoring the business activity or support function or implementing alternate arrangements; and
  - (e) the ability of the [institution] to meet regulatory requirements if there were business continuity problems.

**Risk assessment**

14. [Institutions] must identify plausible disruption scenarios that may lead to short, medium and long-term disruptions to critical business functions and assess the likelihood of these scenarios occurring.

**Business Impact Analysis**

15. A Business Impact Analysis ('BIA') involves identifying all critical business functions, resources and infrastructure of the [institution] and

**DRAFT**

assessing the impact of a disruption on these. Suggested issues to be considered in assessing plausible disruption scenarios are contained in XGN XXX.1.

16. To this end, an [institution] must determine the potential financial, legal, reputational and other consequences if the critical business functions, resources and infrastructure are unavailable for a given period of time.
17. The maximum acceptable downtime during which the institution could not operate without its critical business functions, resources and infrastructure must be determined. The priority and timeframes assigned for the recovery of critical business functions, resources and infrastructure must be determined.
18. The BIA must cover all business units of the [institution], including operations located interstate and offshore, those subsidiary companies providing specialist services to the institution and arrangements with service providers to ensure a whole of business coverage.
19. Senior management should ensure that there is adequate representation and involvement from all business units when undertaking the BIA. The BIA must be validated by senior management.

**Recovery strategy**

20. An [institution] must consider appropriate recovery strategies based on the results of the BIA. These strategies should be subjected to cost/benefit analysis.
21. Senior management should approve the resources needed to implement the agreed strategy and ensure sufficient budgetary and other resources are allocated to allow implementation of the strategy.
22. While it is desirable for an [institution] to have insurance arrangements in place to cover some of the costs of business disruption, this is not in itself a substitute for a comprehensive BCM framework.

**Business Continuity Plan**

23. Each [institution] must maintain at all times a written Business Continuity Plan ('BCP') approved by the Board (or in the case of a foreign branch [ADI] or foreign GI, the Country Head in Australia).
24. The BCP refers to the documented procedures and information which enable the [institution] to respond to a disruption, recover and resume critical business functions and return to normal operations in an orderly manner.

**DRAFT**

25. The BCP must cover all business units, critical business functions, resources and infrastructure of the [institution], including operations located interstate and offshore, those subsidiary companies providing specialist services to the [institution] and arrangements with service providers, to ensure a whole of business coverage.
26. At a minimum, a BCP must contain:
  - (a) the procedures to be followed in response to a material disruption to normal business operations. The procedures should enable the [institution] to manage the initial crisis, and recover and resume the critical business functions, resources and infrastructure outlined in the BCP within the nominated timeframe;
  - (b) detailed procedures for restoring normal business operations. This should include the orderly entry of all business transactions and records into the relevant IT systems and the completion of all verification and reconciliation procedures;
  - (c) a list of all resources needed to run operations in the event the primary operational site is unavailable. This would include, but is not limited to, computer hardware and software, printers, faxes, telephones, standard stationery and forms. Additional resources include suitably trained staff and relevant documentation such as insurance policies and contracts;
  - (d) a communication plan for notifying key internal and external stakeholders if the [institution's] BCP is invoked. Further detail on communication plans is contained in XGN XXX.1;
  - (e) consideration of business continuity as part of any proposed material outsourcing agreement with a third party service provider. Further detail on outsourcing is contained in XGN XXX.1. [Institutions] should refer to XPS 231 for additional requirements regarding outsourcing arrangements; and
  - (f) relevant information about an [institution's] alternate site for the recovery of business and/or IT operations if this forms part of the [institution's] BCP. An alternate site refers to a site used for the resumption of critical business functions. Further detail on alternate sites is contained in XGN XXX.1.
27. A consistent method of documenting the BCP should be implemented throughout the [institution]. Detailed input into the BCP should occur at the business unit level.

**DRAFT**

28. Off-site copies of the BCP must be kept by a number of responsible managers who have designated responsibilities in terms of the BCP and should also be available at the alternate recovery site if applicable. Further detail on issues to be taken into account when using an alternate site is contained in XGN XXX.1.

**Crisis management**

29. The composition and responsibilities of the crisis management team or other group that has the authority to invoke the BCP must be clearly identified in the BCP. This would include, but is not limited to, an assessment of the impact of the disruption, determining the appropriate response, implementing the communications plan, evacuating staff and activating the alternate recovery site(s) if required.

**Review and testing of the BCP**

30. The [institution's] BCP must be reviewed by senior management on a regular basis (but at least annually or more frequently if there are material changes to business operations).
31. The [institution's] internal audit function, or an external expert, must also periodically review the BCP and provide an assurance to the Board or responsible Committee that the BCP is in accordance with the [institution's] formal policy (see paragraphs 37 to 39), addresses the risks it is designed to control and that testing procedures are adequate and have been conducted satisfactorily.
32. An [institution] must thoroughly test its BCP on a regular basis (but at least annually or more frequently if there are material changes to business operations) to ensure that the BCP is capable of meeting its objectives.
33. The results of the testing must be formally reported to senior management and the Board or its responsible Committee. The BCP must be amended to reflect any enhancements as a result of the tests. Further detail on testing is contained in XGN XXX.1.

**Accountability and application**

34. While some [institutions] may rely upon third party service providers for components of their BCP, accountability for BCM remains with the [institution]. It is important for [institutions] to recognise that while outsourcing can be of significant benefit and may in fact reduce some risks, it may also give rise to other risks (refer to XPS 231 Outsourcing).
35. In large conglomerates, where a central service model is employed to provide specialist services, the Board of an [institution] remains

**DRAFT**

responsible and must establish effective oversight and management reporting arrangements.

36. In other cases, [institutions] may be involved in joint ventures, strategic alliances or partnering arrangements that perform the BCP activities. This standard applies regardless of whether activities are outsourced to related or third party service providers. However, APRA will be flexible in applying the standard where the services are provided by another APRA-regulated [institution] within the group. The standard also applies to arrangements where the service provider is located outside Australia, or the functions are performed outside Australia.

**Formal BCM policy as part of risk management framework**

37. Business continuity risks arising from internal and external events should be an integrated component of the [institution's] risk management and control framework.
38. The Board and senior management of the [institution] must consider the [institution's] business continuity risks and controls as part of its overall risk management framework and to this end must attest to a formal policy covering BCM arrangements in the risk management declaration provided to APRA on an annual basis. The BCM policy should be summarised in the Risk Management System Description [ADI] or Risk Management Strategy [GI]. [This will be tailored to each industry].
39. This policy should set out at a minimum, the [institution's] BCM objectives, accountability and reporting responsibilities of individuals, and testing and training requirements.

**Notification requirements**

40. An [institution] must notify APRA as soon as possible and no later than 24 hours after experiencing a major disruption that has the potential to materially impact [depositors / policyholders]. The [institution] should outline to APRA the nature of the disruption, the action being taken and the timeframe for return to normal. APRA must be notified when normal operations are resumed.
41. APRA may request additional information where it considers it necessary to do so in order to understand and assess the impact of the disruption on the [institution's] risk profile.

**DRAFT**

**External audit**

42. Where considered appropriate, APRA may request the external auditor of the [institution], or an appropriate external expert, to provide an assessment of the BCM arrangements within the [institution] or in respect of a third party service provider. Such reports will be paid for by the [institution] and would be made available to APRA.

**Transitional arrangements**

43. This standard comes into immediate effect. Regulated institutions must report on compliance with the Standard in their next annual risk management declaration [refer to APS 310 ADI's, GPS 220 for GI's]. Details of any areas of non compliance must be reported to APRA along with an action plan for rectification.