



Prudential Standard GPS 222

Business Continuity Management

Objective and key requirements of this Prudential Standard

This Prudential Standard aims to ensure that a general insurer (**insurer**) implements a whole of business approach to business continuity management (**BCM**) appropriate to the nature and scale of its operations. BCM increases an insurer's resilience to business disruption arising from internal and external events and reduces the impact on the insurer's business operations, reputation, profitability, policyholders and other stakeholders.

The prime responsibility for the business continuity of the insurer rests with the Board of Directors (**the Board**) of the insurer, or in the case of a foreign general insurer, the senior officer outside Australia with delegated authority from the Board.

The key requirements of this Prudential Standard are:

- the Board and senior management of the insurer must consider the insurer's business continuity risks and controls as part of its overall risk management systems when completing the Board Declaration provided to APRA on an annual basis;
- an insurer must identify, on a whole of business basis, critical business functions, resources and infrastructure which, if disrupted, would have a material impact;
- an insurer 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 necessary resources are readily available to withstand the impact of the disruption;
- an insurer must develop, implement and maintain a Business Continuity Plan (**BCP**) that documents procedures and information which enable the insurer to respond to disruptions and recover critical business functions. The BCP must be reviewed at least annually by responsible senior management and periodically reviewed through the insurer's internal audit function or an external expert; and
- an insurer 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 policyholders.

Authority and application

1. This Prudential Standard, made under section 32 of the *Insurance Act 1973* (**the Act**), applies to all general insurers (**insurers**).
2. *Guidance Note GGN 222.1 Risk Assessment and Business Continuity Management* (GGN 222.1 Risk Assessment and Business Continuity Management) forms part of this Prudential Standard.
3. Requirements relating to an insurer's risk management systems, annual Board Declaration and outsourcing are contained in *Prudential Standard GPS 220 Risk Management for General Insurers* (GPS 220 Risk Management for General Insurers).

Business continuity management

4. 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 material consequences arising from the disruption.
5. To this end, APRA requires all insurers to identify, assess and manage potential business continuity risks to ensure each insurer is able to meet its financial and service obligations to its policyholders and other creditors.
6. BCM involves an integrated process of:
 - (a) risk assessment;
 - (b) business impact analysis;
 - (c) consideration of recovery strategies;
 - (d) business continuity planning;
 - (e) establishing business continuity/crisis management teams; and
 - (f) review and testing.
7. BCM should also be part of the planning phase for new business acquisitions, joint ventures, material outsourcing arrangements and major projects involving the introduction of new business processes and systems.

The role of the Board and senior management

8. The Board of Directors (**the Board**), or in the case of a foreign branch, the senior officer outside Australia with delegated authority from the Board,¹ is ultimately responsible for the business continuity of the insurer.
9. The Board may delegate operational responsibility for BCM to a responsible committee (**the Committee**) and/or senior management of the insurer. The operational responsibility must be clearly expressed in the charter of the Committee and in the performance objectives of responsible senior management.
10. Senior management must similarly establish clear lines of accountability and reporting for individuals with BCM responsibility.
11. In larger insurers, consideration should also be given to establishing a centralised business continuity function² to ensure that common standards and practices are in place across the insurer.

Critical business functions, resources and infrastructure

12. An insurer must identify, on a whole of business basis, its critical business functions, resources and infrastructure.
13. The assessment of criticality is often a subjective one and depends on the circumstances faced by individual insurers. In general, critical business functions, resources and infrastructure are defined as ones that have the potential, if disrupted, to impact materially on the insurer's business operations, reputation or profitability.

Risk assessment

14. Insurers 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. Suggested scenarios to be considered in the risk assessment are contained in GGN 222.1 Risk Assessment and Business Continuity Management.

Business impact analysis

15. A business impact analysis (**BIA**) involves identifying all critical business

¹ For the purposes of this Prudential Standard, a reference to the "Board" in the case of a foreign general insurer (foreign insurer) can be taken to be a reference to the senior officer outside Australia with delegated authority from the Board. *Prudential Standard GPS 510 Governance* will require a foreign insurer to nominate a person to be its senior officer outside Australia with delegated authority from the Board.

² Where a large insurer is part of a conglomerate, the conglomerate may develop processes which allow one centralised business continuity function to be used for the entire conglomerate provided this appropriately addresses any specific risks faced by individual APRA-regulated entities within the conglomerate.

functions, resources and infrastructure of the insurer and assessing the impact of a disruption on these.

16. To this end, an insurer must determine the potential financial, legal, reputational and other material consequences if the critical business functions, resources and infrastructure are unavailable.
17. Factors that APRA would expect to be considered by the insurer when making this determination include:
 - (a) the extent to which the interests of policyholders may be adversely impacted by disruption to the normal services and operations of the insurer;
 - (b) the financial and reputational impact of a failure of the insurer to perform over a given period of time;
 - (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 insurer to meet regulatory requirements if there were business continuity problems.
18. The period of time during which the insurer 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 also be determined.
19. The BIA³ process must cover all business units of the insurer, including operations located inter-state and offshore, those subsidiary companies providing specialist services to the insurer and arrangements with critical service providers, to ensure a whole of business coverage.
20. Senior management must ensure that there is adequate representation and involvement from all business units when undertaking the BIA process. The BIA process must be validated by senior management.

Recovery strategy

21. An insurer must consider appropriate recovery strategies based on the results of the BIA.
22. 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.

³ A reference to the BIA process can be individual or collective. It is acknowledged an insurer may have a number of BIA documents.

23. Insurers should have insurance arrangements in place to cover some of the costs of business disruption. However, this in itself is not considered a substitute for a comprehensive BCM framework.

Business continuity planning

24. Each insurer must maintain at all times a written Business Continuity Plan (BCP)⁴ approved by the Board or delegated representatives.
25. The BCP refers to the documented procedures and information which enable the insurer to respond to a disruption, recover and resume critical business functions. Consideration must also be given to the necessary requirements for return to normal operations. This may be treated as a distinct stage of the business continuity planning process.
26. The business continuity planning process must include all business units and cover all critical business functions, resources and infrastructure, including operations located inter-state and offshore, those subsidiary companies providing specialist services to the insurer and arrangements with critical service providers, to ensure a whole of business coverage.
27. The BCP should reflect the specific requirements of the insurer. 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 insurer to manage the initial business disruption, recover and resume the critical business functions, resources and infrastructure outlined in the BCP within the nominated timeframe;
 - (b) 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;
 - (c) a communication plan for notifying key internal and external stakeholders if the insurer's BCP is invoked. Further detail on communication plans is contained in GGN 222.1 Risk Assessment and Business Continuity Management;
 - (d) consideration of business continuity as part of any material outsourcing agreement with a critical third party service provider. Further detail on outsourcing is contained in GGN 222.1 Risk Assessment and Business Continuity Management. Insurer's should also refer to GPS 220 Risk Management for General Insurers for additional requirements regarding outsourcing arrangements; and

⁴ A reference to a BCP can be individual or collective. It is acknowledged an insurer may have a number of plans.

- (e) relevant information about an insurer's alternate site(s) for the recovery of business and/or IT operations if this forms part of the insurer'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 GGN 222.1 Risk Assessment and Business Continuity Management.
- 28. A consistent method of documenting the BCP should be implemented throughout the insurer. Detailed input into the BCP should occur at the business unit level.
- 29. 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 site(s) if applicable. Further detail on issues to be taken into account when using an alternate site is contained in GGN 222.1 Risk Assessment and Business Continuity Management.

Business continuity/crisis management team

- 30. The composition and responsibilities of the business continuity or crisis management team, or other group that has the authority to invoke the BCP or a separate Crisis Management Plan (**CMP**), must be clearly identified in the BCP and/or CMP. 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 site(s) if required.

Review and testing of the BCP

- 31. The insurer's BCP must be reviewed by responsible senior management at least annually or more frequently if there are material changes to business operations.
- 32. The insurer's internal audit function, or an external expert, must also periodically review the BCP and provide an assurance to the Board or the Committee that the BCP is in accordance with the insurer's formal policy (see paragraph 40), addresses the risks it is designed to control and that testing procedures are adequate and have been conducted satisfactorily.
- 33. An insurer must undertake a testing program of its BCP at least annually, or more frequently if there are material changes to business operations, to ensure the BCP is capable of meeting its objectives. Further detail on testing is contained in GGN 222.1 Risk Assessment and Business Continuity Management.
- 34. The results of the testing must be formally reported to responsible senior management and the Board or the Committee. The BCP must be amended to reflect any enhancements as a result of the tests.

Accountability and application

35. While some insurers may rely upon third party service providers for components of their BCP, accountability for the BCP remains with the insurer. It is important for insurers 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 GPS 220 Risk Management for General Insurers).
36. In large conglomerates, where a central service model is employed to provide specialist services, the Board of an insurer remains responsible for the BCP and must establish effective oversight and management reporting arrangements.
37. In other cases, insurers may be involved in joint ventures, strategic alliances or partnering arrangements that perform the BCP activities. This Prudential Standard applies regardless of whether activities are outsourced to related or third party service providers. However, APRA will be flexible in applying this Prudential Standard where the services are provided by another APRA-regulated entity within the group. This Prudential Standard also applies to arrangements where the service provider is located outside Australia, or the functions are performed outside Australia.

BCM as part of the risk management system

38. BCM should be an integrated component of the insurer's risk management and control systems.
39. The Board and responsible senior management of the insurer must consider the insurer's business continuity risks and controls as part of its overall risk management systems and when completing the Board Declaration provided to APRA on an annual basis as required by GPS 220 Risk Management for General Insurers.
40. An insurer must have a formal policy that sets out its approach to BCM. The policy should be summarised in the insurer's Risk Management Strategy as required by GPS 220 Risk Management for General Insurers.
41. Procedures must be in place to ensure that all business units are fully aware of, and comply with, the BCM policy.

Notification requirements

42. An insurer 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 policyholders. The insurer should outline to APRA the nature of the disruption, the action being taken and the timeframe for return to normal operations. APRA must be notified when normal operations are resumed.
43. 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 insurer's risk profile.

External audit

44. Where it considers it necessary, APRA may request the external auditor of the insurer, or an appropriate external expert, to provide an assessment of the BCM arrangements within the insurer or in respect of a critical service provider. Such reports will be paid for by the insurer and must be made available to APRA.

Transitional arrangements

45. A transitional period of 12 months applies from the date this Prudential Standard is determined. During this transitional period, all insurers must:
 - (a) report on their compliance with this Prudential Standard in their annual Board Declaration (as required under GPS 220 Risk Management for General Insurers); and
 - (b) submit to APRA a plan and timeframe for rectifying areas of non-compliance with this Prudential Standard.