Guidance Note GGN 222.1

Risk Assessment and Business Continuity Management

1. This Guidance Note provides further detail on matters general insurers (**insurers**) should consider when addressing the requirements contained in *Prudential Standard GPS 222 Business Continuity Management* (GPS 222 Business Continuity Management).

Risk assessment

2. The risk assessment should be undertaken at least annually and more frequently if there have been significant operational changes at the insurer or new or changed external factors that would alter the insurer's business continuity risk profile.

3. The worst case disruption scenario should be considered by an insurer and include, but not be limited to:

   (a) loss of precinct;

   (b) loss of building;

   (c) denial of access to building for a limited time;

   (d) loss of IT (data);

   (e) loss of IT (voice);

   (f) loss of vital (non-electronic) records;

   (g) loss of key staff (temporary or permanent); and

   (h) loss of key dependencies.

4. The critical interdependencies of the insurer's Business Continuity Plan (**BCP**) that are not within the direct control of the insurer should be identified and the associated risks assessed. This includes, but is not limited to, dependencies on utilities, third party service providers and key suppliers.

Communication plan

5. The communication plan[1] should incorporate a list of contact names and numbers, including, but not limited to, staff, regulators, customers, counterparties, service providers, market authorities and media. Out-of-hours numbers (including primary/alternate contacts) should be included for all staff with BCP responsibility. The contact list should be reviewed regularly to ensure it is up-to-date.

6. The communication plan should clearly identify the staff authorised to deal with the media if the BCP is invoked.

Outsourcing

7. Business continuity should be considered as part of any proposed material outsourcing agreement with a critical service provider. The insurer should conduct due diligence in this regard as part of the decision making process when assessing service providers.

8. The contract between the insurer and the critical service provider should include a requirement that the service provider have a BCP and testing program in place and provide for regular, and not less than annual, reporting to the insurer.

9. The insurer should recognise that outsourcing a business function does not transfer the associated business continuity risk to the service provider. The insurer should not place undue reliance on the service provider's BCP and should consider alternative contingency arrangements in the event that the service provider is unable to provide the agreed services. This is particularly important where there is no capability of bringing the outsourced business function back in-house (in either the short or medium term), or where an arrangement with an alternative service provider could not be implemented within an acceptably short time period.

10. The insurer's BCP should consider the operational links and interdependencies with the critical service provider's BCP and include arrangements for managing disruptions with the critical service provider.

11. Insurers should refer to APRA's *Prudential Standard GPS 220 Risk Management for General Insurers* for additional requirements regarding outsourcing arrangements.

Alternate sites

12. Alternate site refers to a site used for the resumption of critical business functions.

13. Where an insurer's BCP involves the use of an alternate site for the recovery of business and/or IT operations, this section applies regardless of whether the site

[1] A reference to a communication plan can be individual or collective. It is acknowledged an insurer may have a number of plans.

is another operational site (e.g. inter-state office) owned by the insurer, or a disaster recovery site managed by the insurer or a specialist third party service provider.

14. Where the alternate site is also a primary operational site (e.g. inter-state office) of the insurer, an assessment should be made of the capacity of the site and the timeframe over which the site could operate in a combined business continuity and operational mode.

15. The alternate site(s) should be located at sufficient distance from the primary operational site(s) to minimise the risk of both sites being unavailable simultaneously.

16. Insurers should where possible ensure that the alternate sites are not on the same power grid or telecommunications network as the primary operational sites.

17. Where an insurer has its primary operations in the Central Business District (**CBD**) of a major capital city, APRA would normally expect the alternate site to be located outside that CBD in order to minimise the risk of both sites being impacted by a wide area disruption. Where the two sites are located in the same CBD, the insurer will need to demonstrate to APRA that it has adequate arrangements in place to manage the potential risk of both sites being impacted simultaneously.

18. The transportation arrangements to the alternate site(s) should also be contained in the BCP. Alternate modes of transport to the alternate site(s) should be considered as a particular mode of transport may be unavailable as a result of the disruption.

19. The operational capacity of the alternate site(s) should satisfy the insurer's business continuity objectives set out in the BCP. A review and assessment of the capacity of the alternate site(s) should be undertaken at least annually.

20. Where the alternate site(s) has contracted arrangements with a number of other organisations, including other parts of the insurer or its parent's business, the contract between the insurer and the alternate site provider should clearly state the dedicated and shared functional and seating capacity available to the insurer.

21. The insurer should also assess the reliability of the shared capacity at the alternate site(s) provided by a service provider where the site is likely to be used for a longer duration.

Testing

22. The insurer's testing program could include a range of test approaches from desk-top "walk-throughs", individual component testing (e.g. IT equipment), through to fully integrated tests covering the whole insurer and including third party service providers. Testing scenarios, objectives and procedures should be developed and clearly documented.

23. The program of testing should be overseen by responsible senior management and involve all personnel with specific BCP responsibility.

24. Minimum testing requirements should include, but not be limited to:

    (a) staff evacuation procedures;

    (b) communication plans;

    (c) alternate site activation;

    (d) data back up and recovery;

    (e) physical and computer security; and

    (f) recovery of critical business functions.

25. For outsourcing arrangements, the insurer should involve itself in the critical service provider's testing program or, where this is not possible, seek an independent assurance that the critical service provider's BCP has been satisfactorily tested. The insurer should receive the critical service provider's test results on an annual basis (at a minimum) and these should be reported to responsible senior management and the Board of Directors or its responsible Committee.

Training

26. An insurer should implement a training program to build the knowledge and awareness of the business continuity management program amongst staff.

27. Staff with specific responsibility for the business continuity management program at the insurer should undertake the necessary training to ensure they are able to competently fulfil their responsibilities. The training requirements should be included in the performance objectives of responsible individuals.

28. All staff should be familiar with the relevant BCP for their business unit.