



# Prudential Practice Guide

## **SPG 232 – Business Continuity Management**

July 2013

## Disclaimer and copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

© Australian Prudential Regulation Authority (APRA)

This work is licensed under the Creative Commons Attribution 3.0 Australia Licence (CCBY 3.0).

 This licence allows you to copy, distribute and adapt this work, provided you attribute the work and do not suggest that APRA endorses you or your work. To view a full copy of the terms of this licence, visit [www.creativecommons.org/licenses/by/3.0/au/](http://www.creativecommons.org/licenses/by/3.0/au/).

## About this guide

Prudential Practice Guides (PPGs) provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss legal requirements from legislation, regulations or APRA's prudential standards, but do not themselves create enforceable requirements.

*Prudential Standard SPS 232 Business Continuity Management (SPS 232)* sets out APRA's requirements in relation to business continuity management (BCM). This PPG aims to assist an RSE licensee in complying with those requirements and, more generally, to outline prudent practices in relation to BCM.

For the purposes of this guide, and consistent with the application of SPS 232, 'RSE licensee' has the meaning given in the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

Subject to the requirements of SPS 232, an RSE licensee has the flexibility to manage its BCM arrangements in the way most suited to achieving its business objectives.

Not all the practices outlined in this PPG will be relevant for every RSE licensee and some aspects may vary depending upon the size, business mix and complexity of the RSE licensee's business operations.

## The role of the Board and senior management

1. Although the Board of the RSE licensee (Board) is ultimately responsible for BCM under SPS 232, APRA recognises that the Board may delegate certain functions. A Board may delegate day-to-day operational responsibility to a responsible committee and/or senior management and need not have a detailed knowledge of, or familiarity with, the particulars of the day-to-day management of BCM.

## Business continuity management

2. Business continuity is generally defined as a state of continued and uninterrupted operations of a business. BCM is an approach taken across the whole of the business to ensure business continuity.
3. In order to adopt a whole-of-business approach, many of the processes embedded within an RSE licensee's business operations will need to consider BCM. For example, BCM may need to be considered in:
  - (a) the planning phase for new business acquisitions, joint ventures and major projects involving the introduction of new business processes and systems; and
  - (b) staff training, including those without specific BCM responsibilities, to ensure staff are aware of business continuity issues.
4. A consistent method of documenting the BCM will typically be implemented throughout the RSE licensee's business operations and have detailed input at the business unit level.
5. A centralised business continuity function may be of assistance to ensure that common standards and practices are in place across an RSE licensee's business operations or a corporate group.

## Business Continuity Management Policy

6. The Business Continuity Management Policy (BCM Policy) required by SPS 232 is a high-level strategic document outlining an RSE licensee's objectives and approach in relation to BCM. The BCM Policy of an RSE licensee assists it in ensuring that critical business activities can be maintained or restored in the event of material disruptions and that the financial, legal, regulatory, reputational and other material consequences are minimised.
7. In many corporate groups it is common practice to develop and implement BCM across the group. Where this is the case, SPS 232 requires that an RSE licensee in a group will satisfy itself that the group BCM arrangements meet the RSE licensee's BCM Policy requirements.

## Business impact analysis

8. Business Impact Analysis (BIA) is a dynamic process that involves identifying all critical business activities and assessing the impact of a disruption on these activities. It is used to help shape a Business Continuity Plan (BCP).
9. Typically, a BIA will be conducted at least annually, or more frequently where there have been material changes to business operations or new or changed external factors that would alter the RSE licensee's BIA.
10. Components of a BIA will vary to reflect the size, business mix and complexity of an RSE licensee's business operations, but APRA would ordinarily expect it to detail:
  - (a) the likelihood of a disruption scenario leading to short-, medium- or long-term disruption to critical business activities;
  - (b) particulars of the impact of a disruption to critical business activities;
  - (c) the priority and timeframes assigned for the recovery of critical business activities; and
  - (d) the degree of difficulty, including the time taken, to restore the business activity or support function or implement alternate arrangements.

11. There are numerous disruption scenarios that may be encountered by an RSE licensee. Common scenarios include:
  - (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 staff); and
  - (h) loss of key dependencies.
12. In developing the BIA, critical interdependencies that are not within the RSE licensee's direct control will typically be identified and provided for within the scenario setting. This may include dependencies on utilities, outsourced service providers and key suppliers.
16. An RSE licensee may have a range of strategies to meet the recovery objectives.
17. In assessing recovery objectives, an RSE licensee may also consider the effect of:
  - (a) the increased risk of failed transactions;
  - (b) liquidity risks;
  - (c) solvency problems; and
  - (d) loss of confidence that prolonged disruptions may cause.

A prudent RSE licensee would also consider giving priority to the payment of benefits to beneficiaries ahead of other matters.

### Business continuity planning

### Recovery objectives and strategies

13. Recovery objectives are pre-defined goals for recovering specified critical business activities, to a specified level of service (recovery level) within a defined period (recovery time), following a disruption.
14. A recovery level is the target level of service that will be provided in respect of a specified business operation after a disruption. An RSE licensee may have a range of recovery levels for different business activities.
15. A recovery time is the target time taken to recover a specific business operation. An RSE licensee may divide recovery time as the duration:
  - (a) from the disruption to the activation of the BCP; and
  - (b) from the activation of the BCP to the recovery of the specific business operation.
18. The BCP facilitates the management of a disruption and the recovery of critical business activities. The ultimate objective of a BCP is the full restoration of an RSE licensee's operations to the point where the RSE licensee is able to resume normal business activities. An RSE licensee's BCP will typically include business continuity procedures that enable it to meet immediate and long-term recovery strategies.
19. In developing its BCP, the RSE licensee would usually sequence the recovery of operations according to their business impact, focusing first on critical operations.
20. In managing a disruption and recovering critical business activities, an RSE licensee's recovery strategies may consider the resources needed to run operations in the event that the primary operational site is unavailable. The resources may cover a wide range of things, including operational resources such as computer hardware and software, printers, faxes, telephones, standard stationery and forms. Additional resources may include suitably trained staff and relevant documentation such as insurance policies and contracts, up-to-date contact lists and copies of the BCP.

## BCP responsibilities and authorities

21. A BCP would typically document specific responsibilities and authorities for:
- (a) assessing the impact of the disruption;
  - (b) determining an appropriate response;
  - (c) implementing the communication plan;
  - (d) evacuating staff;
  - (e) activating an alternate site if required; and
  - (f) implementing recovery objectives.
- (iii) the reliability of the shared capacity;
  - (f) whether the alternate site and the primary operational site share the same power grid, telecommunications network or other physical infrastructure;
  - (g) whether the alternate site has sufficient current data and the necessary equipment and systems to recover critical business activities for a sufficient period of time; and
  - (h) whether adequate transport is available to the alternate site.

## Alternate site

22. An alternate site refers to a site used for the temporary resumption of critical business activities. This site may be an operational site owned by the RSE licensee or a disaster recovery site managed by the RSE licensee or an outsourced service provider.
23. In assessing the appropriateness of a particular alternate site, the following would typically be considered by the RSE licensee:
- (a) the capacity of the alternate site;
  - (b) the timeframe over which the site could operate in a particular combined business continuity and operational mode;
  - (c) the distance between the alternate site and the primary operational site, in order to minimise the risk of both sites being unavailable simultaneously;
  - (d) whether an annual review and assessment of the capacity and adequacy of the alternate site has been conducted;
  - (e) where the alternate site has contracted arrangements with a third party:
    - (i) the likelihood of multiple simultaneous calls on shared resources at the alternate site;
    - (ii) the impact of multiple simultaneous calls, for example, on the dedicated and shared functional and seating capacity available; and
24. In order to minimise the risk of a primary operational and alternate site being impacted by a wide area disruption, APRA would normally expect that, if the primary site is in a central business district, the alternate site would be located outside it.
25. An RSE licensee may consider conducting staff training at the alternate site on a regular basis to ensure there are sufficient staff able to recover critical business activities in the event of a disruption.

## Communication plan

26. A communication plan describes the information necessary for notifying key internal and external stakeholders if the BCP is invoked.<sup>1</sup> Examples of information that might be included in a communication plan are:
- (a) the process for notifying APRA, as soon as possible and no later than 24 hours after experiencing a major disruption that has the potential to have a material impact on its risk profile or to affect the RSE licensee's financial soundness, of the nature of the disruption, the action being taken, the likely effect, the timeframe for return to normal operations and when normal operations are resumed;
  - (b) identification of those responsible for communicating with staff and various external stakeholders;

<sup>1</sup> A reference to a communication plan can be individual or collective. An RSE licensee may have a number of plans.

- (c) a list of contact names, numbers and email addresses of, but not limited to, staff, regulators, members, counterparties, service providers, market authorities and media;
  - (d) out-of-hours numbers (including primary/alternate contacts) for all staff with BCP responsibility; and
  - (e) the staff authorised to deal with the media.
27. Ordinarily, contact lists require regular review to ensure they remain up-to-date.

## Outsourcing

28. *Prudential Standard SPS 231 Outsourcing* (SPS 231) defines outsourcing to involve an RSE licensee entering into an arrangement with any other party to perform, on a continuing basis, a business activity that currently is, or could be, undertaken by the RSE licensee itself.
29. Typically, an RSE licensee will have procedures in place to adapt the BCP in the event of any material outsourcing agreement that involves a change to business processes and systems.
30. While some RSE licensees may rely upon outsourced service providers for components of their BCP, accountability for the BCP remains with the RSE licensee. It is important for RSE licensees to recognise that, while outsourcing can be of significant benefit and may reduce some risks, it may also give rise to other risks.<sup>2</sup>
31. APRA expects that an RSE licensee would gain an understanding of the nature and scope of an outsourced service provider's BCP as it applies to the relevant activities under the outsourcing arrangement and satisfy itself that the BCP provides adequate protection to the interests of beneficiaries. A declaration from a service provider may assist an RSE licensee in forming a view as to whether the service provider will respond adequately in the event of a disruption.
32. Alternative contingency arrangements may need to be considered for the event that the outsourced 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.

## Review and testing of the BCP

33. Testing of the BCP is required under SPS 232 and is considered essential to ensuring that the BCP is capable of meeting its objectives. An RSE licensee will typically document testing scenarios, objectives and procedures. Testing would ordinarily be overseen by senior management and involve all personnel with specific responsibility for BCM.
34. There are a range of test approaches available to an RSE licensee, including:
- (a) desk-top 'walk-throughs';
  - (b) individual component testing (e.g. IT equipment);
  - (c) testing from an alternate site; and
  - (d) fully integrated tests covering the entire RSE licensee and outsourced service providers.
35. Areas of the BCP that are likely to require regular testing include:
- (a) staff evacuation procedures;
  - (b) communication plans;
  - (c) alternate site activation and capability;
  - (d) data back up and recovery;
  - (e) readiness of critical service providers;
  - (f) physical and computer security; and
  - (g) recovery of critical business activities.

<sup>2</sup> Refer to *Prudential Standard SPS 220 Risk Management* and SPS 231.



Telephone  
1300 55 88 49

Email  
[info@apra.gov.au](mailto:info@apra.gov.au)

Website  
[www.apra.gov.au](http://www.apra.gov.au)

Mail  
GPO Box 9836  
in all capital cities  
(except Hobart and Darwin)