

The Auditor-General
Audit Report No.46 2008-09
Performance Audit

Business Continuity Management and Emergency Management in Centrelink

© Commonwealth
of Australia 2009

ISSN 1036-7632

ISBN 0 642 81080 X

COPYRIGHT INFORMATION

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights should be addressed to:

Commonwealth Copyright
Administration
Attorney-General's Department
3-5 National Circuit
Barton ACT 2600

<http://www.ag.gov.au/cca>



Canberra ACT
25 June 2009

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in *Centrelink* in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Business Continuity Management and Emergency Management in Centrelink*.

Following its tabling in Parliament, the report will be placed on the Australian National Audit Office's Homepage—<http://www.anao.gov.au>.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Ian McPhee'.

Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office. The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone: (02) 6203 7505
Fax: (02) 6203 7519
Email: webmaster@anao.gov.au

ANAO audit reports and information about the ANAO are available at our internet address:

<http://www.anao.gov.au>

Audit Team

Nathan Williamson
Corinne Horton

Contents

| | |
|--|-----------|
| Abbreviations..... | 7 |
| Glossary | 9 |
| Summary and Recommendations | 11 |
| Summary | 13 |
| Introduction | 13 |
| Audit objectives, scope and criteria | 14 |
| Overall conclusion..... | 15 |
| Key findings..... | 17 |
| Summary of agencies' responses..... | 21 |
| Recommendations | 22 |
| Audit Findings and Conclusions | 25 |
| 1. Introduction | 27 |
| Background..... | 27 |
| Audit approach..... | 30 |
| ANAO Better Practice Guide on business continuity management..... | 31 |
| Structure of the Report..... | 33 |
| 2. Centrelink's Business Continuity Management Framework | 34 |
| Introduction | 34 |
| Business continuity management framework | 34 |
| Business continuity management governance arrangements..... | 36 |
| Crisis coordination..... | 40 |
| Business resumption through interim processing..... | 43 |
| Supporting documentation and other resources..... | 43 |
| Maturity of Centrelink's business continuity management framework..... | 44 |
| 3. Implementing the Business Continuity Management Framework | 46 |
| Introduction | 46 |
| Project initiation (Better Practice Guide Step 1) | 48 |
| Key business processes identification and business impact analysis (Better Practice Guide Steps 2 and 3)..... | 50 |
| Design and implementation of continuity treatments (Better Practice Guide Steps 4 and 5)..... | 57 |
| Testing and maintenance of plans (Better Practice Guide Step 6)..... | 65 |
| Business continuity management training | 69 |
| Review and improvement | 70 |
| 4. Update on Centrelink's Response to ANAO Audit Report No.9 2003–04, <i>Business Continuity Management and Emergency Management in Centrelink</i> | 74 |
| Introduction | 74 |
| Summary and assessment against previous audit recommendations | 74 |

| | |
|---|-----------|
| Appendices | 85 |
| Appendix 1: Department of Human Services' Response to the Audit Recommendations..... | 87 |
| Appendix 2: Centrelink's Business Continuity Priorities..... | 88 |
| Appendix 3: Centrelink's IT Disaster Recovery Plans | 89 |
| Appendix 4: IT Business Continuity Risks..... | 90 |
| Index..... | 96 |
| Series Titles..... | 98 |
| Current Better Practice Guides | 103 |

Abbreviations

| | |
|---------|--|
| ACCC | Area Crisis Coordination Centre |
| AGDRP | Australian Government Disaster Recovery Payment |
| BC | Business Continuity |
| BCCM | Business Continuity and Crisis Management Section |
| BCCM&S | Business Continuity, Crisis Management and Security Sub-committee |
| BCM | Business Continuity Management |
| BCP | Business Continuity Plan |
| BDC | Bruce Data Centre |
| BIA | Business Impact Analysis (or Assessment) |
| BPA | Business Partnership Agreement |
| BPG | ANAO Better Practice Guide |
| CCC | Crisis Coordination Centre |
| CDC | Canberra Data Centre (at Tuggeranong) |
| CEIs | Chief Executive Instructions |
| CEO | Chief Executive Officer |
| COF | Centrelink Operations Facility |
| CSC | Customer Service Centre |
| DEEWR | Department of Education, Employment and Workplace Relations |
| DHS | Department of Human Services |
| EM | Emergency Management |
| EMP | Emergency Management Plan |
| FaHCSIA | Department of Families, Housing, Community Services and Indigenous Affairs |
| ISIS | Income Security Integrated System |
| ITIL | IT Information Library |

| | |
|------|--|
| MAO | Maximum Allowable (or Acceptable) Outage |
| MoU | Memorandum of Understanding |
| NCCC | National Crisis Coordination Centre |
| NECC | National Emergency Call Centre |
| NSO | National Support Office |
| ORC | Operational Readiness Checklist |
| PIR | Post-implementation Review |

Glossary

| | |
|--|--|
| Business continuity | The uninterrupted availability of all key resources to support essential business processes. |
| Business continuity management | The development, implementation and maintenance of policies, frameworks and programs to assist an entity to manage a business disruption event, as well as build entity resilience. |
| Business continuity plan (BCP) | A collection of procedures and information that is developed, compiled and maintained in readiness for use in a business disruption event. |
| Business Impact Analysis (or Assessment) (BIA) | A management level analysis, which evaluates the risks of disruption to critical business processes, including consideration of the impacts of capability loss over time and the need for, and interdependencies of, resources. |
| Business resumption team | A team responsible for maintaining the business recovery procedures and coordinating the recovery of business functions and processes. |
| Community recovery | For Centrelink, the business processes involved in making payments of the Australian Government Disaster Recovery Payment (AGDRP) and ex gratia assistance, and in providing other community support such as social work services, in the event of a disaster. |
| Continuity treatment | Treatments designed to minimise the effects of disruptions to each key business process. |
| Crisis | An outage that exceeds the Maximum Acceptable Outage period or requires the organisation to respond to a community |

| | |
|--------------------------------|---|
| | emergency, such as a natural disaster. |
| Crisis response | The use of procedures to ensure that immediate actions are taken and issues escalated appropriately to the crisis leadership. |
| Emergency management | A range of controls and procedures for managing an incident that endangers or threatens to endanger life, property or the environment and that requires a significant and coordinated response. |
| Maximum Allowable Outage (MAO) | The maximum period of time that an entity can tolerate the disruption of a critical business process before the achievement of its objectives is adversely affected. |

Summary and Recommendations

Summary

Introduction

1. In 2007-08, Centrelink distributed \$70.5 billion in payments to 6.5 million customers. To deliver these payments, Centrelink employs a workforce of more than 26 000 staff who operate from over 1000 service delivery points across Australia. Supporting its staff and service delivery network, Centrelink also relies on a large and sophisticated information technology (IT) environment that processes approximately 6 billion transactions annually.

2. To ensure continuity of the vital services it provides to the community, Centrelink must have in place systems and processes that both reduce the risks of business interruptions and also helps restore functions when disruptions occur. These systems and processes should be complemented by appropriately trained staff that can react when interruptions occur or threaten to occur. It is the development, implementation and maintenance of a control framework to manage business disruptions and build entity resilience that constitutes an entity's approach to business continuity management (BCM).

3. Emergency management (EM) is linked with BCM and involves managing an emergency, such as a flood, that has an impact on the entity's activities. In Centrelink's case this can have an internal and/or external impact:

- An internal impact, such as a flooded building, that must be evacuated. This requires Centrelink to activate its business continuity plan and crisis coordination arrangements, and establish recovery and interim processes that can, over time, lead to a return to business as usual.
- An external impact, such as a town being flooded and residents requiring emergency assistance. In this respect Centrelink plays an important role in community recovery operations following a disaster through facilitating the payment of government financial assistance (the Australian Government Disaster Recovery Payment (AGDRP) and ex gratia payments) and providing other community support, such as social work and family liaison officer services, to people affected by disasters.

In some cases, internal and external impacts occur at the same time such that Centrelink may be required to simultaneously activate its business continuity plan and play a role in a community emergency response.

4. Accordingly, in addition to having BCM arrangements in place, it is important that Centrelink develops, implements and maintains arrangements to prepare for, respond to, and recover from, emergencies.

5. In 2003-04, the Australian National Audit Office (ANAO) undertook an audit of BCM and EM in Centrelink.¹ The audit ('previous audit') concluded that Centrelink generally had an appropriate framework for BCM and EM, however, it identified a number of continuity risks and made 11 recommendations to improve the implementation of BCM and EM in the agency. Centrelink agreed to all 11 recommendations.

Audit objectives, scope and criteria

6. The objectives of this audit were to:

- assess the current status of BCM and EM arrangements in Centrelink and identify opportunities for improvement; and
- review Centrelink's response to the recommendations and suggestions of the previous audit.

7. Centrelink's EM arrangements include an internal and an external component.² Community recovery operations form a major part of the external component but are not included within the scope of this audit. They will be addressed in a separate audit report to be published during 2009-10. Centrelink's role in providing services and payments to those people affected by the Queensland floods and Victorian bushfires during January/February 2009 will be examined as part of the separate audit report.

8. As the community recovery aspect of EM will be considered in a separate report, Recommendation No.11 from the previous audit is not considered in this report.³

9. The criteria for this audit included an examination of:

- Centrelink's progress in implementing the 10 recommendations and eight suggestions in the previous audit;

¹ Australian National Audit Office, ANAO Audit Report No.9 2003-04, *Business Continuity Management and Emergency Management in Centrelink*, Canberra.

² Refer Chapter 1, Figure 1.1, p. 29.

³ Recommendation No.11 related to Centrelink monitoring and reviewing its emergency stakeholder liaison and response planning at a national level.

- the alignment of recent Centrelink BCM and EM reforms with better practice;
- the extent to which BCM and EM arrangements reflect Centrelink’s strategic issues and risks; and
- Centrelink’s capacity to respond to business disruptions and community emergencies.

Overall conclusion

10. Centrelink is a primary contributor to Australian Government service delivery, administering over \$70 billion of payments on an annual basis. It is therefore critical that Centrelink has in place a mature BCM framework that can successfully limit and, where required, respond to business disruptions. A significant or prolonged disruption to Centrelink’s ‘business as usual’ activities has the potential to disrupt the delivery of payments to customers, often the more vulnerable members of the community, and more broadly impact on Centrelink’s ability to efficiently and effectively achieve its purpose of ‘assisting people to become self-sufficient and supporting those in need’.⁴

11. Centrelink has an established BCM and EM framework that it continues to develop and which is supported by operational policies, processes and staff. Given its geographically dispersed network, a strength of Centrelink’s BCM is its business resumption arrangements, which include the ability to seamlessly divert calls/processing from one call centre/customer service centre to another in the event of a disruption or failure. Centrelink also has effective crisis coordination arrangements that allow it to respond to a business continuity incident or disaster in an appropriate and timely manner.

12. Centrelink’s implementation of its BCM framework generally follows the six steps outlined in the 2000 ANAO Better Practice Guide.⁵ Centrelink has in place processes that allow continuity risks and treatments for new projects

⁴ About Us Index [Internet], Centrelink, available from: http://www.centrelink.gov.au/internet/internet.nsf/about_us/index.htm [accessed 19 April 2009].

⁵ ANAO Better Practice Guide—*Business Continuity Management—Keeping the Wheels in Motion: A Guide to Effective Control*, January 2000, Canberra, p. 30-64.

Given the timing of this audit and the release of the ANAO’s updated BPG – ‘*Business Continuity Management: Building resilience in public sector entities*’ – in June 2009, the original BPG has been used as the basis for analysing Centrelink’s BCM framework. Where relevant, regard has been given to the updated BPG.

to be identified and addressed, while continuity risks and recovery priorities are also identified for current services on an annual basis.

13. In some areas, however, the BCM framework and its implementation lack the maturity (that is the progress from planning, identifying risks and testing treatments to integration into 'business as usual') that could be reasonably expected of an organisation of Centrelink's size and complexity. Specifically, there is:

- scope to improve the clarity, high-level oversight and coordination of the framework, in particular the coordination of IT business continuity and the implementation of BCM and risk management arrangements;
- inadequate assurance that the continuity risks and recovery priorities identified for individual processes and services reflect an agency-wide perspective, or whether they can be met;
- a need to improve business continuity planning (which currently focuses on the initial crisis response) and tests of continuity plans and risk treatments, which in turn will help clarify the approach to, and management of, the different phases of BCM; and
- a need to identify and report on key performance indicators that measure the success or otherwise of BCM arrangements and identify areas for improvement.

14. Once a clearer and maintainable BCM framework has been implemented, Centrelink will need to shift its emphasis towards the testing, training and identification of opportunities for performance improvement. It is testing, training and continuous improvement which will assist Centrelink in building its capability and instilling a culture of readiness. This will in turn improve the maturity of its business continuity preparedness.

15. The BCM framework and its implementation require further development and this is reflected in the fact that, of the 11 recommendations in the previous audit of BCM and EM, Centrelink has fully implemented five recommendations and partially implemented five recommendations.⁶

16. The ANAO has made five recommendations in this audit aimed at assisting Centrelink to further improve its BCM framework and its application,

⁶ As the community recovery aspect of emergency management has been separated from this report (refer paragraphs 7-8), Recommendation No.11 from the previous audit is not considered in this report.

and address the areas not covered in the partial implementation of five recommendations from the previous audit.

Key findings

Current status of business continuity management arrangements in Centrelink (Chapters 2 and 3)

Centrelink's business continuity management framework

17. Centrelink's BCM framework includes a Business Continuity (BC) Policy,⁷ governance arrangements for the operation and high-level oversight of BCM, crisis escalation and coordination arrangements, identification of high-level BC priorities and other supporting processes and documents.

18. High-level oversight of BCM is provided by the Business Continuity, Crisis Management and Security (BCCM&S) Sub-committee, with day-to-day operational responsibility residing with the Business Continuity and Crisis Management Section. Until it was reconstituted in February 2009, the BCCM&S Sub-committee received reports on BCM and EM activities but not on IT continuity issues. This meant that the Sub-committee was not in a position to fully exercise agency-wide oversight of BCM issues. While the reconstitution of the Sub-committee occurred after the audit fieldwork was completed, Centrelink advised the ANAO that the Sub-Committee is now better positioned to provide agency-wide oversight of BCM and will receive regular reports on IT business continuity.⁸

19. Centrelink's BC Policy recognises that BCM is part of risk management. There are limited processes in place, however, to coordinate the planning and implementation of BCM and risk management policies and to exploit synergies between the two. For example, the risk assessments undertaken for risk management and BCM planning are completed separately, meaning they are not necessarily used to inform the other. High-level oversight of each process is also the responsibility of a different strategic committee. Centrelink has advised the ANAO that it plans to integrate BCM planning with its business and risk management planning from 2009–10.⁹

⁷ Centrelink, *Business Continuity Policy*, Canberra, 2007.

⁸ This is supported by early evidence of reporting to the February 2009 meeting of the BCCM&S Sub-committee that included IT business continuity related information.

⁹ Centrelink advice 16 April 2009.

20. Centrelink published its BC Policy and supporting processes in a coordinated package of booklets in 2005. While information on Centrelink's BCM framework is now maintained on its Intranet, some of this information, such as planning templates, requires improvement. Within the documentation and processes supporting Centrelink's framework, there is a lack of clarity in the use of terms relating to a disaster. This lack of clarity can limit a common understanding among staff of the steps and strategies involved in responding to a disaster and in turn impact on the organisation's BCM and EM preparedness. The framework could be improved by more clearly distinguishing the approaches to the initial crisis response, and the subsequent BCM and EM phases and treatments.

21. Centrelink has effective crisis coordination arrangements that include: established escalation arrangements; the ability to convene National and/or Area Crisis Coordination Centres; a number of core 'business resumption teams' to coordinate the restoration of services and support the National Crisis Coordination Centre (NCCC); and the Centrelink Operations Facility that monitors network performance and acts as the conduit for other internal and external information vital to an event.

22. Centrelink is planning further development and refinement of its BCM framework and supporting tools. Improvements in BC planning and testing, together with clarification and better agency-wide oversight of the framework, will provide Centrelink with the opportunity to improve its BC readiness and ability to respond quickly and effectively to continuity disruptions.

Implementation of business continuity management framework in Centrelink

23. In implementing its BCM framework, Centrelink has largely followed the steps outlined in the 2000 ANAO Better Practice Guide.¹⁰ There remain, however, some areas where implementation has either not fully covered the steps outlined in the BPG or where improvements can be made.

24. To ensure sufficient coverage of BC within an organisation, there is a need for all key business services and supporting processes to be identified. The impact of an interruption to these services and processes should then be analysed to establish the maximum length of time they can be interrupted before business objectives are compromised - the 'maximum allowable outage'

¹⁰ ANAO Better Practice Guide—Business Continuity Management—Keeping the Wheels in Motion: A Guide to Effective Control, January 2000, Canberra, p. 30-64.

(MAO). This can be done through a business criticality review, which allows an organisation to establish where its service risks exist, assess their relative importance through comparison (including using agreed MAOs) and identify strategies to address them. Centrelink last conducted a business criticality review in 2002 and has since then relied on annual assessments by National Support Office branches of MAOs for the services or processes they manage. These are complemented by seven high-level service business continuity priorities that were endorsed by Centrelink's Executive in 2008.

25. There are some limitations in this approach. In particular, there is no assurance that the MAOs determined by individual branches represent an agency-wide view of the relative criticality of those services or processes, or that they can be achieved. Given that it has been seven years since a formal business criticality review has been undertaken for all business processes performed within the agency, and there have been changes in Centrelink's business during this time, it is timely that Centrelink conduct another such review. A centralised annual review and endorsement of MAOs determined by branches would also help address the ability for an ongoing agency-wide assessment of the relative criticality of services and processes.

26. Branches' annual assessments of MAOs are prepared using a business impact analysis (BIA) template. The BIA assesses the tangible and intangible impacts of a business process being affected or downgraded for different time periods. A BIA is intended to guide the development of a business continuity plan (BCP), with the BCP including treatments (such as disaster recovery plans or interim processing) to deal with any continuity risks identified in the BIA. Centrelink business units currently only prepare emergency management plans (EMPs). EMPs have a focus on the initial crisis response phase and include checklists of immediate steps to be taken in the event of a crisis. While EMPs are a useful tool they do not identify continuity risks to business processes and proposed treatments for the risks that can then be tested – both of which are important elements of BCPs.

27. Centrelink is reviewing its continuity planning templates. Given the role of BCPs in the BCM framework, it is important that the BCP template is finalised and that business units are required to identify continuity risks and treatments in their BCPs. This process should align to the existing BIA process and usefully also link to business units' risk management planning.

28. Once BCPs have been prepared, Centrelink's focus can increasingly move to testing the continuity treatments in them and bedding BCM into its

'business as usual' operations. In this regard, and in the absence of BCPs, the continuity testing of EMPs has been ad hoc in nature. Centrelink does schedule tests of its IT disaster recovery plans but these are not necessarily being completed in a timely manner because of operational priorities. More regular and rigorous testing of its BCPs (once implemented) and disaster recovery plans will be useful for informing Centrelink of both strengths and weakness in its BCM framework and its application.

29. The previous audit identified a number of BC risks and/or opportunities for improvement in Centrelink's IT infrastructure and applications. Three of those risks related to Centrelink's data centres, off-site data storage and IT back-up arrangements. Centrelink is taking ongoing action to address these issues.

30. With the exception of the completion of scheduled tests of IT disaster recovery plans, Centrelink does not have established measures against which BCM performance can be assessed and areas for improvement identified. Accordingly, performance measurement could be improved by establishing key performance indicators and then reporting against those to the BCCM&S Sub-committee so that an agency-wide assessment of BCM preparedness can be provided to the Executive. Further, in line with the BCCM&S Sub-committee fulfilling its role and endeavouring to seek improved performance, post-implementation review reports on continuity incidents, including IT continuity incidents, should also be submitted to the Sub-Committee for consideration.

Update on Centrelink's response to the recommendations of the previous audit (Chapter 4)

31. Centrelink has fully implemented five of the recommendations (Nos. 2, 3, 5, 8 and 10) and partially implemented five of the recommendations (Nos. 1, 4, 6, 7, and 9) of the previous audit that relate to business continuity.

32. Areas where Centrelink has not fully implemented the recommendations of the previous audit include: under-utilising links between BCM and risk management arrangements, gaps in the BC planning and rehearsal area (reliance on EMPs only, with BCPs still to be implemented, and no minimum standards for plan rehearsals), inadequate maintenance of other key documentation (such as the IT Services Catalogue) that support IT continuity planning, and limited identification of corporate records and treatments for their protection.

Summary of agencies' responses

33. Summary responses to the proposed audit report and its recommendations were provided by Centrelink and the Department of Human Services. These responses are set out below.

Centrelink

Centrelink welcomes this report and considers that implementation of the recommendations will further enhance Business Continuity Management in Centrelink. In particular, the recommendations will inform the governance and performance management and testing of business continuity arrangements in Centrelink.

Centrelink agrees with the recommendations in the report.

Department of Human Services

The Department of Human Services (DHS) welcomes the follow-up report and notes that Centrelink agrees with the overall recommendations outlined in the Section 19 report.¹¹ Of the eleven recommendations made in the previous report, five recommendations have been fully implemented. A further five areas have been identified where improvements can be made. DHS notes the ANAO's acknowledgement that the reforms and initiatives already in hand address the outstanding matters raised in the Report.

¹¹ Refers to the proposed report provided to DHS for comment under sub section 19(3) of the *Auditor-General Act 1997*.

Recommendations

Recommendation No.1
Paragraph 2.17 To improve the governance arrangements for business continuity management (BCM) in Centrelink, the ANAO recommends that:

- (a) the recently constituted Business Continuity, Crisis Management and Security Sub-committee be provided with regular reports on IT business continuity issues; and
- (b) Centrelink review existing BC and risk management planning and implementation activities to identify areas where coordination and collaboration could be further improved.

Centrelink Response: Agree.

Recommendation No.2
Paragraph 3.29 In order to identify key business processes and provide for the regular comparative assessment of Maximum Allowable Outage periods (MAOs), the ANAO recommends that Centrelink:

- (a) commission a formal Business Criticality Review of its operations, including National Support Office, Area Offices and its service delivery channels; and
- (b) establish a process for the annual review and endorsement of MAOs determined by branches to ensure that they represent a collective view on the relative criticality of the services that Centrelink provides.

Centrelink Response: Agree.

Recommendation No.3**Paragraph 3.50**

The ANAO recommends that Centrelink develop and promulgate a business continuity plan (BCP) template and require business units to develop BCPs that identify:

- (a) risks to the business/service and their impact, based on the respective business impact analysis; and
- (b) risk treatments and business resumption tasks to manage these risks, which can then be tested on a regular basis.

Centrelink Response: Agree.

Recommendation No.4**Paragraph 3.85**

The ANAO recommends that the Business Continuity, Crisis Management and Security Sub-committee:

- (a) endorse an annual program of scheduled testing for business continuity plans, including relevant Disaster Recovery Plans for all services and systems assessed by the agency as being business critical; and
- (b) receive performance reports on the completion and key results of plan testing.

Centrelink Response: Agree.

Recommendation No.5**Paragraph 3.103**

The ANAO recommends that Centrelink:

- (a) develop performance measures against which its business continuity management preparation and response can be regularly monitored and assessed by the Business Continuity, Crisis Management and Security Sub-committee; and
- (b) provide reports to the Business Continuity, Crisis Management and Security Sub-committee on the findings and implementation of the recommendations of post-implementation review reports on business continuity incidents, including IT-related incidents.

Centrelink Response: Agree.

Audit Findings and Conclusions

1. Introduction

This chapter provides background on business continuity management and emergency management and the importance of such arrangements in Centrelink. It also explains the approach, objective and methodology of the audit.

Background

1.1 Business continuity management (BCM) is a risk management approach that is an essential business practice and represents an integral component of effective governance. BCM is the development, implementation and maintenance of policies, frameworks and programs (business controls) to assist an entity to manage a business disruption as well as build entity resilience to possible disruptions.¹²

1.2 Emergency management (EM) is linked with BCM and is the range of controls and procedures for managing an incident that endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response. An incident that requires EM can be one that either has an internal focus (for example, a building is flooded and requires evacuation) and/or an external focus, which involves an entity managing the impact of a community emergency (for example, a town has flooded and residents require emergency assistance). In some cases, internal and external impacts occur at the same time such that an entity may be required to simultaneously activate its business continuity plan and manage a community emergency response.¹³

Business continuity management and emergency management in Centrelink

1.3 Centrelink delivers government payments and services on behalf of a number of policy departments, in particular the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) and the Department of Education, Employment and Workplace Relations (DEEWR). In 2007-08, Centrelink distributed \$70.5 billion in payments to

¹² ANAO Better Practice Guide—*Business Continuity Management: Building resilience in public sector entities*, Canberra, 2009, p. 2.

¹³ *ibid.*, p. 6.

6.5 million customers who included retirees, families, carers, Indigenous people, parents and people with disabilities. To deliver these payments, Centrelink employs a workforce of more than 26 000 staff who operate from over 1000 service delivery points (including 316 customer service centres and 25 call centres) across Australia. Supporting its staff and service delivery network, Centrelink also relies on a large and sophisticated information technology (IT) environment that processes approximately six billion transactions on an annual basis.

1.4 To ensure continuity of service from its network and payments to its clients, often the more vulnerable people in the community, Centrelink must have in place systems and processes that both reduce the risks of business interruptions and also help restore functions when disruptions occur. These systems and processes, together with the ability of staff to react appropriately when interruptions occur or threaten to occur, underpin Centrelink's ability to continue to supply vital services to Australians in the event of a critical business system failure.

1.5 Centrelink also plays an important role in community response and recovery operations following a disaster, such as a flood or bushfire, through facilitating the payment of government financial assistance (the Australian Government Disaster Recovery Payment (AGDRP) and ex gratia payments) and providing other community support, such as social work and family liaison officer services, to people affected by disasters. Accordingly, it is important that Centrelink develops, implements and maintains arrangements to prepare for, respond to and recover from community emergencies.

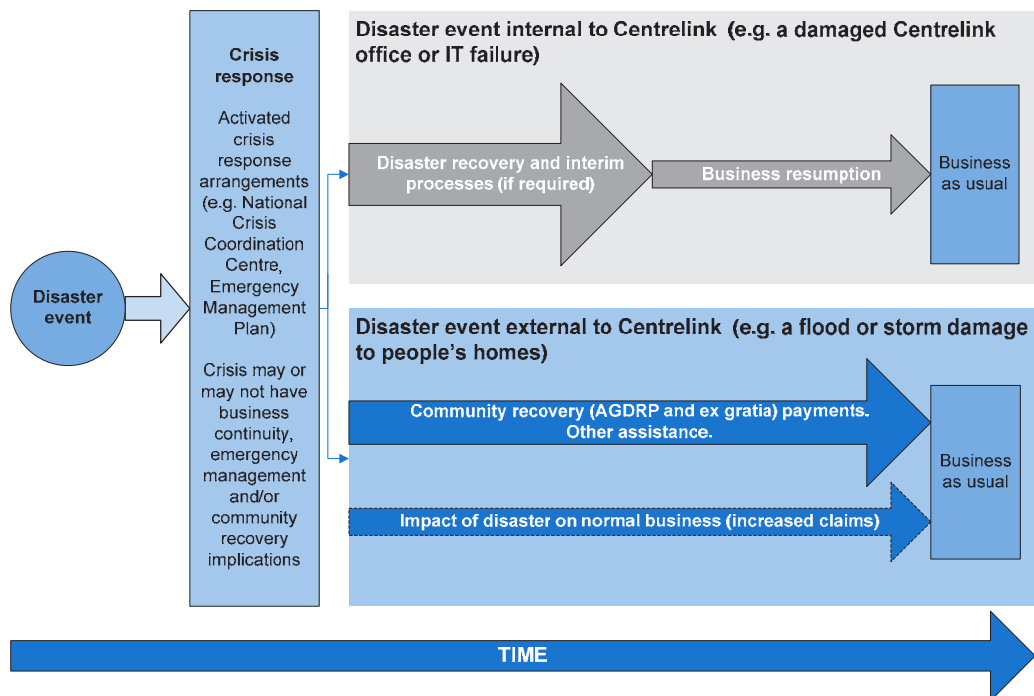
1.6 When a disaster occurs there is a need for a timely and effective initial response ('crisis response'), followed by:

- where a disaster affects Centrelink's capacity to provide services (for example, a failure of its IT systems or a flooded office), the implementation of disaster recovery and, if required, interim processes to restore adversely affected services; and/or
- in the case of a disaster affecting the community, such as a flood, the provision of community recovery assistance.

1.7 Figure 1.1 outlines the BCM and EM phases following a disaster and their inter-relationships.

Figure 1.1

Phases of business continuity and emergency management in Centrelink following a disaster event



Source: ANAO analysis

Previous audit

1.8 In 2003–04, the ANAO undertook an audit of BCM and EM in Centrelink.¹⁴ The audit ('previous audit') concluded that Centrelink generally had an appropriate framework for BCM and EM and that Centrelink had been successful at that time in delivering services continually and responding to emergencies. However, it identified a number of continuity risks and made 11 recommendations to improve the implementation of BCM and EM in Centrelink. Centrelink agreed to all 11 recommendations.

¹⁴ Australian National Audit Office, ANAO Audit Report No.9 2003–04, *Business Continuity Management and Emergency Management in Centrelink*, Canberra.

Audit approach

Audit objectives and scope

1.9 The objectives of this audit were to:

- assess the current status of Centrelink's BCM and EM arrangements in Centrelink and identify opportunities for improvement; and
- review Centrelink's progress in implementing the recommendations of ANAO Audit Report No.9 2003-04, *Business Continuity Management and Emergency Management in Centrelink*, and its response to the suggestions made in that report.

1.10 Centrelink's community recovery operations, which can be largely categorised as an external component of its EM arrangements, are not within the scope of this audit but will be addressed in a separate audit report to be published during 2009–10. Centrelink's role in providing services and payments to those people affected by the Queensland floods and Victorian bushfires during January/February 2009 will be examined as part of the separate audit report.

1.11 In assessing Centrelink's performance against the audit objectives the ANAO examined:

- Centrelink's progress in implementing the 10 recommendations of the previous audit and its response to the suggestions made by that audit;
- changes to Centrelink's BCM and EM frameworks over the past five years and how well they reflect Centrelink's current strategic issues and risks and accord with better practice;
- the adequacy of Centrelink's BCM processes, particularly as they affect its IT environment;
- action Centrelink has taken to ensure that staff at all levels of the organisation are aware of the importance of BC and their roles; and
- examples of Centrelink's responses to instances of service disruption and community emergencies in the past five years.

Audit methodology

1.12 To conduct the audit, the ANAO:

- asked Centrelink to document what action it had taken in response to the recommendations and suggestions of the previous audit;
- collected and reviewed Centrelink documentation, including reports, committee meeting minutes, emails, performance data and financial information;
- interviewed Centrelink staff and stakeholders; and
- visited Area Offices involved in responding to community emergencies over the past five years.

ANAO Better Practice Guide on business continuity management

1.13 The ANAO published a Better Practice Guide (BPG) on BCM in January 2000.¹⁵ An updated BPG was published in June 2009.¹⁶

1.14 The original BPG outlines a six step better practice approach to BCM that is shown in Figure 1.2 and aims to give practical assistance to agencies on how to organise business continuity management. While it outlines the essential elements of a successful BCM framework and provides guidance on how a BCM framework can be developed into an effective BC plan, it does not seek to prescribe the construct of BCM for every agency. The appropriate implementation of BCM will depend largely on factors such as an agency's objectives, functions, size, location(s), material assets and clients.







¹⁵ ANAO Better Practice Guide—*Business Continuity Management—Keeping the Wheels in Motion: A Guide to Effective Control*, Canberra, 2000.

¹⁶ ANAO Better Practice Guide—*Business Continuity Management: Building resilience in public sector entities*, Canberra, 2009.

Given the timing of this audit and the release of the updated BPG, the original BPG has been used as the basis for analysing Centrelink's BCM framework. However, where relevant, regard has been given to the updated BPG.

Figure 1.2

Steps in the business continuity process

| | | | |
|---|--|---|---|
|  | <p>1. Project initiation</p> <ul style="list-style-type: none"> Document objectives, scope boundaries Establish management committee Establish budget and timetable | <p>Project plan</p> | <p>Executive management involvement required</p> |
|  | <p>2. Identify Key business processes</p> <ul style="list-style-type: none"> Identify key business objectives Identify key business outputs Align business processes with key outputs Understand key activities, resources and inter-dependencies | <p>Key activity and resource schedule</p> | <p>For key business processes only</p> <ul style="list-style-type: none"> Activities Resources |
|  | <p>3. Undertake business impact analysis</p> <ul style="list-style-type: none"> Identify key personnel Schedule and conduct interviews Document concerns, priorities and expectations Determine Maximum Acceptable Outage for each process | <p>'Maximum acceptable outage' schedule</p> | <p>Treatments designed to:</p> <p>Prevent</p> <ul style="list-style-type: none"> Reduce likelihood Reduce consequence <p>Recover</p> <ul style="list-style-type: none"> Respond Interim Restore |
|  | <p>4. Design continuity treatments</p> <ul style="list-style-type: none"> Review existing controls Identify and evaluate options Select alternative activities and resources Implement treatments | <p>Risk treatment plan</p> | <p>Contents</p> <ul style="list-style-type: none"> Cover page Table of contents Event log Management plan Service area plans References Technical items Contract lists Inventory Limitations |
|  | <p>5. Implement continuity treatments</p> <ul style="list-style-type: none"> Establish recovery teams Document service area action steps Establish event escalation process Obtain contract and inventory lists Document recovery management process | <p>Contracts with vendors, suppliers.</p> <p>Updates to policy and procedure manuals</p> <p>Business continuity plan</p> | |
|  | <p>6. Test and maintain plan</p> <ul style="list-style-type: none"> Paper test Manual verification Supply validation Supply, service & equipment availability Structured walkthrough Unannounced team assembly | <p>Test plan</p> | <p>Timing</p> <ul style="list-style-type: none"> Annually |

Source: Australian National Audit Office, ANAO Better Practice Guide-*Business Continuity Management- Keeping the Wheels in Motion: A Guide to Effective Control*, Canberra, January 2000, p. 30.

Structure of the Report

1.15 The structure of the report is outlined below:

Chapter 2: Centrelink’s Business Continuity Management Framework

Examines the framework and overarching structures for business continuity management in Centrelink, including developments since the previous audit.

Chapter 3: Implementing the Business Continuity Management Framework

Analyses Centrelink’s implementation of its business continuity management (BCM) framework using the steps set out in the 2000 ANAO Better Practice Guide – *Business Continuity Management-Keeping the Wheels in Motion: A Guide to Effective Control*. It also examines Centrelink’s approach to reviewing and improving the implementation of its BCM framework and the BCM training that is provided to staff.

Chapter 4: Update on Centrelink’s Response to Audit Report No. 9 2003-04, *Business Continuity Management and Emergency Management in Centrelink*

Compares the findings of this audit with the 10 recommendations on business continuity management made in ANAO Audit Report No. 9 2003-04, *Business Continuity Management and Emergency Management in Centrelink*.

2. Centrelink's Business Continuity Management Framework

This chapter examines the framework and overarching structures for business continuity management in Centrelink, including developments since the previous audit.

Introduction

2.1 BCM is an integral component of public sector governance. It must support and sustain the entity's business strategy, goals and objectives in the face of disruptive events.¹⁷ Accordingly, having in place an effective BCM framework that can be tested and applied is critical to the ongoing success of an organisation.

Business continuity management framework

2.2 Centrelink has developed a Policy¹⁸ and supporting processes for the implementation of BCM that it collectively describes as its Business Continuity Control Framework. The Policy and processes:

- identify seven broad BC priorities (refer Appendix 2);¹⁹
- outline the governance arrangements for BCM, in particular:
 - the roles and responsibilities of National Support Office (NSO) and Area Office staff for BCM and EM; and
 - the arrangements for the high-level oversight of BCM;
- provide for the establishment, when needed, of crisis escalation and coordination arrangements. These are invoked both for incidents affecting the continuity of Centrelink's services and for disasters where Centrelink needs to provide community recovery assistance;

¹⁷ Australian National Audit Office, ANAO Better Practice Guide-*Business Continuity Management: Building resilience in public sector entities*, Canberra, 2009, p. 7.

¹⁸ Centrelink, *Business Continuity Policy*, 2007.

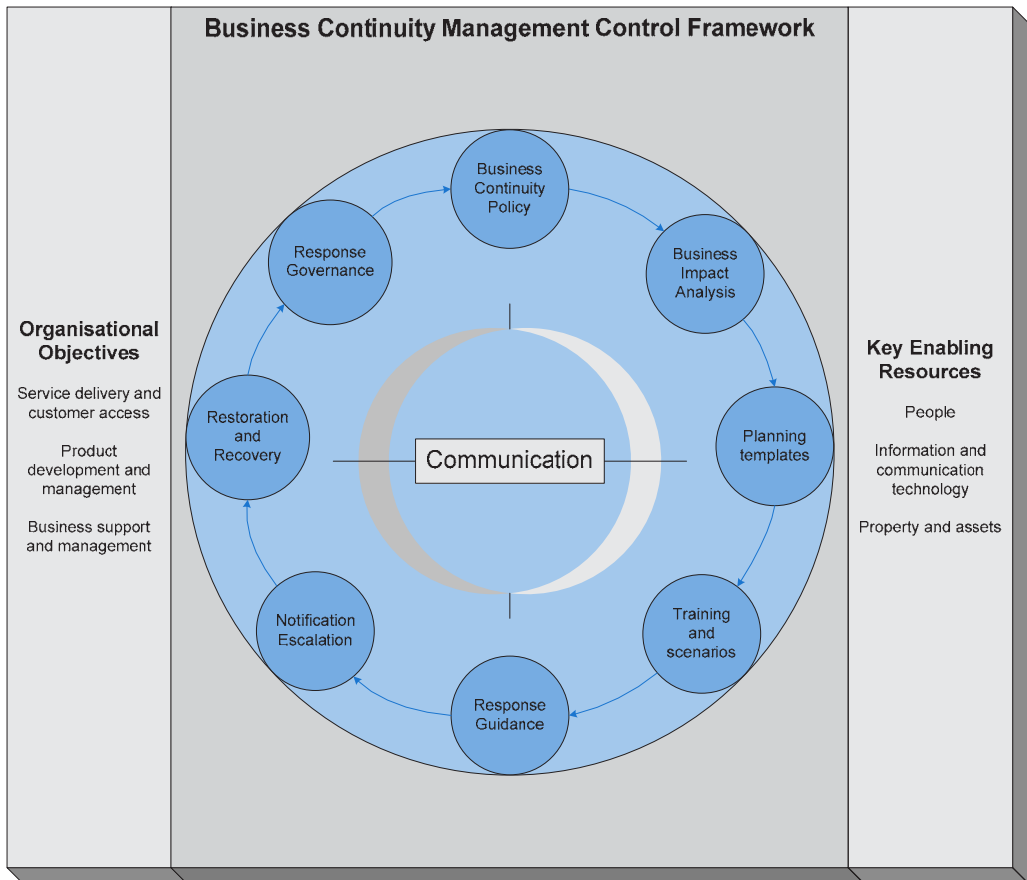
¹⁹ These were approved by the Centrelink Executive Committee in April 2008.

- provide that business units should assess continuity risks and have in place suitable risk continuity treatments, such as disaster recovery plans; and
- contain a number of supporting guidance documents, planning templates, tools and other resources.

2.3 Centrelink's BCM control framework is depicted in Figure 2.1.

Figure 2.1

Centrelink's business continuity management control framework



Source: Adapted from a diagram in Centrelink's Business Continuity Policy 2007.

2.4 In examining Centrelink's BCM framework, the ANAO reviewed particular aspects that included the governance arrangements, crisis coordination procedures and processes, business resumption, supporting documentation and process and the overall maturity of the framework.

Business continuity management governance arrangements

2.5 Under Centrelink's governance framework, the Chief Executive Officer (CEO) delegates responsibilities to individual members of Centrelink's Senior Executive Service (SES) and holds them accountable for the decisions and actions they take on the CEO's behalf. Each SES officer is responsible for managing continuity risks for the services that they manage.²⁰ At the same time, strategic committees bring together senior managers to oversee, monitor and review Centrelink's business activities.

Organisational arrangements for the oversight of day-to-day business continuity management in Centrelink

2.6 Centrelink has established the Business Continuity and Crisis Management (BCCM) Section in the Network Coordination and Emergency Management Branch as a central point of oversight with responsibility for BCM and EM throughout the agency.²¹ BCCM's role is to:

- maintain and improve the BCM control framework and its application across the Centrelink business environment;
- manage the National Emergency Call Centre (NECC), a virtual call centre that is activated, under Prime Ministerial direction, at times of national emergency;²² and
- coordinate Centrelink's preparedness for a possible pandemic.²³

2.7 Given the significant role played by IT systems and process in Centrelink's business, an IT Service Continuity Management (ITSCM) Team has also been established within the IT Service Delivery Strategy and Management Branch. The ITSCM Team is intended to complement the BCCM

²⁰ The roles and responsibilities of Centrelink staff for BCM are listed in Centrelink's Business Continuity Policy 2007, op. cit., p. 2. Delegation of responsibilities for specific matters occurs through the Chief Executive Instructions.

²¹ Centrelink advice 5 June 2009. The Network Coordination and Emergency Management Branch had been divided into two branches from 4 May 2009. The BCCM Section is contained within the newly formed Emergency Management Branch.

²² The NECC is intended as a first point of contact for the public in the event of an emergency or disaster of national significance to ensure a coordinated, whole of government response to both the delivery and receipt of information.

²³ Given the potentially significant BC implications of a pandemic, all Commonwealth Government agencies are working on strategies to deal with such a situation.

and has responsibility for IT continuity issues. It is designed to ensure the existence of an IT contingency and recovery capability that supports the continued delivery of critical business services in the event of a disaster; and also recover critical business services within agreed timeframes.

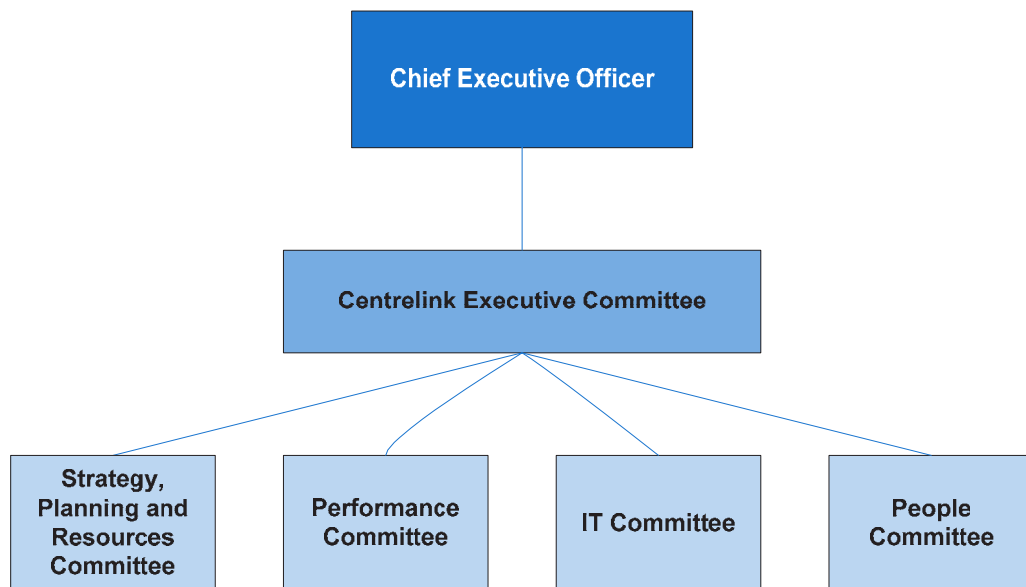
2.8 Given Centrelink has two key areas within different branches that are collectively responsible for the agency's BCM arrangements it is important that the BCCM Section and the ITSCM Team work collaboratively in order for Centrelink to have a coordinated and agency-wide view of BCM. In this regard, there has been a long association between the BCCM Section and the ITSCM Team in managing Centrelink BCM and EM, particularly given their previous co-location, and the two areas continue to work closely in promoting BCM in Centrelink. For example, they consult each other during BCM planning, particularly when advising business units on undertaking business impact analysis and in identifying vital records.

High-level oversight of business continuity management

2.9 High-level oversight of Centrelink's operations is provided through its strategic committees. This consists of an Executive Committee, which is supported by four high-level committees who have various sub-committees that report to them. This committee structure is shown at Figure 2.2.

Figure 2.2

Centrelink’s strategic committee structure



Source: Centrelink

2.10 Centrelink has a Business Continuity, Crisis Management and Security (BCCM&S) Sub-committee that provides high-level oversight of BCM and reports to the Performance Committee. The BCCM&S Sub-committee meets bi-monthly and is chaired by the General Manager of the Network Performance Division.²⁴

2.11 Until its reconstitution in February 2009,²⁵ the BCCM&S Sub-committee did not receive reports on IT-related BCM issues. Instead, high-level oversight of IT, including BC issues, was provided by the IT Committee. This meant that the BCCM&S Sub-committee was limited in its ability to exercise agency-wide oversight of BCM arrangements and effectively provide appropriate assurances to the Executive.

²⁴ The BCCM&S Sub-committee includes representatives from the Audit, Governance and Assurance Division; Property and Environment Branch; Network Coordination and Emergency Management Branch; People Services Branch; Security and Information Protection Branch; and the IT Service Delivery Strategy and Management Branch.

²⁵ Before February 2009, this committee was known as the Business Continuity, Emergency Management and Security Sub-committee and it reported to the then Strategic Planning & Resources Committee.

2.12 The reconstitution of the BCCM&S Sub-committee occurred after the audit fieldwork was completed. Centrelink advised the ANAO that the Sub-Committee is now better positioned to provide agency-wide oversight of BCM and will receive regular reports on IT business continuity.²⁶ While the IT Committee will continue to focus on treating IT-specific continuity risks, regular and sufficient reporting from the IT Service Delivery Strategy and Management Branch to the BCCM&S Sub-committee on IT continuity issues will better allow the Sub-committee to exercise agency-wide oversight of BCM arrangements and effectively provide appropriate assurances to the Executive.

Links between risk management and business continuity management in Centrelink

2.13 While every organisation faces a range of risks, such as business continuity, effective organisations put in place arrangements to systematically identify and treat such risks. Centrelink recognises the close relationship between risk management and BCM. For example:

- Centrelink's risk management framework includes a requirement for an annual facilitated BC risk assessment at the corporate level;²⁷ and
- Centrelink's BC Policy states that:
Business Continuity is that part of risk management that establish (*sic*) effective treatments should a business continuity incident occur.²⁸

2.14 The Centrelink Executive Committee provides high-level oversight of strategic risks to the agency²⁹ while the Planning and Risk Management Section in the Planning and Demand Management Branch is responsible for overall management of Centrelink's risk management policies.

2.15 Despite recognising the relationship between risk management and BC, there are limited processes in place to coordinate the planning and implementation of BC and risk management policies and to exploit any synergies between the two. As a result:

²⁶ This is supported by early evidence of reporting to the February 2009 meeting of the BCCM&S Sub-committee that included IT business continuity related information.

²⁷ Centrelink, *Centrelink's Risk Management Policy Framework and Handbook*, 2007, p. 34.

²⁸ Centrelink, *Business Continuity Policy*, op. cit., p. 4.

²⁹ Progress in implementing risk management strategies is also reported to the Audit Committee.

- BCM planning does not utilise risk assessments or the expertise of the Centrelink Risk Management Team;³⁰ and
- risk management planning does not utilise the business impact analysis that Centrelink National Support Office (NSO) branches undertake as part of their BC planning, and which could also usefully feed into risk management planning if BC and risk management planning were coordinated.

2.16 Centrelink advised the ANAO that it is now planning to integrate BC planning into its 2009–10 annual business planning cycle and to require business units to consider continuity risks when preparing business and risk management plans.³¹ Such a step has the potential to improve coordination in the planning and implementation of its BCM and risk management policies.

Recommendation No.1

2.17 To improve the governance arrangements for business continuity management (BCM) in Centrelink, the ANAO recommends that:

- the recently constituted Business Continuity, Crisis Management and Security Sub-committee be provided with regular reports on IT business continuity issues; and
- Centrelink review existing BC and risk management planning and implementation activities to identify areas where coordination and collaboration could be further improved.

Centrelink Response

2.18 Agree.

Crisis coordination

2.19 It is important that appropriate and timely action is taken in response to a business continuity incident or disaster. This includes the need for timely notification and escalation procedures and established arrangements for the effective and efficient coordination of response efforts.

³⁰ Centrelink Internal Audit Report, *Business Continuity Management* (June 2008), p. 18.

³¹ Centrelink advice 16 April 2009.

Escalation procedures

2.20 Centrelink has established escalation procedures for crisis situations that ensure that senior management, the Department of Human Services (DHS) and the Minister for Human Services (the Minister) are advised, as needed.

2.21 Under arrangements agreed in 2008,³² Centrelink must first inform the Secretary of DHS of the disruption and DHS is then responsible for advising the Minister or their office and the Department of the Prime Minister and Cabinet. Relevant client agencies are informed of the disruption by Centrelink after DHS has advised the Minister. Under previous arrangements, the Centrelink CEO would advise the Minister directly about the business disruption. The ANAO is not aware of any difficulties in the operation of the current escalation arrangements, but notes that with an additional layer in the notification process, care is needed to ensure that there is no undue delay in advising the Minister and stakeholders of a disaster situation.

Crisis coordination centres

2.22 Centrelink establishes crisis coordination centres (CCCs) at the National and/or the Area level, depending on the nature of the crisis and the response that is required.

National Crisis Coordination Centre

2.23 The National Crisis Coordination Centre (NCCC) is used in the event of a crisis, business disruption or emergency that has a large impact on Centrelink or its customers. It provides an initial response for large or serious incidents, as well as disaster assessment, reporting and, where necessary, escalation of issues for decision by Ministers. Centrelink's primary NCCC is located in the NSO,³³ where there is a specific and purpose-designed room that is equipped with video and telephone conference facilities. It is located close to the BCCM and Community Recovery Sections, which have ready access to business continuity documentation and provide support services to the NCCC. A secondary centre is located in Centrelink's Area Office South West NSW.³⁴

³² Centrelink, *Protocol for the Escalation process in Centrelink of major problems and how and who to advise DHS and Purchasing Departments*, 2008.

³³ Caroline Chisholm Centre, Tuggeranong, Canberra, Australian Capital Territory.

³⁴ Queanbeyan, New South Wales.

This is also equipped with telephone conference facilities and the Area Office is able to provide other services, such as computer access, that may be needed.

2.24 Centrelink has identified a number of core 'business resumption teams' or core business areas within Centrelink to coordinate the restoration of services (such as implementing disaster recovery procedures and establishing interim processes) and to support the NCCC.³⁵ Business resumption teams are also responsible for maintaining business recovery procedures.

2.25 Centrelink did not activate the NCCC for Cyclone Larry in 2006, and instead chose to activate an Area CCC. The post-implementation review of Centrelink's response to Cyclone Larry recommended that the NCCC be activated where there is a likelihood that the disaster will require a substantial amount of national coordination in response.³⁶ Following the Cyclone Larry PIR, Centrelink activated the NCCC for all community disasters that were examined.³⁷

2.26 The ANAO had the opportunity to observe the operation of the NCCC in the event of a community disaster,³⁸ and saw that it brought together stakeholders from throughout Centrelink and FaHCSIA and enabled emerging issues to be identified and addressed quickly.

Area Crisis Coordination Centres

2.27 An Area Crisis Coordination Centre (ACCC) is established where the Area Office determines that a continuity incident cannot be managed through existing functional structures and responsibilities. For instance, in the 2008 South-east Queensland floods, an ACCC was established (in addition to the NCCC) to coordinate the Area response effort because of the difficulties posed by the severe weather.³⁹ ACCC sites in Centrelink Area Offices, like the secondary centre for the NCCC in the Area South-West office, are equipped with telephone conference facilities and the Area Office is able to provide other

³⁵ These NCCC recovery teams are: CEO/Deputy CEO; Applications Infrastructure Team; I&T Infrastructure Team; People Management Team; Voice Communication Team; Area Command Group; Secretariat; Buildings Team; Recovery Director; Command Centre Team; Finance & Payments Team; Communication and Marketing Team; and Media spokesperson.

³⁶ Centrelink, *Post-implementation review of Centrelink's Response to Cyclone Larry (June 2006)*, p. 31.

³⁷ Hunter & Central Coast storms and floods (June 2007), Queensland storms and floods (January 2008), Mackay floods (February 2008) and South-East Queensland storms and floods (November 2008).

³⁸ South-east Queensland storms and floods in November 2008.

³⁹ Centrelink, *National Crisis Coordination Centre minutes*, 19 November 2008.

services, such as computer access, that may be needed. Designated Area Office staff retain contact lists and other materials for use in crisis situations.

Centrelink Operations Facility

2.28 In October 2008, Centrelink established an operations room – the Centrelink Operations Facility (COF) – at its NSO to monitor network performance and gather other internal and external information (from the media and other sources), and so promote better informed operational management decisions. The COF is located adjacent to the NCCC and the facilities of both are linked. During the course of the audit Centrelink was required to provide support to Australians affected by the Mumbai terrorist attacks. Centrelink used the COF during this emergency to monitor developments during the crisis. As the functionality of the COF is expanded in the future, it can be expected to play an increasingly significant role in providing up-to-date information to members of the NCCC.

Business resumption through interim processing

2.29 Given the scope and complexity of Centrelink's business it is important that effective redundancy arrangements to provide service resilience. In many cases, if an area of Centrelink suffers from a business disruption, it is able to relocate the service provided by that area to another part of the network or through a different channel. For example, if one of Centrelink's call centres has a disruption or fails, Centrelink can divert calls to another functioning call centre. Similarly, where there is a disruption in a customer service centre (CSC), a minimal presence can be maintained at the CSC or in a temporary location,⁴⁰ and processing for that CSC can be redirected to other locations.

Supporting documentation and other resources

2.30 In 2005, Centrelink published a BCM Policy and supporting processes in a coordinated package of booklets.⁴¹ Information on Centrelink's BCM Policy, BCM priorities, BCM and EM program and supporting processes are now maintained on its Intranet. While collectively these provide a reasonably

⁴⁰ Centrelink is able to fly in equipment to enable a temporary service to be provided.

⁴¹ The ANAO found that some areas continued to use these booklets, although they had not been updated and reissued to reflect changes to the business or processes and procedures since 2005. Centrelink advised on 16 April 2009 that they are to be withdrawn.

good explanation of Centrelink's BCM Policy, some supporting processes (such as planning templates and regular testing of business continuity plans-refer paragraphs 3.39-3.49 and 3.69-3.74) require improvement.

2.31 Within the documentation and processes supporting Centrelink's framework there is a lack of clarity in the use of terms relating to a disaster.⁴² For instance, in some cases, Centrelink used the term 'Emergency Management' to refer to its management of an emergency and in particular, its initial crisis response.⁴³ While in other cases 'Emergency Management' referred to Centrelink's overall management of the community recovery assistance it provides in the event of a community emergency.⁴⁴

2.32 This lack of clarity can limit a common understanding among staff of the steps and strategies involved in responding to a disaster and in turn impact on the organisation's BCM and EM preparedness. To address this risk, there would be benefit in Centrelink more clearly and consistently using terms associated with BCM and EM and their subsequent treatments in its policy, operational documents and procedures. In particular, this should involve clearly distinguishing between the approaches to the initial crisis response (which can apply to one or both of BC disruptions and/or community disaster responses) and the subsequent BCM and EM phases and treatments following a disaster.

Maturity of Centrelink's business continuity management framework

2.33 A BCM framework and related processes exist to increase the capacity of an organisation to minimise the impact of disaster events on the continuity of its services. Once in place, the focus should be on testing BC plans and strategies and on embedding a culture of BCM in the organisation. The plans and strategies are tools to improve the preparedness of the organisation to respond effectively to disaster events - they are not ends in themselves.

⁴² This lack of clarity was not assisted by Centrelink's *Emergency Planning and Preparedness Glossary* <<http://centrenet/homepage/divnetpf/bmcem/glossary.htm>> [accessed 13 November 2008], which contained a combined definition for BCM and EM. Centrelink advised on 16 April 2009 that this was an error and that the definition related only to Emergency Management. It has since amended the Glossary.

⁴³ For example, Centrelink's Emergency Management Plans.

⁴⁴ For example, a paper to the then Security, Emergency Management and Business Continuity and Security Sub-committee on 30 September 2008, item 4.3 and Centrelink's annual reports for 2005-06, 2006-07 and 2007-08 (p. 97-100).

2.34 Centrelink commissioned an external review of its BCM strategy in 2007, which was received in April 2008.⁴⁵ Consistent with the ANAO's findings in this audit, this review concluded that, while ensuring that deliverables such as business impact analyses and business continuity plans were reviewed and tested, crisis coordination arrangements are important in the context of a relatively immature continuity environment:

we recommend that Centrelink work in future years to establish outcomes in terms of readiness, maturity and ability, rather than plans, assessments and documents.⁴⁶

2.35 Once having established a clearer and maintainable BCM framework, it will be important that Centrelink shifts its emphasis towards the testing, training and identification of opportunities for performance improvement. It is testing, training and continuous improvement, which will assist Centrelink to build its capability and instil a culture of readiness that will improve the maturity of its BC preparedness.

2.36 The ANAO notes that Centrelink is planning further development and refinement of its BCM strategy and supporting tools, such as improvements in BC planning and testing. This further development, together with the clarification of the framework and increased integrated oversight that is recommended in this audit, will provide the opportunity to improve Centrelink's BC readiness and ability and therefore the maturity of the BCM framework.

⁴⁵ Protiviti, *Review of Business Continuity Strategy for 2007-08* (April 2008).

⁴⁶ *ibid.*, p. 13.

3. Implementing the Business Continuity Management Framework

This chapter analyses Centrelink's implementation of its business continuity management (BCM) framework using the steps set out in the 2000 ANAO Better Practice Guide, Business Continuity Management-Keeping the Wheels in Motion: A Guide to Effective Control. It also examines Centrelink's approach to reviewing and improving the implementation of its BCM framework and the BCM training that is provided to staff.

Introduction

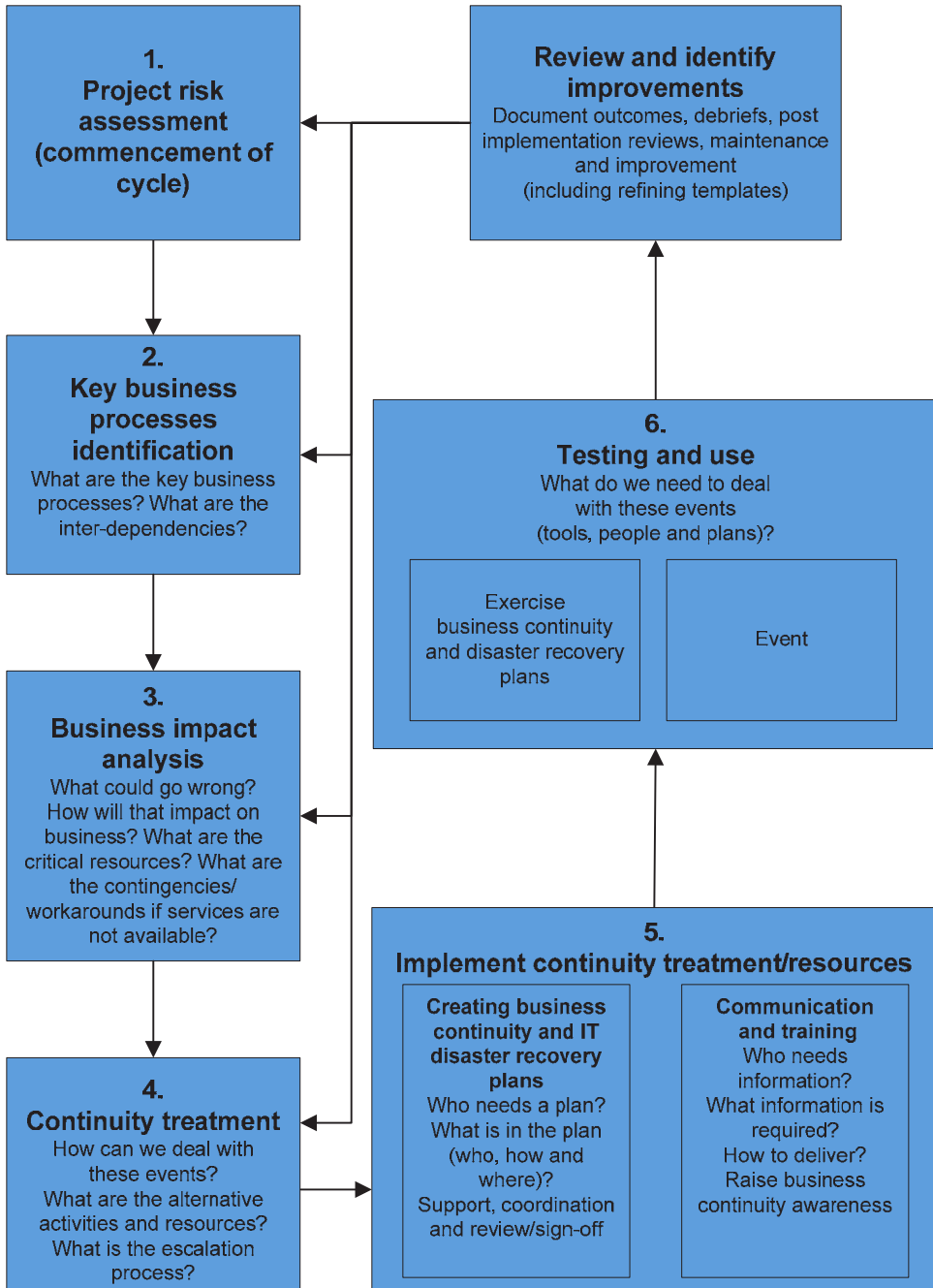
3.1 The 2000 ANAO BPG on BCM⁴⁷ presents a structured approach to BCM within a risk management framework. This involves identifying preventative treatments for continuity risks that can be routinely managed, and developing an organisation-wide business continuity plan to deal with the consequences should the preventative treatments fail.

3.2 The BPG outlines six steps in the BCM process that follow the development, implementation, testing and maintenance of a business continuity plan. The six steps were used to analyse Centrelink's implementation of its BCM framework and the application of these steps to Centrelink is depicted in Figure 3.1. Figure 3.1 also includes the review and identification of improvements that are implicit in the BPG model.

⁴⁷ Australian National Audit Office, ANAO Better Practice Guide—*Business Continuity Management-Keeping the Wheels in Motion: A Guide to Effective Control*, Canberra, 2000.

Figure 3.1

Business continuity management better practice process management in Centrelink



Source: ANAO analysis

Project initiation (Better Practice Guide Step 1)

Business continuity strategic planning

3.3 At the project initiation stage a plan should be prepared that documents the objectives, scope and boundaries of the BC planning project.

3.4 Centrelink has for many years had in place a BCM framework that has continued to evolve. At the same time, the services that Centrelink provides, and the supporting administrative systems, have also changed and there is a continuing need to ensure that, as this occurs, adequate consideration is given to new and emerging BC issues.

3.5 To improve its BCM framework, the BCCM Section produced a Strategic Plan for 2007–08. This was essentially its business plan to improve BCM throughout Centrelink and included measures such as improving the implementation of BC planning and testing. The plan was examined as part of the 2008 review of BC strategy⁴⁸ but has not been updated in the light of that review.

3.6 In relation to IT-related BCM, the ITSCM Team has also developed a strategy⁴⁹ aimed at improving IT-related BCM over the period 2007 to 2010. The Strategy, however, has not been endorsed by management and a plan for its implementation is yet to be developed. Further, the Strategy lacks a clear link with Centrelink's overall strategy and plan for BCM.

Project management

3.7 As new services are introduced or new processes implemented, BC impacts need to be considered. Under Centrelink's Project Management Framework, new projects are required to address BC as part of their Project Management Plans (PMPs) and, where needed, include treatments for any identified continuity risks.⁵⁰ To complete the BC component of a PMP, project managers are required to identify mission critical business elements and determine the impact on Centrelink's business operations should these elements be disrupted or lost. Project managers also conduct risk assessments

⁴⁸ Protiviti, *Review of Business Continuity Strategy for 2007–08* (April 2008).

⁴⁹ Centrelink, *IT Service Continuity Management Strategy, 2007–10* (Version 0.6).

⁵⁰ The Project Management Framework recognises that different projects have different levels of complexity. This will determine the level of detail to be included in the Project Management Plan (PMP).

of the threats to these processes and develop risk management plans for projects. The risk management template that is available for this purpose asks business managers to consider and document the strategies they have in place to address any continuity risks. Project managers are required to consult with, and receive sign-off from, the BCCM Section during this step of the process.

3.8 Most projects have an IT component and Centrelink has a well developed Operational Readiness Checklist (ORC) for IT-related projects that cover both risk management and business continuity considerations. The ORC provides IT project managers and/or change initiators in the agency with a list of checkpoints that need to be passed whenever they plan a change to Centrelink's IT system. The ORC is a critical part of the IT change management process in Centrelink.

3.9 Completion of the ORC has been mandatory for all new projects in Centrelink since 1 January 2005. It covers key components of the system development process and importantly includes a requirement that project managers receive a BC assessment by the BCCM Section, an IT service continuity assessment from the ITSCM Team and a risk management assessment from the Risk Management Section.⁵¹ In this regard the ORC acts as a useful tool for project managers in ensuring the project is considered broadly across the agency.

3.10 The ORC requires that project managers follow steps that are similar to those outlined in the BPG in relation to identifying key business processes and undertaking a business impact analysis (BIA). In particular, project managers are required to:

- carry out a risk assessment, which is an integral starting point for business planning and managing BC;
- undertake a BIA;
- develop appropriate treatment strategies for all identified risks;
- determine if a BC plan is required and, if so, ensure that the plan is aligned with the appropriate IT Disaster Recovery Plans; and

⁵¹ Where the ORC cannot be finalised and the project manager still wishes to proceed with the implementation, a residual risk assessment can be completed before release. Source: Centrelink—Operational Readiness Checklist.

- review relevant business continuity plans to ensure that the treatment strategies will achieve BC within the acceptable allowable outage timeframes.

3.11 As part of the ORC process, the ITSCM Team assesses projects according to operational readiness criteria, including whether:

- the project meets the required and agreed business recovery timeframes and IT recovery priority;
- the project complies with the IT Disaster Recovery Design Policy; and
- IT Disaster Recovery Plans are created and/or appropriately amended to reflect business requirements.

3.12 The audit team selected and reviewed five projects on the ORC database to assess whether BC and IT service continuity checkpoints had been passed.⁵² The selected projects had all completed the necessary checkpoints and the responsible project managers had comprehensively documented essential BC processes centrally on the *Teamroom*⁵³ ORC database. Centrelink advised that it is also seeking to ensure that, in future, project managers will record project documentation on its Project Register, since this ensures that documentation for all projects is readily accessible.

3.13 Centrelink has also been trialling the use of a specific template to assess the BC requirements for projects. As a separate risk management template is already available for projects, the ANAO suggests that Centrelink consider the value of combining or linking the two templates. This would help to strengthen the relationship between risk management and BCM and potentially simplify the work of project staff.

Key business processes identification and business impact analysis (Better Practice Guide Steps 2 and 3)

3.14 To ensure sufficient coverage of BC within an organisation, it is necessary to identify all key business services and their processes and then analyse the impact of their interruption in order to establish the maximum

⁵² These included two completed (Web Services for CCeS POS, National Emergency Call Centre Capability) and three active (Baby Bonus, DIAC Datalink Project, Refresh 1.3 Third party service portal) projects.

⁵³ A Lotus Notes application that Centrelink uses to support some processes where people across the agency work together.

length of time they can be interrupted before business objectives are compromised – the ‘maximum allowable outage’ (MAO).⁵⁴ Steps two and three of the BPG envisage that organisations will undertake an assessment of how critical each service is to the organisation’s function, identify their key business processes, document any concerns, priorities and expectations about them and derive MAOs for each process.

3.15 Centrelink does this by requiring each branch in its NSO to complete a BIA each year and for each new project. Centrelink also has in place arrangements for its IT processes, such as the IT Information Library (ITIL) framework, that complement the BIAs.

Business criticality reviews

3.16 A business criticality review allows an organisation to establish where its service risks exist, compare these risks to make an assessment of their relative importance and identify strategies to address them. Often a business criticality review is informed by business impact analyses that are undertaken at an individual service or business level.

3.17 An important part of a business criticality review is an assessment of the MAOs provided by the business. The MAOs identify the impact on the business when there is a business disruption to services for different periods of time. They provide an indication of the criticality of various services and therefore the urgency with which they need to be restored.

3.18 Centrelink last undertook a business criticality review in 2002.⁵⁵ The review involved 270 staff in 44 locations and identified key business processes and accompanying MAOs. There were, however, notable omissions including:

- a clear analysis of data and telecommunications systems as critical resources to support business processes;
- aspects of electronic service delivery; and
- the impact of an incident affecting an Area Office.⁵⁶

⁵⁴ Centrelink sometimes also calls the MAO the ‘maximum acceptable outage’ period.

⁵⁵ This review was conducted internally. Previous business criticality reviews in 1997 and 1998 were completed externally by a consultant.

⁵⁶ Australian National Audit Office, ANAO Audit Report No.9 2003–04, op. cit., paragraph 4.14.

3.19 Given that it has been seven years since a formal business criticality review has been undertaken for all business processes performed within the agency and there have been changes in Centrelink's business during this time, it is timely that Centrelink conduct another such review (refer Recommendation No.2).

Business impact analysis (BIA)

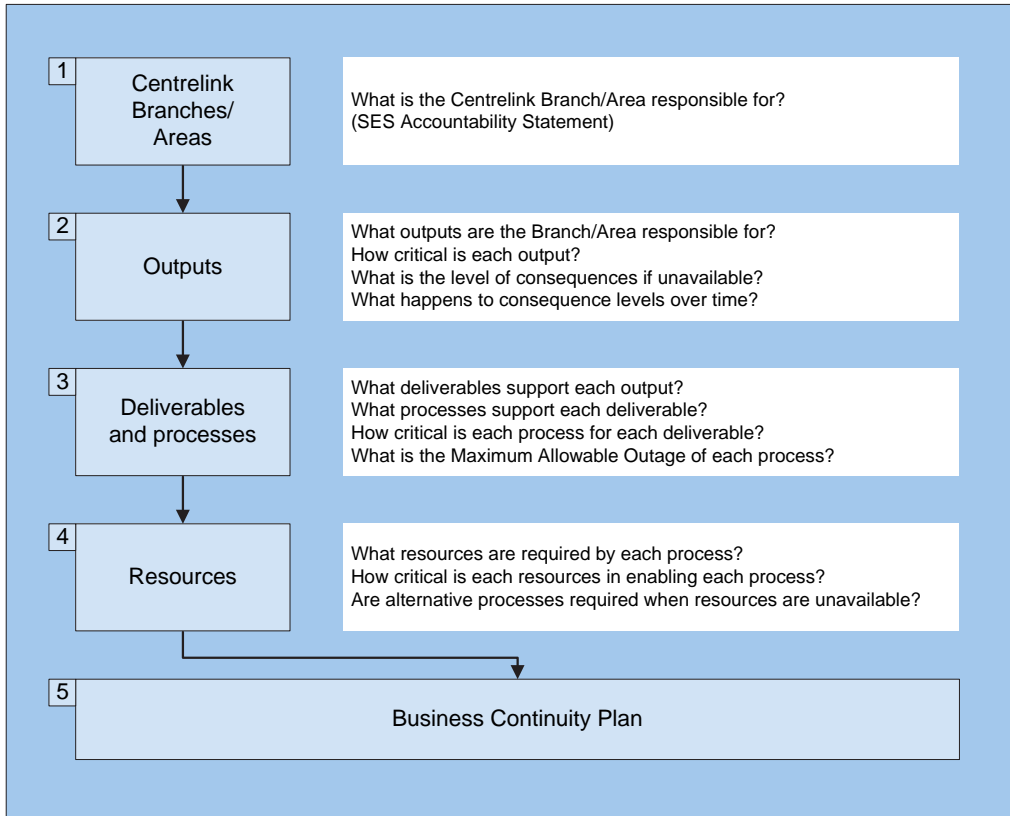
3.20 Since the 2002 review, Centrelink has required NSO branches to prepare an annual BIA. The BIA assesses the tangible and intangible impacts (consequences) of a business process (output/service) being affected or downgraded for different time periods.

3.21 Centrelink has developed a template to assist branches in completing a BIA⁵⁷, with the steps involved in developing a BIA depicted in Figure 3.2.

⁵⁷ Centrelink is currently reviewing this template.

Figure 3.2

Steps in the business impact analysis



Source: Centrelink’s BIA template

3.22 The BIA is intended to guide the development of business continuity plans (BCPs). Although the BIAs help to provide a better understanding of BC issues, Centrelink has yet to provide guidance to users on how to translate this work into the development of BCPs. This is discussed further in paragraphs 3.36 to 3.49.

3.23 According to Centrelink’s records, 24 out of 26 NSO branches completed BIAs in 2007–08,⁵⁸ while all 14 NSO Divisions completed BIAs in 2008-09.⁵⁹ The ANAO selected and reviewed a sample of the 2007–08 and

⁵⁸ Centrelink, *BIA Completion Rate*, 9 November 2007.

⁵⁹ Centrelink advice 7 May 2009. In 2008-09 compliance was reported at the Divisional level rather than Branch level as it was in 2007-08.

2008-09 NSO BIAs⁶⁰ from program, IT and corporate support areas and verified that they had been completed. The BIAs selected also generally demonstrated a useful assessment of the business processes that each branch administers and of their criticality.

3.24 While the BIAs had only been completed by Centrelink's NSO at the time of the audit, Centrelink advised that, by the end of June 2009, all Area Offices, CSCs and Call Centres will be required to complete them.⁶¹

Maximum Allowable Outage (MAO) periods

3.25 An important part of Centrelink's BIA process is the assessment of the MAOs relating to the services provided by each branch. Following the completion of individual BIAs, the BCCM Section collates the branch-assessed MAOs to provide a 'bottom-up' assessment of the criticality of Centrelink's services.⁶²

3.26 Centrelink has recognised that branches' analysis of the criticality of the services for which they are responsible needs to be complemented by a 'top-down' assessment of Centrelink's business priorities and key resources. Accordingly, in 2008, Centrelink endorsed seven BC priorities (refer Appendix 2) as a high level indication of critical services. The then Emergency Management Branch listed the MAOs identified by branches in 2007 under each of these as 'operational business continuity priorities'.⁶³ The effectiveness of this process, however, was limited due to:

- the seven key priorities being shaped at a very high level, for example, 'Delivery of Payments', and therefore they can cross many parts of the business;
- the lack of clarity in how an overall Centrelink-wide assessment of the relative criticality of processes and services is determined and the respective MAOs are agreed; and

⁶⁰ These covered most IT areas, a large number of program areas (DEEWR, FaHCSIA, Education, Employment & Disability Network, Network Support Tools and Seniors, Families & Customer Contact branches) and other areas such as Centrelink Call, International Branch and the Service Delivery Coordination Branch.

⁶¹ Centrelink advice 24 April 2009. On 5 June 2008, Centrelink further clarified that, by June 2009, BIA templates will be provided to ASOs, CSCs and Call Centres for use and that it now intends to provide workshops to ASOs, CSCs and Call Centres to assist in BIA completion for the 2009-10 financial year.

⁶² These were last completed in 2007. The 2008 assessments have not been completed.

⁶³ Centrelink Business Continuity Priorities October 2007 (Version 1.05, 1 April 2008).

- the lack of clarity surrounding the extent to which branch determined MAOs could be achieved.

3.27 Relying on individual branch analysis and high-level priorities without a central review mechanism can lead to a risk that gaps in the BCM framework are not considered or addressed. For instance, individual service MAOs may warrant review and alteration when compared to other service priorities in the business. Branches are unlikely to be able to factor this into their business impact analysis and resulting MAOs because their BIAs reflect individual branch priorities and understandings of agency processes, rather than agency-wide priorities and understandings of agency processes.

3.28 Accordingly, it is important that Centrelink is able to bring together the 'top down' and 'bottom up' approach to present a complete assessment of the organisation's key business processes and applicable MAOs. In this regard the ANAO notes that a mechanism for the central review and endorsement of MAOs exists within Centrelink through the work of the BCCM Section and the BCCM&S Sub-committee.

Recommendation No.2

3.29 In order to identify key business processes and provide for the regular comparative assessment of Maximum Allowable Outage periods (MAOs), the ANAO recommends that Centrelink:

- (a) commission a formal Business Criticality Review of its operations, including National Support Office, Area Offices and its service delivery channels; and
- (b) establish a process for the annual review and endorsement of MAOs determined by branches to ensure that they represent a collective view on the relative criticality of the services that Centrelink provides.

Centrelink Response

3.30 Agree.

Control of key IT business processes

3.31 Centrelink has a number of tools to assist it in documenting and managing key IT business processes. These include:

- an ITIL framework, or collection of best practices in IT Service Management, which provides a framework to improve capabilities and service management;⁶⁴
- an Enterprise Service Desk Incident and Problem Management suite of tools ('Service First'), which automates the management and monitoring of Centrelink's IT systems, particularly for newly developed systems;
- the 'Centrelink Repository', a central database holding documentation for services that need to be recovered quickly in the event of a crisis. It includes such things as procedure files, data files and data models for ISIS as well as midrange software; and
- the IT Services Catalogue,⁶⁵ which provides a useful listing of the IT services supporting the business of Centrelink and its clients. However, the Catalogue has not been maintained since 2006 and is to be replaced with a recognised ITIL Service Level Management (SLM) framework.⁶⁶

3.32 The IT Services Catalogue, when maintained, was used to:

- structure work plans according to services;
- record work efforts according to services;
- define agreed availability and outputs according to services; and
- align business criticality by services.

3.33 Centrelink's Planning and Demand Management Branch has commenced developing a comprehensive Customer Services Catalogue. This Catalogue, which is only at an early stage of development, would describe each of Centrelink's main business services, the related priorities and the processes underlying them. It has the potential to clarify the relationship between IT applications and business functions and to help ensure that business resumption priorities, as reflected in the MAOs, align with business needs. It would not, however, avoid the need for the IT Services Catalogue or its replacement.

⁶⁴ The ITIL framework was originally developed by the UK Office of Commerce in the 1980s.

⁶⁵ Centrelink, *IT Services Catalogue*, Version 6.1, July 2006.

⁶⁶ Centrelink advised on 18 April 2009 that it anticipates that a draft ITIL SLM framework will be completed in late 2009.

3.34 The ITSCM Team uses information from the IT Services Catalogue, the 2002 Business Criticality Review, NSO branches' BIAs and the ORC to prepare an 'I&T Service Recovery Priority List'.⁶⁷ This provides an indicative listing of priorities for recovery of IT Services in the event of a disaster and guidance to Centrelink management on appropriate resource allocations (for example, an immediate failover design may be most appropriate for priority one services only). It also suggests a disaster recovery testing frequency along priority lines.

3.35 The 'I&T Service Recovery Priority List' plays a fundamental role in assisting Centrelink to restore IT services in the event of a disaster. Underpinning it, however, is a Business Criticality Review conducted in 2002 (refer Recommendation No.2) and an unmaintained IT Services Catalogue. Therefore, given the increasingly limited value of the existing IT Services Catalogue, the ANAO suggests that Centrelink expedite the update or replacement of the Catalogue.

Design and implementation of continuity treatments (Better Practice Guide Steps 4 and 5)

Business continuity planning

3.36 A BCP is a collection of procedures and information that is developed, compiled and maintained in readiness for use in a business disruption event.⁶⁸ It addresses business disruption from the initial disaster response to the point at which normal business operations are resumed. It can include crisis response procedures such as emergency management plans and/or disaster recovery plans that are service area specific and include the detailed procedures to respond to, and recover from a business disruption.

3.37 An organisation with mature BCM processes will have developed its BCM framework towards an operating BCP. This involves business units within the organisation, in their BIAs, formally identifying and prioritising key business processes, risks to the continuity of those business processes and suitable continuity risk controls or treatments for these risks. A BCP should include procedures that will assist the organisation to maintain and test each

⁶⁷ Centrelink, *I&T Service Recovery Priority List Version 2.3*, August 2008.

⁶⁸ ANAO Better Practice Guide—*Business Continuity Management: Building resilience in public sector entities*, Canberra, 2009, p. 67.

risk control or treatment and include appropriate performance measurement and reporting processes.

Business continuity planning in Centrelink

3.38 Centrelink's Business Continuity Policy⁶⁹ sets out the roles and expectations of Centrelink managers and staff in regard to the continuity of Centrelink payments, services and key enabling resources. Under the Policy, all General Managers, National Managers, Area Managers, CSC Managers and Call Centre Managers are expected to develop and maintain BCPs for the payments, services and business functions for which they are responsible. The Policy also requires testing of those plans and the development of continuity response guidelines and processes. The Policy, however, is not being fully implemented due to the absence of BCPs for all payments, services and business functions.

Emergency management plans

3.39 As part of the BCM planning templates Centrelink promulgates for use across the agency,⁷⁰ the ANAO found that emergency management plans (EMPs) are used as a proxy for BCPs. EMPs (and the accompanying Recovery Guidance) have a focus on the initial crisis response phase and include crisis escalation and response procedures, key contacts and resources, and the identification of responsibilities for particular issues. Unlike BCPs, however, the EMPs do not identify and prioritise key business processes and include treatments to deal with any identified continuity risks. The ANAO notes that, before the introduction of EMPs in 2006–07, Centrelink did require business units to prepare a 'Business Continuity & Emergency Management Plan', which included Business Disruption Action Strategies to deal with identified continuity risks.⁷¹

3.40 EMPs had been completed by all Area Offices, CSCs and Call Centres and were held centrally by the BCCM Section. While not all NSO branches EMPs were held centrally by the BCCM Section, the ANAO requested and was

⁶⁹ Centrelink, *Business Continuity Policy 2007*, op. cit., p. 2.

⁷⁰ Centrelink, *Business Continuity Management Control*, 2008.

⁷¹ The EMP was also originally titled the 'Business Continuity and Emergency Management Plan', but renamed as the 'Emergency Management Plan' in 2007–08.

provided with copies of EMPs from different branches within NSO nominated by the ANAO.⁷²

3.41 The EMP templates for all business units followed a consistent format such as providing clear instructions to notify the CEO of significant business continuity or emergency/disaster situations; and the Network Coordination and Emergency Management Branch of all potentially significant failures or incidents. The plans list the emergency contact telephone numbers of all relevant NSO and Area staff.

3.42 The notification and escalation framework within the EMP template sets out four levels of notification for each resource interruption impact level: 'critical', 'high', 'medium' and 'low'.⁷³ The framework's principle is that when there is an interruption in the availability of a key enabling resource (or component of it), it is the responsibility of the resource owner (for example, the National Manager) to ensure that all those relying on the resource to deliver organisational objectives are appropriately notified. This initial notification should allow users of the resource to respond to the interruption by implementing planned contingencies.

Development of new business continuity plans

3.43 In addition to EMPs, and consistent with the BC Policy, the BCCM Section has been developing a separate BCP template for the use of NSO divisions and branches in the first instance, with the idea of later extending its use throughout Centrelink. Centrelink has advised that this template was completed in April 2009 and will be rolled out for use in the NSO divisions and branches during 2009-10.⁷⁴

3.44 While most business units in Centrelink are not preparing BCPs that address business continuity risks and treatments, the ANAO did identify two business units that had prepared BCPs and one Area Office that was working with a state emergency services agency to develop a BCP. Areas covered by one or both of the business unit BCPs included:

- identification of key business processes;

⁷² These comprised eight branches from IT divisions, program divisions and corporate divisions.

⁷³ Centrelink, EMP template, p. 6.

⁷⁴ Centrelink advice 5 June 2009.

- identification of key risks or incidents that may impact on those processes;
- risk treatments and restorative actions in a BC Action Plan; and
- provision for testing of the BCP.

3.45 The development and implementation of BCPs is a key element to improving Centrelink's ability to respond to business disruptions and in the context of BC planning, helping to instil a discipline that requires business units to identify:

- risks to the business/service and their impact, based on the BIAs; and
- risk treatments and business resumption tasks, both proactive and reactive tasks, to manage these risks that can then be tested regularly.

3.46 BCPs should be linked directly with the BIA process (and usefully also with other risk management planning). It is also important that, where needed, Centrelink identify timeframes for responding to incidents and business resumption processes, consistent with established MAOs. This is particularly important during the initial crisis response.

3.47 Further, in order to maximise the use and effectiveness of the BCPs, a high level of user acceptance of the planning and response templates is required. In this regard, the ANAO notes that:

- a June 2008 Centrelink Internal Audit Report found that:

Stakeholders have expressed concern over the lack of consultation with them regarding the design and usability of the BIA and other business continuity related templates. The majority of stakeholders were not aware of the existence of the Business Continuity Policy and Strategy.

While the templates were designed with the intention of capturing the necessary information, the minimal stakeholder consultation regarding the design has contributed to the difficulty using these templates, particularly by the IT stakeholders;⁷⁵

- staff in one Area Office visited during fieldwork indicated to the ANAO that they considered that the current EMPs did not fully meet their needs (for example, they did not include provision for response timeframes).

⁷⁵ Centrelink Audit Report, op. cit., June 2008, p. 20.

3.48 Once developed, the risk treatments and business resumption tasks in the BCPs are only likely to need minor modification each year, unlike the crisis response plan, which contains contact lists that will continue to require regular updates during the year. Once the BCPs have been developed, the focus can then be on testing the plans and developing a culture of BC readiness and performance improvement.

3.49 The introduction of BCPs across Centrelink does not replace the need for the business to have in place crisis escalation and response arrangements, similar to those in its existing EMPs. Rather, with the broader focus on the initial crisis response through to the resumption of business as usual activities, BCPs combined with EMPs (and other planning tools such as disaster recovery plans) form complementary components within the BCM framework.

Recommendation No.3

3.50 The ANAO recommends that Centrelink develop and promulgate a business continuity plan (BCP) template and require business units to develop BCPs that identify:

- (a) risks to the business/service and their impact, based on the respective business impact analysis; and
- (b) risk treatments and business resumption tasks to manage these risks, which can then be tested on a regular basis.

Centrelink Response

3.51 Agree.

IT disaster recovery plans

3.52 Centrelink has a large and sophisticated IT environment with the IT systems of the agency processing approximately:

- six billion transactions annually;
- 25 terabytes⁷⁶ of data per week; and
- 31 million telephone calls each year.

⁷⁶ A terabyte equals 1000 gigabytes or 10¹² bytes.

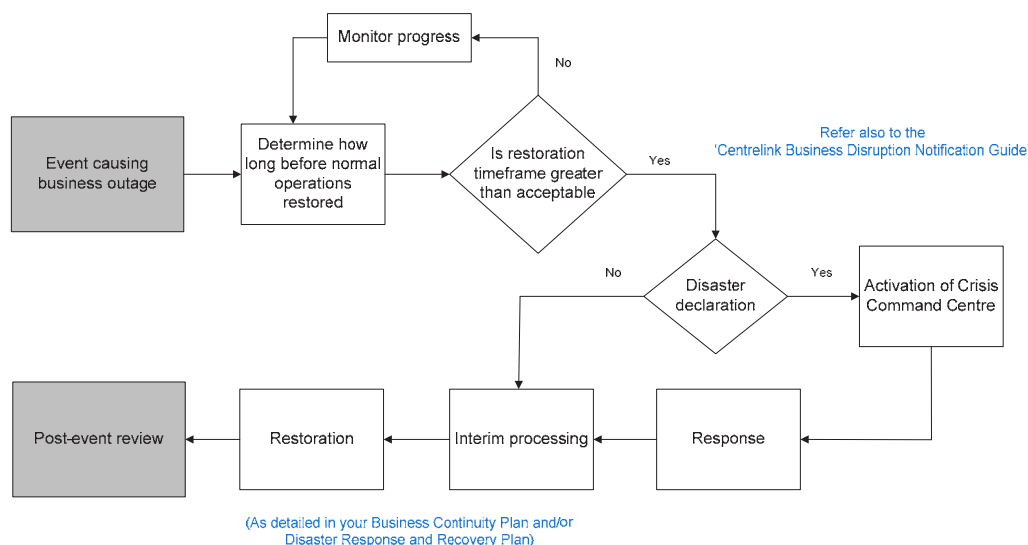
3.53 Centrelink’s core mainframe customer information system, namely the Income Security Integrated System (ISIS), processes 25 787 MIPS (millions of instructions per second) at peak capacity.

3.54 Centrelink operates two data centres; the Canberra data centre (CDC) at NSO and the Bruce data centre (BDC).

3.55 To ensure the continuing operation of its IT services, it is important that Centrelink maintains well developed and tested BC strategies, processes and procedures. Figure 3.3 describes steps to be undertaken by IT areas where there is a service disruption.

Figure 3.3

Steps to be followed in the event of a disruption in IT services



Source: Centrenet – IT Service Continuity Management Business Services

3.56 IT disaster recovery plans (DR plans) enable Centrelink to recover core parts of its IT infrastructure in the event of a disaster. They form part of the treatments that have been developed to meet identified IT continuity risks.

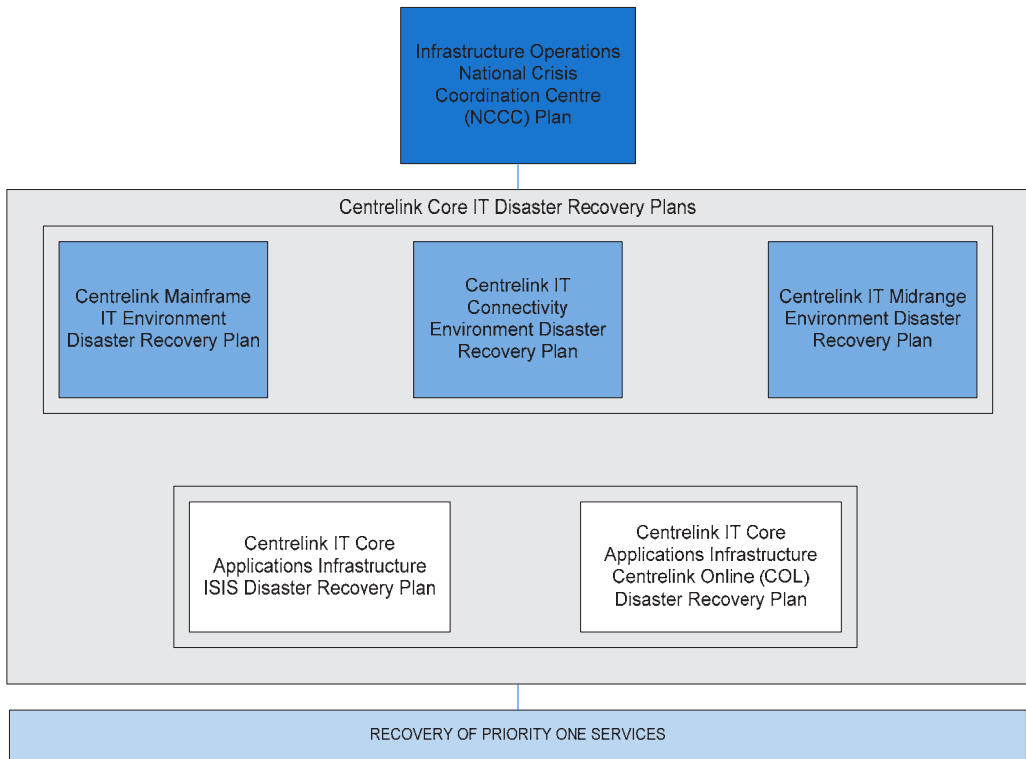
3.57 Centrelink does not have a single IT DR plan that applies to all IT architecture, applications and systems within the agency. Rather, it has a suite of infrastructure (mainframe, connectivity and midrange environment), core applications and IT security⁷⁷ DR plans. Plans relating to the DR of Centrelink’s

⁷⁷ Security Access Management, Gateway and Security Framework.

main IT infrastructure are depicted at Figure 3.4. An overview of these plans is at Appendix 3.

Figure 3.4

Centrelink’s IT disaster recovery plans



Source: Centrelink

3.58 The hardware and applications infrastructure core DR plans cover a number of business critical related services. These services are not only the backbone of the computing environment but enable the delivery of IT services. The plans cover, for example, a disaster being declared because of the complete loss of the BDC and the recovery of all BDC based ‘Priority One’ services at the CDC, and vice versa. As a result, there are two versions of each plan, making a total of 16 plans.

3.59 Each core DR plan is designed to outline the necessary steps to recover infrastructure in case of destruction. These steps include:

- an overview of the recovery strategy;
- detailed recovery activities as outlined in the recovery strategy; and
- instructions and a template for event and issue logs.

3.60 Centrelink advised the ANAO that 12 of 16 identified core DR plans had been completed, and that work is under way to ensure that all plans are up-to-date by the end of September 2009, in preparation for testing commencing in October 2009.⁷⁸

3.61 The ANAO reviewed the 12 core DR plans that had been completed. Each plan included review and sign-off by affected stakeholders and/or those responsible for the plans. The plans also adopted a consistent and logical approach and provided easy-to-follow, step-by-step guidance to recovering IT systems following a disaster, including advice on other organisations that should be consulted.

3.62 In completing, updating and testing the DR plans it is important that the BCCM&S Sub-committee is briefed on the progress and outcomes so it can assure itself that these important components of Centrelink's disaster recovery arrangements are up-to-date and being regularly tested.

IT business continuity risks

3.63 In the examination of Centrelink's IT infrastructure and applications in the previous audit there were a number of risks and/or opportunities for improvement identified. Three of those risks related to Centrelink's data centres, off-site data storage and IT back-up arrangements.

3.64 The risks relating to the data centres and off-site data storage included the potential loss of a data centre(s) from a natural disaster, the location and capacity constraints of the data centres and the contents and protection of the off-site data storage facility. In recent years, Centrelink has undertaken ongoing work in this area including commissioning external consultants to undertake a hazard analysis for its two data centres and the off-site data repository⁷⁹ and present options for a future data centre strategy.⁸⁰

3.65 Through a combination of internal work and improvements and the assurances provided by the external reviews, Centrelink continues to monitor and respond to issues as they arise in these areas. In this regard Centrelink has

⁷⁸ Centrelink advice 24 April 2009.

⁷⁹ Risk Frontiers, *Hazard Analysis for Centrelink's Canberra Data Centres and Off-site Storage Facilities*, June 2005.

⁸⁰ IBM Global Services, *The Enterprise Data Centre of the Future: Centrelink Data Centre Strategy 2008-2028*, June 2008.

been examining options to address the urgent capacity constraint on its data centres and the risks to business continuity that it poses. Centrelink has developed a business case for consideration by Government with the options having regard to the recommendations of the Gershon Report⁸¹ for consolidation of data centres across agencies.

3.66 Centrelink's mainframe storage and back-up practices are mature. Strategy and procedures have also been developed for the midrange environment and these are still maturing. Centrelink has a comprehensive enterprise data storage management policy, supported by a guide, specific strategies and procedures. Additionally, a project currently underway to reconfigure Centrelink's ISIS environment will have a significant impact on how Centrelink handles data back-up into the future.

3.67 Further discussion of these IT-related issues is provided at Appendix 4.

Testing and maintenance of plans (Better Practice Guide Step 6)

3.68 Once BCPs have been implemented it is important that they are maintained and the continuity treatments are tested on a regular basis. The ANAO examined Centrelink's process for testing its BC and DR plans and how these plans were maintained over time.

Business continuity plans: testing and in practice

3.69 The BPG describes various levels of testing that an organisation can undertake to validate its BCPs. These range from paper based reviews of resource requirements to virtual or real live simulation of disruption events. Such rehearsals not only confirm the validity of the plans, they provide opportunities to improve them. They are also a training tool, helping staff to become familiar with the plans and their roles and responsibilities when business continuity disruptions occur. The simulations can also help improve communication between the people responsible for performing business recovery actions.

3.70 In recent years Centrelink has conducted some limited BC testing, which has tended to be on an ad-hoc basis rather than an agreed forward

⁸¹ Gershon, P, *Review of the Australian Government's Use of Information and Communication Technology*, Commonwealth of Australia, 2008.

program designed to cover the spectrum of the business. Due to the reliance on EMPs rather than BCPs in the testing, it has mainly focused on the initial response to a disaster rather than the efficacy of the continuity treatments.

3.71 Most recently, beginning in March 2008 (with the assistance of a consultant), Centrelink commenced a series of desk-top BC scenario simulation exercises with Area Offices and CSCs. Centrelink has now developed a forward testing program for 2009 that provides for the completion of these exercises in all Areas. Centrelink advised the ANAO that future exercises will be conducted by staff in Centrelink's BCCM Section or by Area Office staff (for exercises at CSCs within their Areas).

3.72 As BCPs are developed, Centrelink will also need to use testing exercises to determine how useful and accurate the plans are and what further preparations (such as work-arounds) the Area Offices and CSCs may need to undertake to ensure the continued provision of services to the public.

3.73 To improve BCM testing practices, it is important that Centrelink maintain an annual program of simulation and planning assessment exercises. These regular exercises should include minimum standards that not only guide anticipated outcomes but also help embed a BC culture in the organisation. For example, each Area/CSC should conduct on an annual basis, at least one simulation exercise in a format that is approved by the BCCM Section. These exercises can then be evaluated and reported on to ensure that lessons learnt from them are used to further improve Centrelink's BCM framework.

3.74 In addition to reviewing Centrelink's testing of continuity plans, the ANAO examined a number of real life situations in which Centrelink's services had been disrupted and continuity plans were put into action. In each case Centrelink's response was appropriate. For example, after a CSC in the Newcastle region was flooded, Centrelink established a temporary shopfront and arranged for other services, such as back-end processing, to be undertaken by other CSCs. Also, after an office was flooded in Mackay, Centrelink staff acted quickly to remove and dry wet carpets and restore the office, so as to minimise the disruption to customers.

Business continuity plan maintenance

3.75 The structure of the EMP template provides for EMPs to be updated every six months, although contact lists are expected to be maintained and updated on a more regular basis.⁸²

3.76 Once a BCP template has been developed, Centrelink will need to ensure that these are updated annually and put in place processes to allow the BCCM Section and, where necessary the BCCM&S Sub-committee, to monitor the completion, maintenance and adequacy of the plans.

IT disaster recovery testing and maintenance

3.77 The ITSCM Team is responsible, in consultation with relevant stakeholders in technical areas, for IT DR testing, including:

- scheduling the testing timetable and coverage;
- developing test plans;
- conducting tests; and
- post-implementation review (PIR) reporting as part of IT balanced scorecards to the IT Committee.

3.78 The DR test plan template provided a clear framework and specific steps for testing IT recovery that were based closely on the core DR plans.⁸³ Test exercise tasks detailed pre-test tasks, test exercise activities (based on DR plan steps) and post-test tasks. All tasks were clearly presented and allocated to responsible personnel/areas.

3.79 The ANAO examined all IT DR tests planned and conducted during the 14 month period from September 2007 to November 2008. It reviewed the overall testing regime of DR plans for frequency; comprehensiveness of test plans and test procedures; timeliness in rectifying/follow-up of issues arising from testing; and reporting. It found that:

- while Centrelink does have a schedule of IT tests, not all of these are being conducted in a timely manner. For example, the IT Balanced Scorecard reports to the IT Committee on DR for the March 2008 and

⁸² Centrelink, EMP template checklist, p. 18.

⁸³ The test plan requires identification of the IT core plan and activity to be tested; test objectives; success criteria; scope and constraints; personnel and skill sets required; and stakeholders.

June 2008 quarters indicated that 11 per cent and 33 per cent respectively, of planned DR plan tests were completed. This was well below Centrelink's long term strategic target that 100 per cent of IT DR plans for critical business systems are developed and tested; and

- there was no evidence of testing of the IT security environment.

3.80 Centrelink advised the ANAO that its ability and capacity to conduct DR tests generally depends on the production schedule of releases, emergency fixes and availability of relevant technical staff. IT production and emergency priorities take precedence over DR tests. While recognising this, it remains essential that IT DR plans for critical business systems, such as Centrelink's Income Security Integrated System (ISIS),⁸⁴ are tested regularly in environments which as closely as possible resemble those of production to provide Centrelink confidence of its BC capability in the event of disaster.

3.81 During the audit, the ANAO attended a simulated 'desk-top' exercise conducted by the IT Business Systems Division (ITBSD). The exercise objective was to gauge the robustness of ITBSD's incident management process, particularly how teams interact with each other. The exercise was internal to the division and involved many sections. The exercise confirmed ITBSD's ability to deal with major incidents/crises and identified some areas for improvement.

3.82 An area identified for improvement was the maintenance of documentation. Some teams maintained extensive contact lists but did not maintain specific procedural documentation; some stored documentation only in the shared drive that might not be readily available in a crisis, and some seemed to have adequate BC and/or standard operating procedures and succession planning in place. The exercise also identified how other areas would need to be involved in the resolution of the crisis.

Testing and maintenance of plans conclusion

3.83 Centrelink has many skilful, knowledgeable and committed staff that can help to ensure smooth and timely business resumption when disruptions occur. There are, however, limitations to this, and there is a need to have a more rigorous program of testing BC plans and other continuity situations.

⁸⁴ A test of Centrelink's ISIS system was conducted on 7 February 2009. The previous test was conducted in 2004.

Preparing plans and testing responses to simulated crisis events that require a BC response help to ensure that a culture of BC is fostered in the agency. Additionally, the forward planning involved in this activity should help Centrelink to reduce the likelihood and impact of business disruptions.

3.84 Given the importance of regular and comprehensive BC testing to an organisation such as Centrelink, it is essential that there are mechanisms in place to oversight the test program and its implementation as well as use the results to identify areas for improvement. Accordingly, the ANAO considers that the BCCM&S Sub-committee, as the central governance committee for BCM, should endorse an annual test program for BCPs and DR plans for all services or systems (such as the ISIS system) that the agency has assessed as being critical. Further, the Sub-committee should then be provided with performance reports on the completion and key results from such tests.

Recommendation No.4

3.85 The ANAO recommends that the Business Continuity, Crisis Management and Security Sub-committee:

- (a) endorse an annual program of scheduled testing for business continuity plans, including relevant Disaster Recovery Plans for all services and systems assessed by the agency as being business critical; and
- (b) receive performance reports on the completion and key results of plan testing.

Centrelink Response

3.86 Agree.

Business continuity management training

3.87 In addition to testing BCPs, it is also important that Centrelink staff receive BCM training in order to build and improve their understanding and skills.

3.88 Training for Centrelink staff in BC preparedness is conducted by Comcare, as part of its regular training courses for APS staff. The Comcare course seeks to:

- explain BCM and insurance in the context of the Australian Government sector;

- describe the process of risk management and its relationship with BC and insurance;
- outline the key elements of a BC plan;
- explain the linkages between disaster recovery, BC planning and crisis management; and
- describe how to accurately estimate property and business interruption limits.

3.89 Despite having the course in place, the ANAO found that the BCCM Section does not coordinate or monitor BC training requirements, other than for the Network Coordination and Emergency Management Branch. Instead, in the absence of a targeted approach to developing BCM capability levels across the organisation, it is left to the discretion of individual branches and staff to identify training needs and to self nominate to undertake the Comcare course.

3.90 The risk with this approach is that there is limited analysis undertaken to determine the level of BCM skills and knowledge across the broader Centrelink network or the effectiveness of the course in meeting the desired outcomes. In the absence of this information, it is difficult to fully assess the effectiveness of the current arrangements and whether all BCM training needs are being met.

3.91 The ANAO suggests that Centrelink could improve the current BCM training arrangements through better:

- identifying the BCM skills and understanding required by officers across the network (particularly those outside the BCCM Section with a direct interest in BCM issues); and
- monitoring of the effectiveness of the course conducted by Comcare in meeting Centrelink's BCM training needs (i.e. improving officers' skills and understanding).

Review and improvement

Performance measurement

3.92 Monitoring and review of BCM performance is important to ensure that BC processes are working effectively. At its most basic, this process should include a system of regular reporting to management against agreed performance indicators or targets.

3.93 The BCCM&S Sub-committee is provided with regular reports on BCM performance, however, reports are not based on identified performance measures. Rather, they provide a descriptive account of current developments and issues. Conversely, the IT Committee is provided with regular reports on IT BCM that are based on the IT Balanced Scorecard and include some measures such as the testing of completed IT DR plans.

3.94 The absence of performance measures and reporting against them (other than for IT) means that it is not possible to easily assess the performance of Centrelink's implementation of BCM policy and procedures. Further, the different treatment and reporting of IT BCM performance limits the ability of the organisation to gain an agency-wide view of BCM.

3.95 BCM measures Centrelink could consider adopting include:

- the number/percentage of business units⁸⁵ that have completed (and lodged with the BCCM Section) their BIAs, BCPs and crisis response plans;
- the number/percentage of business units that have completed a testing of their BCPs and crisis response plans and the results of those tests;
- the number/percentage of key identified processes where satisfactory BC strategies have not yet been developed and the steps being taken to both mitigate the risks and put in place appropriate strategies;
- completion of annual consolidated BIAs; and
- the number of staff who have completed BCM or emergency management training.

3.96 While performance reports should be developed, care should also be taken to ensure that performance measures are well defined, targeted and based on reliable data. For example, Centrelink's long-term target for IT DR plans is that tested IT DR plans must exist for all critical business systems.

3.97 Reports to the IT Committee use a traffic light system – 'Green' (100 per cent), 'Amber' (80 per cent to <100 per cent) and 'Red' (<80 per cent) – to denote performance in completing and testing core DR plans. Table 3.1 shows that the IT DR Plan target had not been fully met as at 30 June 2008. While the completion rates in Table 3.1 were correctly identified

⁸⁵ Business units include NSO branches, Area Offices, Customer Services Centres and Call Centres.

as 'Amber' (for completion of DR plans) and 'Red' (for testing of DR plans), the overall summary rating for the completion and testing of DR plans in the report to the IT Committee was 'Amber' (making it appear that the low level of testing of the plans is a matter of less concern).

Table 3.1

IT Balanced Scorecard – Ratio of disaster recovery plans developed for IT and business services to total required for Quarter 4, 30 June 2008

| DR Plan Development 07/08 | Planned | Completed | Planned 4 th Quarter | Completed 4 th Quarter | % Completed |
|--------------------------------|---------|-----------|---------------------------------|-----------------------------------|-------------|
| Development of DR Plans | | | | | |
| Identified Core DR Plans | 16 | 12 | N/A | N/A | 75% |
| Identified Core DR Test Plans | 9 | 8 | 9 | 8 | 88% |
| DR Plan Testing | | | | | |
| Testing of Core DR Test Plans | 9 | 3 | 3 | 2 | 33% |

Source: IT Committee Report 28 August 2008

3.98 The ANAO examined IT Committee minutes for the period from June 2008 to October 2008 and found no issues and/or concerns raised by the Committee regarding non-achievement of the testing of core DR plans, despite the DR testing measure being consistently red (33 per cent). The reason for this may relate to the way that these measures are reported. Combining 'development' and 'testing' of DR plans into a single performance measure in this instance can obscure a particular BC weakness that exists in relation to inadequate DR testing.

3.99 Accordingly, there would be merit in Centrelink reviewing the presentation of the IT Balanced Scorecard results so as to improve the visibility of key issues that the IT Committee should be made aware of. Further, while quantitative measures are easy to monitor, the existing measures could also be supplemented by qualitative measures (such as level of satisfaction with preparedness for disasters) to provide a complete picture on the health of BC in the particular area.

Post-implementation reviews

3.100 Centrelink undertakes PIRs of significant continuity incidents, such as those affecting Centrelink's IT systems in 2007 and 2008, and its IT DR plan

tests. This is to ensure that lessons learnt are identified and applied to future responses. However, PIR reports of IT-related continuity incidents have been reported to the IT Committee and not necessarily also to the BCCM&S Sub-committee. Consistently providing reports on the findings of PIRs on BC incidents, including IT incidents, and the implementation of approved recommendations to the BCCM&S Sub-committee would increase the level of assurance that PIR findings and recommendations are being considered in the context of Centrelink's overall BCM framework.

3.101 The ANAO noted that Centrelink had improved its PIR template for testing of IT DR plans. The 2008 PIR testing template was more structured and informative than that of 2007. It contained a number of useful elements, such as success criteria, scope, constraints, findings/issues and resolution strategies. However, the templates did not provide for:

- assessment of whether success criteria had been met;
- setting completion timeframes for the resolution strategies;
- allocating issues and resolution strategies identified in the reports to appropriate personnel/areas for resolution/follow-up; and
- review and/or sign-off of the PIR.

3.102 Accordingly, the ANAO suggests that Centrelink consider introducing these elements to future iterations of the PIR testing template.

Recommendation No.5

3.103 The ANAO recommends that Centrelink:

- (a) develop performance measures against which its business continuity management preparation and response can be regularly monitored and assessed by the Business Continuity, Crisis Management and Security Sub-committee; and
- (b) provide reports to the Business Continuity, Crisis Management and Security Sub-committee on the findings and implementation of the recommendations of post-implementation review reports on business continuity incidents, including IT-related incidents.

Centrelink Response

3.104 Agree.

4. Update on Centrelink's Response to ANAO Audit Report No.9 2003–04, Business Continuity Management and Emergency Management in Centrelink

This chapter examines the ANAO findings against the recommendations made in ANAO Audit Report No.9 2003–04, Business Continuity Management and Emergency Management in Centrelink.

Introduction

4.1 In 2003–04, the ANAO completed an audit that examined Centrelink's BCM and EM framework and its implementation. The audit found that Centrelink generally had an appropriate framework for BCM and EM, and that this effectively addressed the main elements of BCM outlined in the better practice literature. However, it also found that there were a number of areas in which improvements could be made. The ANAO made eleven recommendations and a number of suggestions to improve the implementation of BCM and EM in Centrelink. Centrelink agreed to the eleven recommendations.

4.2 As the community recovery aspect of emergency management has been separated from this report (refer paragraph 8), Recommendation No. 11 from the previous audit is not considered in this report.

Summary and assessment against previous audit recommendations

4.3 Centrelink has fully implemented five of the recommendations (Nos. 2, 3, 5, 8 and 10) and partially implemented five of the recommendations (Nos. 1, 4, 6, 7, and 9) of the previous audit.

4.4 The following provides the ANAO's assessment of Centrelink's implementation of the 2003–04 audit report recommendations with references to the detailed findings from this audit.

Overarching management and quality control of business continuity management and emergency management

Findings of the previous audit

Overarching management and quality control of BCM and Community Recovery

A more comprehensive and structured system of central guidance, support, oversight, analysis and reporting would add value to Centrelink's BCM and EM processes by improving performance and enhancing assurance of an effective response to any crisis.

Recommendation No. 1 of the previous audit

The ANAO recommends that Centrelink develop a comprehensive, formal system of overarching management and quality control of business continuity management and emergency management. In addition to providing guidance, support and oversight of business continuity management and emergency management, this system may also involve:

- implementing recommended minimum standards for plan maintenance, rehearsal and training for all relevant areas throughout Centrelink;
- monitoring and reporting performance against these standards; and
- undertaking regular formal analysis of this centrally collected information by a central business continuity management unit, to assist in quality control and to aid dissemination of better practices.

Findings of this audit

4.5 Centrelink has partially implemented Recommendation No. 1 of the previous audit. Centrelink has established an overarching management and quality control framework for BCM and EM. Centrelink has not, however, implemented minimum standards for plan maintenance, rehearsal and training for all relevant areas, and there is scope to improve performance monitoring and reporting.

4.6 This is discussed further in Chapter 2 at paragraphs 2.2-2.16 and Chapter 3 at paragraphs 3.69-3.99.

Business continuity management guide

Findings of the previous audit

Business continuity management guide

The ANAO had some difficulty in quickly obtaining information outlining comprehensively but succinctly Centrelink's BCM framework and processes.

One of the objectives of the previous audit was to establish whether Centrelink's BCM and risk management frameworks were complementary.⁸⁶ The audit concluded that risk management and BCM in Centrelink were well aligned at both overarching and operational levels, but there was scope for further improvement.

Recommendation No. 2 of the previous audit

The ANAO recommends that Centrelink produce a business continuity management guide that:

- a) outlines the main elements of its business continuity management framework, such as:
 - its strategic approach;
 - roles and responsibilities;
 - coverage;
 - rehearsal program;
 - plan maintenance and development program;
 - awareness raising and training;
 - performance monitoring; and
 - integration with other risk management efforts.
- b) incorporates Centrelink's emergency management framework and processes, emphasising the alignment between business continuity management, emergency management and risk management; and
- c) is regularly updated.

Findings of this audit

4.7 Centrelink has implemented Recommendation No. 2 of the previous audit, however, the ANAO considers that there remains scope for further improvements.

4.8 In relation to parts (a) and (c), Centrelink published its BCM Policy and supporting tools and resources in 2005. While many of the original booklets are still in use they have not been updated since 2005.⁸⁷ However, Centrelink now maintains its BCM and EM documentation on its Intranet and updates this information on a periodic basis. The BCM & EM documentation on the Intranet includes details of Centrelink's BCM Policy, BCM priorities and its BCM and

⁸⁶ The first criterion for the previous audit was to establish whether Centrelink's BCM framework was integrated into its risk management framework so that BCM focuses on the main business risks and critical business functions.

⁸⁷ Centrelink advised the ANAO on 16 April 2009 that the booklets are now being withdrawn.

EM program, however, there remain some areas, such as a rehearsal program and performance monitoring, that require further attention (refer paragraphs 3.68-3.84 and 3.92-3.102).

4.9 In relation to part (b), Centrelink's documentation incorporates its BCM and EM framework and processes, and emphasises the link with risk management. There is scope, however, to further improve the clarity of the framework and its associated documentation (refer paragraphs 2.30-2.36); and the coordinated implementation of BCM, EM and risk management arrangements (refer paragraphs 2.13-2.16).

Oversight of business continuity treatments

Findings of the previous audit

Oversight of BC treatments

The ANAO considered that the lack of central recording and oversight of the BC elements of new project plans had contributed to a lack of effectiveness of the process to address BC for new projects.

Recommendation No. 3 of the previous audit

The ANAO recommends that, in order to ensure continuity treatments are adequately addressed for new projects, Centrelink:

- a) centrally record the business continuity sections of project plans to provide the capacity for subsequent analysis of the business continuity provided; and
- b) institute an oversight function to check that business continuity treatments for new projects have been undertaken in accordance with the relevant section of each project plan.

Findings of this audit

4.10 Centrelink has implemented Recommendation No. 3 of the previous audit. Centrelink's Project Management Framework requires new projects, where appropriate, to address BC as part of their Project Management Plan (PMP). Centrelink has also implemented an 'Operational Readiness Checklist' for projects that include an IT component to ensure that as part of project planning BC considerations and treatments are addressed.

4.11 This is discussed further in Chapter 3 paragraphs 3.7-3.13.

Planning templates

Findings of the previous audit

Planning templates

The previous audit found that plans at the National level generally adhered to better practice guidelines, however, the plans used in the wider network (for example, Area Offices and CSCs) varied considerably. The plans used for Area Offices and CSCs had a range of formats, names and purposes and did differentiate between responses to local community emergency and responses to disruptions to Centrelink's own operations. Many of the local office plans focused solely on their response to broader community emergency needs.

Recommendation No. 4 of the previous audit

The ANAO recommends that Centrelink revise its templates for continuity plans in the network: to improve consistency; clearly differentiate business continuity from community emergency response; and improve linkages between Customer Support Centres, Area Support Offices and the National Support Office.

Findings of this audit

4.12 Centrelink has partially implemented Recommendation No. 4 of the previous audit. Centrelink has improved the consistency in some of its continuity planning templates, for example, there is a standard template for emergency management plans (EMP) that all areas of Centrelink are required to complete and keep up to date.

4.13 The EMP templates, however, have a focus on the initial crisis response to disasters. They do not identify continuity risks and proposed treatments (refer paragraphs 3.38-3.49). These are critical components of a business continuity plan (BCP). Continuity risks identified through BIAs are expected to lead to the development of BCPs that identify treatments for these risks. Completion of BIAs has also not been mandated across the organisation, although Centrelink advises that it has plans to do so (refer paragraph 3.24).

Training and accreditation of Centrelink staff

Findings of the previous audit

Training and accreditation of Centrelink staff

Centrelink did not have a formal approach to training staff in BCM and EM. Instead, Centrelink typically had an ad hoc approach to such training.

Recommendation No. 5 of the previous audit

The ANAO recommends that Centrelink implement a structured process to develop a competency and learning framework to ensure that relevant Centrelink staff:

- a) have appropriate business continuity management skills; and
- b) are appropriately trained and accredited for required special and community emergency response roles.

Findings of this audit

4.14 Centrelink has implemented Recommendation No. 5 of the previous audit. Centrelink relies on a course conducted by Comcare for training staff in BCM preparedness. There remains scope, however, for Centrelink to better identify staff BCM training needs and in turn monitor the effectiveness of the existing training arrangements in meeting these outcomes (refer paragraphs 3.87-3.91).

Control of IT applications

Findings of the previous audit

Control of IT applications

Centrelink documentation supporting principal applications was largely incomplete, inconsistently defined, improperly dated and relatively inaccessible. There was often little explanation of the relationship between applications and business functions. Without such documentation, a risk existed that incorrect understanding of the IT applications will compromise continuity and capacity to recover quickly from interruptions.

Recommendation No. 6 of the previous audit

The ANAO recommends that, to aid business continuity, Centrelink:

- a) review and update documentation for its principal applications on a program and system level, as part of its system development / change control methodology and in conformance with industry standards and timeframes, to reflect the current nature and functionality of those applications;
- b) ensure system development / change controls procedures reflect continuity considerations with respect to the applications; and
- c) clarify the relationship between applications and business functions.

Findings of this audit

4.15 Centrelink has partially implemented Recommendation No. 6 of the previous audit.

4.16 Centrelink has implemented part (a) by introducing the IT Information Library (ITIL) framework and 'Service First', an Enterprise System Desk Incident and Problem Management suite of tools that automates the management and monitoring of Centrelink's IT systems. It has not, however, fully implemented part (c) because its control system to clarify the relationship between applications and business functions, an IT Services Catalogue, is now out-of-date (refer paragraphs 3.31-3.35).

4.17 In response to part (b), Centrelink introduced the Operational Readiness Checklist, which provides IT project managers and/or change initiators in the agency with a list of checkpoints that need to be engaged

whenever they plan a change to Centrelink's IT system. This is a critical part of the IT change management process (refer paragraphs 3.8-3.12).

IT business continuity plans

Findings of the previous audit

IT business continuity plans

The ANAO considered that Centrelink needed to extend the criticality analysis in the *Business Criticality Review* to all important applications and then implement appropriate continuity and recovery plans.

Plans for the mainframe environment were narrowly defined. For example, the *Centrelink Business Disruption Data Centre Technical Recovery Manual* was not a BCP. Rather, it was, as it described itself, 'a reference guide to the recovery and restoration of Data Services in the event of the loss of services at either of the Data Centres'.

The ANAO considered that Centrelink had not adequately addressed BC for its mid-range equipment and network environments.

Recommendation No. 7 of previous audit

The ANAO recommends that Centrelink review existing business continuity plans and, where they do not exist, consider preparing comprehensive business continuity plans for:

- a) principal information and technology applications;
- b) its two data centres in Canberra; and
- c) all major hardware and system software components of its operations.

Contingencies should be identified, such as alternative resources, facilities and respective business activities, to enable the continued functioning of particular applications and infrastructure.

Findings of this audit

4.18 Centrelink has partially implemented Recommendation No. 7 of the previous audit. Centrelink has identified the need for 16 IT disaster recovery (DR) plans covering a range of infrastructure and core applications.⁸⁸ These DR plans detail the steps to be taken in recovering the core IT applications and infrastructure and producing two versions of each plan provides for the recovery of 'Priority One' data in the event of the complete loss of either of its two data centres.

4.19 The DR plans, with the exception of the IT security plans, have been regularly reviewed by the ITSCM Team. The DR plans, however, have not been regularly and comprehensively tested on an annual basis and Centrelink has not consistently achieved its IT balanced scorecard target on the ratio of

⁸⁸ The DR plans cover the aspects that would be included in a business continuity plan. Therefore the ANAO has determined that the DR plans have the same function as a business continuity plan, in the terms of Recommendation No. 7 from the previous audit.

disaster recovery plans developed and tested to total required (refer paragraphs 3.52-3.62).

Possible loss of both data centres and off-site back-up storage

Findings of the previous audit

Possible loss of data centres and off-site back-up storage

The 2003 ACT firestorm highlighted the possibility of total devastation of both data centres and the off-site back-up storage facility in Canberra as real risks to be considered by Centrelink. Centrelink does not periodically assess the contents, environmental protection and security aspects of its offsite back-up storage facility.

Recommendation No. 8 of the previous audit

The ANAO recommends that Centrelink:

- a) consider developing formal contingencies to implement in the event of destruction of both data centres and its off-site back-up storage facility;
- b) consider the limitations associated with the location of the off-site back-up storage facility; and
- c) periodically, at least annually, assess the content, environmental protection and security aspects of off-site back-up storage.

Findings of this audit

4.20 Centrelink has implemented Recommendation No. 8 of the previous audit.

4.21 In relation to part (a), Centrelink considered the need for formal contingencies in the event of destruction of both data centres and its off-site back-up storage facility, but decided not to develop contingencies on the basis of findings from a report completed in June 2005 that indicated the likelihood of their simultaneous destruction is very remote (refer Appendix 4).

4.22 In relation to part (b), Centrelink commissioned a 'Mainframe Recoverability Assessment' in 2004, which examined the off-site storage process in the context of Centrelink's IT disaster recovery strategy (refer Appendix 4).

4.23 In relation to part (c), the June 2005 report on the data centres also examined the environmental protection at Centrelink's off-site storage facility. It concluded that the risks were low, although the ANAO notes it did not provide a comprehensive assessment of the control procedures at the facility. Based on the risk assessments Centrelink has undertaken, it does not consider it to be an operational requirement to undertake annual reviews of its back-up

storage.⁸⁹ Notwithstanding this, it remains important that Centrelink continue to assess the content, environmental protection and security aspects of its off-site back-up storage on a regular basis.

Records management

Findings of the previous audit

Records management

Although Centrelink had attempted to improve its internal corporate record keeping practices, in the particular context of BC planning, Centrelink had not fully adopted better practice as advocated by the National Archives of Australia.

Recommendation No. 9 of the previous audit

The ANAO recommends that:

- Centrelink's business continuity plans be updated to include the identification of vital records, in all storage formats, and that resulting plans aim to ensure preservation and / or recovery of vital records in the event of a disaster; and
- Centrelink adopt National Archives of Australia guidance on record-keeping disaster preparedness in order to ensure that business continuity planning and treatments for vital corporate records are aligned with accepted better practice.

Findings of this audit

4.24 Centrelink has partially implemented Recommendation No. 9 from the previous audit.

4.25 Most of Centrelink's vital records are computer-based and Centrelink has arrangements in place to back up these records on a regular basis. Centrelink's BIA templates also make provision for business units to identify vital records, although until now only NSO branches and divisions have completed the BIAs. However, as business units are currently only required to complete EMPs (rather than BCPs), which do not require the inclusion of treatments for risks to vital records identified in the BIAs, Centrelink has not implemented the first part of the Recommendation.

4.26 Centrelink has implemented the second part of the Recommendation. Centrelink's Chief Executive Instructions (CEIs)⁹⁰ remind staff of the need to comply with all legislative requirements⁹¹ and require them to act in

⁸⁹ Centrelink advice 24 April 2009.

⁹⁰ Centrelink, *Chief Executive Instructions No. 17*, 3 July 2007.

⁹¹ These include the *Archives Act 1983*, the *Privacy Act 1988*, the *Freedom of Information Act 1982*, the *Commonwealth Evidence Act 1995* and the *Electronic Transactions Act 1999*.

accordance with the Australian Standard ISO 15489-2002, *Records Management* and the standards and guidelines promulgated by the National Archives of Australia. This includes the National Archives guidance on record-keeping disaster preparedness.

4.27 Centrelink's *Policy for Recordkeeping* was last updated in 2002 but is currently being reviewed. In this context, the ANAO suggests that this review provides Centrelink with the opportunity to assess how well the National Archives guidance on business continuity is being applied.

Crisis coordination

Findings of the previous audit

Crisis coordination

The ANAO noted the following coordination and control aspects of the BCM and emergency response framework:

- the designated alternate NCCC is in close proximity to the primary NCCC, risking both centres to be unusable by a single event;
- documentation boxes and crisis plans for key Business Recovery Teams were not located in the designated NCCC;
- heavy reliance was placed on a small team to fulfil secretariat and coordination roles, which can become unsustainable beyond one standard working shift; and
- documented escalation and declaration guidelines are not consistently followed.

Recommendation No.10 of the previous audit

The ANAO recommends that Centrelink take immediate steps to ensure that:

- a) primary and alternative National Crisis Command Centres are designated and appropriately equipped as per existing Centrelink plans;
- b) documentation boxes and crisis plans for key Business Resumption Teams are available within the National Crisis Command Centres; and
- c) a protocol for activation of back-up shifts for key staff is implemented to make sure that fatigue and occupational health and safety issues are adequately addressed for National Crisis Command Centre staff.

Findings of this audit

4.28 Centrelink has implemented Recommendation No.10 of the previous audit.

4.29 Primary and secondary National Crisis Coordination Centres (NCCC) have been established at NSO and Area Office South-west NSW respectively. These NCCCs are appropriately equipped to handle Centrelink's business needs. Each NCCC site is equipped with two boxes of equipment that include hard copies of plans, satellite phones and basic supplies, such as stationery. National and Area Office crisis coordinators interviewed by the ANAO also

indicated that they retain readily accessible copies of plans and contact information.⁹²

4.30 Centrelink advised that rostering, rotation and relief arrangements were in place by March 2005 for the community recovery surge team. The ANAO also observed that the Network Coordination section in the Network Coordination and Emergency Management Branch also provided support during crises (refer paragraphs 2.22-2.26).



Ian McPhee

Auditor-General

Canberra ACT

25 June 2009

⁹² One copy in the office and another at their home or in their vehicle.

Appendices

Appendix 1: Department of Human Services' Response to the Audit Recommendations

Centrelink

Centrelink welcomes this report and considers that implementation of the recommendations will further enhance Business Continuity Management in Centrelink. In particular, the recommendations will inform the governance and performance management and testing of business continuity arrangements in Centrelink.

Centrelink agrees with the recommendations in the report.

Department of Human Services

Thank you for your letter of 12 May 2009 providing the proposed Audit Report *Business Continuity Management and Emergency Management in Centrelink* and requesting comments pursuant to sub-section 19(4) of the *Auditor General Act 1997*.

The Department of Human Services (DHS) welcomes the follow-up report and notes that Centrelink agrees with the overall recommendations outlined in the Section 19 report.⁹³ Of the eleven recommendations made in the previous report, five recommendations have been fully implemented. A further five areas have been identified where improvements can be made. DHS notes the ANAO's acknowledgement that the reforms and initiatives already in hand address the outstanding matters raised in the Report.

Centrelink has indicated that the recommendations in the Audit Report will be taken on board as a measure of its commitment to continual improvement. DHS and Centrelink look forward to utilising the updated ANAO Better Practice Guide on BCM to further develop a framework that supports a robust Business Continuity plan.

I would like to thank you for drawing this matter to the Department's attention and for providing the opportunity for early consideration of the report.

⁹³ Refers to the proposed report provided to DHS for comment under sub section 19(3) of the *Auditor-General Act 1997*.

Appendix 2: Centrelink’s Business Continuity Priorities

In the event of an interruption in the availability of key enabling resources (people, information communications technology and property) the following business functions are the highest priority for recovery following restoration of the interrupted resource.

Action to advise the Government and key stakeholders of any interruption to payments, services and recovery action will be performed simultaneously.

1. Delivering Payments

Maintaining delivery of Commonwealth Government payments to eligible customers (based on the customer’s recorded circumstances)

2. Delivering Services

Maintaining delivery of services to eligible citizens on behalf of policy departments and other contracting agencies including the capability to register and process claims and other changes in circumstances, for these services and payments

3. Maintaining Customer and 3rd Party Access to Centrelink

Maintaining access to Centrelink through the face to face, call and online channels

4. Maintaining Payment Integrity

Maintaining the integrity of government outlays delivered through social security legislation and policy

5. Maintain Effective Governance and Business Management

Maintaining Centrelink’s capability to make and enact strategic management decisions, and keep the organisation functioning within legislative and operational requirements.

6. Providing a Community Recovery Capability

Maintaining Centrelink’s capability to support local communities following a disaster or emergency including the National Emergency Call Centre, participation in evacuation & recovery centres and delivery of Government assistance such as the Australian Government Disaster Recovery Payment.

7. Providing Information to Internal & External Stakeholders

Maintaining the availability and flow of system generated information and performance data to meet key stakeholder expectations.

Appendix 3: Centrelink's IT Disaster Recovery Plans

| DR Plan Name | DR Plan Scope | DR Plan Component |
|--|--|--|
| Hardware Infrastructure Disaster Recovery Plans | | |
| Mainframe Environment DR Plan | The Mainframe Environment Core Disaster Recovery Plans describes all of the prerequisite and behind the scenes work required to 'condition' or 'configure' the alternate Data Centre Mainframe Computing Environment, which in this case is CDC, to cater for the recovery and execution of BDC based mainframe priority one services. | Components included in the Mainframe Computing Environment Disaster Recovery Plan include: <ul style="list-style-type: none"> All physical and logical mainframes; All mainframe software and services; and All mainframe storage. |
| Connectivity Environment DR Plan | The Connectivity Environment Disaster Recovery Plan describes the configuration of all hardware and software infrastructure which establishes and maintains connectivity between all components within the Centrelink IT Computing Environment. | Components included in the Connectivity Environment Disaster Recovery Plan include: <ul style="list-style-type: none"> All File and Print Servers All LAN/WAN Hardware & Software (Novell) All Routers & Switches All Desktop Services All Telecommunications All Communication Software and Protocols (WebSphere MQ, TCP/IP, SNA, VTAM) |
| Midrange Environment DR Plan | In the context of Disaster Recovery, the Midrange Environment describes the configuration of all the IT non mainframe components with the exception of Desktop, File and Print servers and Communications Infrastructure hardware & software which are included in the Connectivity Environment Core Disaster Recovery Plan. | Components included in the Midrange Environment Disaster Recovery Plan include: <ul style="list-style-type: none"> All Unix based servers; All Windows based (WINTEL) servers; and All Windows NT based servers. |
| Applications Infrastructure Disaster Recovery Plans | | |
| ISIS DR Plan | The ISIS Core Disaster Recovery Plans describes all of the work required to recover and establish the complete Income Security Integrated System (ISIS) environment at the alternate Data Centre, which in this case is BDC, to deliver all ISIS based Priority One services. | |
| Centrelink Online DR Plan | The Centrelink Online (COL) Core Disaster Recovery Plans describes all of the work required to recover and establish the complete COL Frame (COLF) environment at the alternate Data Centre, to deliver all COLF based Priority One services. | |

Appendix 4: IT Business Continuity Risks

A number of major IT business continuity risks were identified in the previous audit. An update on these risks is discussed below.

Data centres

Potential loss of Centrelink data centres from a natural disaster

Centrelink operates two data centres, both of which are located in Canberra. It stores back-up data at a third site that is also in Canberra. At the time of the previous audit, Centrelink had not formally considered the implications of the simultaneous loss of both data centres and its offline data storage facility. For this reason, and in light of the 2003 Canberra bushfires, the previous audit recommended that Centrelink review the risk of the loss of both data centres.

In response to this recommendation, Centrelink commissioned an external consultant, Risk Frontiers, to undertake a hazard analysis for the data centres in Tuggeranong and Bruce and the off-site data storage repository. The report was completed in June 2005.⁹⁴

The report looked at possible impacts of earthquake, windstorm, flood and bushfire. The report found that there was no significant potential for any of these events to cause the simultaneous inoperability or destruction of these sites. The off-site data storage site was found to be vulnerable only to floods with a risk of occurring less than once in a 100 year period, on average. One of the data centres was found to have a low risk of bushfire damage. The possibility of the two data centres being extensively damaged by earthquake was calculated to have a return period of less than 200 000 years. The report observed, however, that a moderate earthquake could render back-up data temporarily inaccessible.

On the basis that the risks posed by these particular natural disasters were negligible, Centrelink has not further considered the need for contingencies if both data centres were to simultaneously fail for this reason. The ANAO considers this to be reasonable to the extent that the natural perils considered in the report are the most obvious catastrophes that could cause simultaneous failure of both Centrelink's data centres. The issue of where Centrelink should

⁹⁴ Risk Frontiers, *Hazard Analysis for Centrelink's Canberra Data Centres and Off-site Storage Facilities* (June 2005).

locate data centres, how they should be configured and managed is, however, an ongoing risk management issue for Centrelink to actively monitor.

Other risks and advantages in locating the data centres in Canberra

As the existing data centres are nearing capacity, Centrelink has recently been considering options for the future of its data centre operations. An IBM report on Centrelink's future data centre strategy has highlighted a number of weaknesses of the current centres, including the identification of potential single points of failure in the design of the facilities.⁹⁵

The location of Government data centres within the ACT was considered as part of the recently completed Gershon report. The report found that a large proportion of government agencies had more than one data centre located in the ACT. Of particular concern to a number of agencies consulted as part of the review was the issue of Canberra's reliance on a single power grid, with a limited number of feeds to that grid.⁹⁶

Centrelink has previously experienced a number of power outages to its data centres. For example, in September 2006 there was a power failure at the BDC in which the back-up power also failed. In December 2007, there was another failure at the BDC that led to a failure of all IT systems at the BDC and the loss of all Centrelink services for 19 hours, with subsequent flow-on impacts and service disruption.⁹⁷

Experiences of other cities have also shown that the catastrophic failure of a power grid to a city is a real threat.⁹⁸ Therefore, this risk will need to be considered as part of Centrelink's consideration of where it should locate future data centres.

While there are risks in locating the data centres in Canberra, there are also advantages. The 'Sysplex' system used by Centrelink enables it to treat the two

⁹⁵ IBM Global Services, *The Enterprise Data Centre of the Future: Centrelink Data Centre Strategy 2008-2028* (June 2008), p. 49.

⁹⁶ Gershon, P, *Review of the Australian Government's Use of Information and Communication Technology*, Commonwealth of Australia (2008), p. 29. There are two feeds from NSW to the single ACT power grid. One feed provides 85 per cent of electricity to the ACT and the other 15 per cent. The smaller 15 per cent feed is only to the immediate Fyshwick area and is insufficient to support agency needs.

⁹⁷ This outage took place on a weekend. Further, five hours of the outage were outside service agreement hours, meaning that there was a 14 hour disruption to normal services.

⁹⁸ Examples of power disruptions to major urban areas include those that occurred in New York in 1977 and 2003. In 1998 the Central Business District of Auckland had a power failure that lasted three weeks. In 1985 an industrial dispute caused ongoing disruptions to the power supply to large parts of Brisbane.

data centres as one logical data centre. A considerable advantage to Centrelink of this arrangement is that it attracts only a single licence cost, therefore saving the agency an estimated \$5 million dollars annually.⁹⁹ Sysplex also provides the added benefits of 'high availability through failover, resource sharing and workload balancing'.¹⁰⁰ The constraints of Sysplex are that the sites must be within 100 kilometres of one another and preferably within 40 kilometres.¹⁰¹

The IBM report on Centrelink's future data centre strategy examines a number of options for typical data centre configurations with a strong focus on the issues of business continuity and disaster recovery. The report makes a strong case for Centrelink to continue with its current configuration of two data centres with DR capability within 40 kilometres of one another in the ACT.

The Government's decision to adopt the recommendations of the Gershon Report means that all agencies will need to give consideration to a broad range of continuity and e-security issues. Some of these were highlighted by the Prime Minister in the Australian Government's inaugural security statement.¹⁰² This means that, in implementing the Gershon recommendations, Centrelink will need to ensure that its long-term data centre strategy addresses potential continuity issues, such as the simultaneous failure of its data centres.

Capacity constraints

Centrelink will need to relocate its current data centres in the very near future due to limited continued capacity. There is no floor space available for future expansion and relocation of the Tuggeranong data centre is considered urgent, with capacity expected to be reached in June 2009. There are also air-conditioning and other operational issues requiring urgent attention at both centres.¹⁰³

Centrelink has a Memorandum of Understanding with FaHCSIA on the location of its primary data centre (CDC) in the Tuggeranong Office Park. The MoU only provides Centrelink with continued tenure in the building until

⁹⁹ IBM Global Services, op. cit., p. 61.

¹⁰⁰ *ibid.*

¹⁰¹ *ibid.*

¹⁰² Rudd, K (Prime Minister) 2008, The First National Security Statement to the Parliament, address, available from <http://www.pm.gov.au/media/Speech/2008/speech_0659.cfm>. For example, terrorism, cyber attacks and pandemic were all highlighted by the Prime Minister as ongoing or emerging threats.

¹⁰³ IBM Global Services, op. cit., p. 49-51.

2012. Centrelink has identified the lack of a formal contract covering the CDC as a potential risk to the agency.

Centrelink has been examining options to address the urgent capacity constraint on its data centres and the risk to business continuity that it poses and has developed a business case for consideration by the Government. These options have regard to the recommendations of the Gershon Report for consolidation of data centres across agencies.

Off-site data storage

The previous audit noted that Centrelink did not periodically assess the contents, environmental protection and security aspects of its off-site back-up storage facility. The ANAO notes that Centrelink commissioned a 'Mainframe Recoverability Assessment' in 2004 that looked into the off-site storage process in the context of Centrelink's IT disaster recovery strategy. This report concluded that the offsite storage process fulfilled the basic requirements of the Centrelink's disaster recovery strategy.

The Risk Frontiers review in 2005 looked at the environmental protection of Centrelink's off-site storage facility at Fyshwick, and concluded that the risks at the facility were low. It did not, however, provide a comprehensive assessment of the control procedures at the facility.

The ANAO notes also that Centrelink is currently developing its data back-up capabilities and that these refinements will reduce the agency's reliance on the data that is currently stored off-site. Notwithstanding this, it remains important that Centrelink continue to assess the content, environmental protection and security aspects of its off-site back-up storage on a regular basis.

Centrelink's IT back-up arrangements

The Storage and Tuning Services Section (STS) within the Infrastructure Services Branch of the IT Corporate Systems Division manages the mainframe and enterprise open-systems networked (mid-range) storage environments.¹⁰⁴

Centrelink's back-up policy¹⁰⁵ is to provide storage for corporate and customer data, which are stored in the shared drives. Both home and shared data drives

¹⁰⁴ The mainframe hardware and storage environment includes managing the mainframe configuration, Direct Access Storage Disk (DASD), Virtual Tape technologies, and real tape including automated tape silos. Enterprise disk storage includes the Storage Area Network (SAN) for Midrange servers (which include UNIX, Linux, Windows and Novell operating systems).

are backed up nightly. If a file is changed, a new copy is taken and this becomes the active copy. Up to 14 versions of modified files are kept for recovery purposes. If a file is deleted, only the active copy of the file on the home or shared drive is kept as a back-up. All other copies are kept for 90 days.¹⁰⁶

In the event of a disaster, the STS Section can recover data from archive storage. Individual files that are made inactive (deleted) are kept on archive storage for 90 days. Active file back-ups are kept indefinitely. If a file is deleted, corrupted or modified incorrectly, the STS Section can restore the individual file within approx 30 minutes after receiving a request from the service desk.

For mainframe back-up, Centrelink uses 'Control M' software to automatically monitor all its scheduled jobs. Control M will detect any jobs that fail during the back-up procedure. Data centre operations staff monitor for such failures. There are adequate standard operational procedures for staff to perform when there are failed jobs.

For all server back-ups, Centrelink uses Tivoli Storage Management (TSM) as the back-up product.¹⁰⁷ TSM uses an 'incremental-forever' philosophy and begins by covering a server with an initial full back-up and then backs up only changed files (that is, increments) indefinitely. By backing up only changed files, TSM saves time, disk space, tapes, and network usage.¹⁰⁸

The ANAO undertook a back-up procedure walkthrough with the STS team and Data Centre Operations to gain an understanding of how back-up processes are conducted and it sighted standard operational procedures used in the process.

Centrelink's mainframe storage and back-up practices are mature. Strategy and procedures have also been developed for the midrange environment and

¹⁰⁵ Enterprise Data Storage Management Guide August 2008. Home drives are usually used to store system profile information and not corporate information.

¹⁰⁶ Microsoft Office, Lotus SmartSuite, Internet favourites and files associated with Lotus Notes (including email) are home files that are available for restoration.

¹⁰⁷ Centrelink Midrange Server Backup Strategy – provided by STS Team.

¹⁰⁸ TSM determines that a file has changed if any of the following have changed: last modified time stamp, file attributes, file security attributes and file size. Archive or change bits are not used to determine if a file has changed. TSM maintains its back-ups according to management classes. The product owners dictate management class attributes.

these are still maturing. Centrelink has a comprehensive enterprise data storage management policy, supported by a guide, specific strategies and procedures. There was evidence that various teams, whose functions are interlinked, work closely together. For example:

- the ITSCM team works with other areas to ensure that service level objectives are clearly defined and understood in relation to enterprise data storage and that that Centrelink meets its business objectives for business continuity, availability, disaster recovery and reporting; and
- the Capacity and Service Delivery Section receives vital information from other areas of Centrelink to ensure that sufficient disk space is maintained.

A project currently under way to reconfigure Centrelink's ISIS environment will have a significant impact on how Centrelink handles data back-up.¹⁰⁹ Changes to the system in early 2009 have introduced peer-to-peer remote copy (PPRC) across data centres. The process involves cross-site disk replication that effectively creates 'mirror' images of ISIS data disks at the remote site.

The main advantage of the PPRC design is that recovery times will be shorter than the current tape based system. The design also eliminates manual handling of tape-based data and, in the event of a system failure, should provide a higher degree of confidence in the integrity of the recovered data. Under the newly configured system, back-up data can potentially also be transferred to tape more easily as it can be taken from a PPRC copy of data at a single site.

¹⁰⁹ *M204 PPRC High Availability Project - Future online processing high level decision document - Centrelink internal document.*

Index

A

- Area Crisis Coordination Centre, 7, 18, 42
- Area Office, 31, 34, 41–42, 51, 54–55, 58–60, 66, 71, 78, 83
- Australian Bureau of Statistics (ABS), 99
- Australian Government Disaster Recovery Payment, 7, 9, 13, 28, 88

B

- Bruce data centre, 7, 62–63, 89, 91
- Business Continuity and Crisis Management Section, 7, 17, 36–37, 41, 48–49, 54–55, 58–59, 66–67, 70–71
- Business continuity management, 7, 13–21, 27–40, 43–46, 48, 50, 57–58, 61, 66, 69–71, 73–79, 83
- Business continuity management framework, 15–20, 31, 33–35, 44–46, 48, 57, 61, 66, 73, 76
- Business continuity plan, 7, 9, 13, 16, 19, 27, 45–46, 50, 53, 57, 59–61, 67, 69, 78, 80, 82
- Business Continuity Policy, 17, 18, 34–36, 39, 43, 58–60, 76
- Business Continuity, Crisis Management and Security Subcommittee, 7, 17, 20, 38, 39, 40, 44, 55, 64, 67, 69, 71, 73
- Business Criticality Review, 55, 57, 80
- Business impact analysis, 7, 9, 19, 37, 40, 49, 50–55, 60–61, 82
- Business Partnership Agreement, 7
- Business resumption team, 18, 42, 83

C

- Canberra data centre, 7, 62–63, 89, 92
- Centrelink Operations Facility, 7, 18, 43
- Chief Executive Instructions, 7, 36, 82
- Continuity treatment, 19, 35, 57, 65–66, 77

- Crisis, 7, 9, 10, 40–41, 69, 73, 83
- Crisis Coordination Centre, 7, 18, 41–42
- Crisis response, 10, 16, 18–19, 28, 44, 57–58, 60–61, 71, 78
- Customer Service Centre, 7, 15, 28, 43, 58, 66
- Cyclone Larry, 42

D

- Department of Education, Employment and Workplace Relations, 7, 27, 54
- Department of Families, Housing, Community Services and Indigenous Affairs, 7, 27, 42, 54, 92
- Department of Human Services, 7, 21, 41, 87
- Department of the Prime Minister and Cabinet, 41

E

- Emergency management, 10, 13, 16, 19, 27, 29, 57–58, 71, 74–76, 78
- Emergency management plan, 7, 19, 57–59, 67, 78

I

- Income Security Integrated System, 7, 56, 62, 65, 68–69, 89, 95
- Index, 15
- IT Disaster Recovery Plans, 20, 49, 50, 61–65, 67–69, 71–73, 80, 89
- IT Information Library, 7, 51, 56, 79
- IT Service Continuity Management (ITSCM) Team, 36
- IT Service Continuity Management Team, 36–37, 49, 50, 57, 67, 80
- IT Service Delivery Strategy and Management Branch, 36, 38–39
- IT Services Catalogue, 20, 56–57, 79

M

- Maximum acceptable outage, 8–10, 19, 51, 54–55

Memorandum of Understanding, 8, 92

N

National Crisis Coordination Centre, 8, 18, 41–43, 83

National Emergency Call Centre, 8, 36, 50, 88

National Support Office, 8, 19, 34, 40, 41, 43, 51–55, 57–59, 62, 71, 78, 82–83

O

Operational Readiness Checklist, 8, 49, 77, 79

P

Planning and Demand Management Branch, 39, 56

Post-implementation Review, 8, 20, 42, 67, 73

Project Management Plan, 48, 77

Q

Queensland floods, 14, 30, 42

R

Risk management, 16–17, 19–20, 27, 39, 40, 46, 49–50, 60, 70, 76–77, 91

Risk Management Team, 40

S

Service First, 56, 79

V

Victorian bushfires, 14, 30

Series Titles

ANAO Audit Report No.1 2008–09
Employment and Management of Locally Engaged Staff
Department of Foreign Affairs and Trade

ANAO Audit Report No.2 2008–09
Tourism Australia

ANAO Audit Report No.3 2008–09
Establishment and Management of the Communications Fund
Department of Broadband, Communications and the Digital Economy
Department of Finance and Deregulation

ANAO Audit Report No.4 2008–09
The Business Partnership Agreement between the Department of Education, Employment and Workplace Relations (DEEWR) and Centrelink
Department of Education, Employment and Workplace Relations
Centrelink

ANAO Audit Report No.5 2008–09
The Senate Order for Departmental and Agency Contracts (Calendar Year 2007 Compliance)

ANAO Audit Report No.6 2008–09
Illegal, Unreported and Unregulated Fishing in the Southern Ocean
Australian Customs Service

ANAO Audit Report No.7 2008–09
Centrelink's Tip-off System
Centrelink

ANAO Audit Report No.8 2008–09
National Marine Unit
Australian Customs Service

ANAO Report No.9 2008–09
Defence Materiel Organisation—Major Projects Report 2007–08

ANAO Audit Report No.10 2008–09
Administration of the Textile, Clothing and Footwear Post–2005 (SIP) Scheme
Department of Innovation, Industry, Science and Research

ANAO Audit Report No.11 2008–09
Disability Employment Services
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.12 2008–09
Active After-school Communities Program
Australian Sports Commission

ANAO Audit Report No.13 2008–09
Government Agencies' Management of their Websites
Australian Bureau of Statistics
Department of Agriculture, Fisheries and Forestry
Department of Foreign Affairs and Trade

ANAO Audit Report No.14 2008–09
Audits of Financial Statement of Australian Government Agencies for the Period Ending June 2008

ANAO Audit Report No.15 2008–09
The Australian Institute of Marine Science's Management of its Co-investment Research Program
Australian Institute of Marine Science

ANAO Audit Report No.16 2008–09
The Australian Taxation Office's Administration of Business Continuity Management
Australian Taxation Office

ANAO Audit Report No.17 2008–09
The Administration of Job Network Outcome Payments
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.18 2008–09
The Administration of Grants under the Australian Political Parties for Democracy Program
Department of Finance and Deregulation

ANAO Audit Report No.19 2008–09
CMAX Communications Contract for the 2020 summit
Department of the Prime Minister and Cabinet

ANAO Audit Report No.20 2008–09
Approval of Funding for Public Works

ANAO Audit Report No.21 2008–09
The Approval of Small and Medium Sized Business System Projects
Department of Education, Employment and Workplace Relations
Department of Health and Ageing
Department of Veterans' Affairs

ANAO Audit Report No.22 2008–09
Centrelink's Complaints Handling System
Centrelink

ANAO Audit Report No.23 2008–09
Management of the Collins-class Operations Sustainment
Department of Defence

ANAO Audit Report No.24 2008–09
The Administration of Contracting Arrangements in relation to Government Advertising to November 2007
Department of the Prime Minister and Cabinet
Department of Finance and Deregulation
Department of Education, Employment and Workplace Relations
Department of Health and Ageing
Attorney-General's Department

ANAO Audit Report No.25 2008–09
Green Office Procurement and Sustainable Office Management

ANAO Audit Report No.26 2008–09
Rural and Remote Health Workforce Capacity – the contribution made by programs administered by the Department of Health and Ageing
Department of Health and Ageing

ANAO Audit Report No.27 2008–09
Management of the M113 Armoured Personnel Upgrade Project
Department of Defence

ANAO Audit Report No.28 2008–09
Quality and Integrity of the Department of Veterans' Affairs Income Support Records
Department of Veterans' Affairs

ANAO Audit Report No.29 2008–09
Delivery of Projects on the AusLink National Network
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.30 2008–09
Management of the Australian Government's Action Plan to Eradicate Trafficking in Persons
Attorney-General's Department
Department of Immigration and Citizenship
Australian Federal Police
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.31 2008–09
Army Reserve Forces
Department of Defence

ANAO Audit Report No.32 2008–09
Management of the Tendering Process for the Construction of the Joint Operation Headquarters
Department of Defence

ANAO Audit Report No.33 2008–09
Administration of the Petroleum Resource Rent Tax
Australian Taxation Office

ANAO Audit Report No.34 2008–09
The Australian Taxation Office's Management of Serious Non-Compliance

ANAO Audit Report No.35 2008–09
Management of the Movement Alert List
Department of Immigration and Citizenship

ANAO Audit Report No.36 2008–09
Settlement Grants Program
Department of Immigration and Citizenship

ANAO Audit Report No.37 2008–09
Online Availability of Government Entities' Documents Tabled in the Australian Parliament

ANAO Audit Report No.38 2008–09
Administration of the Buyback Component of the Securing our Fishing Future Structural Adjustment Package
Department of Agriculture, Fisheries and Forestry

ANAO Audit Report No.39 2008–09
Administration of the Securing our Fishing Future Structural Adjustment Package Assistance Programs
Department of Agriculture, Fisheries and Forestry

ANAO Audit Report No.40 2008–09
Planning and Allocating Aged Care Places and Capital Grants
Department of Health and Ageing

ANAO Audit Report No.41 2008–09
The Super Seasprite
Department of Defence

ANAO Audit Report No.42 2008–09
*Interim Phase of the Audit of Financial Statements of General Government
Sector Agencies for the Year ending 30 June 2009*

ANAO Audit Report No.43 2008–09
Construction of the Christmas Island Immigration Detention Centre
Department of Finance and Deregulation

ANAO Audit Report No.44 2008–09
Security Risk Management

ANAO Audit Report No.45 2008–09
Funding for Non-government Schools
Department of Education, Employment and Workplace Relations

Current Better Practice Guides

The following Better Practice Guides are available on the Australian National Audit Office Website.

| | |
|---|-----------|
| Business Continuity Management | June 2009 |
| Building resilience in public sector entities | |
| Developing and Managing Internal Budgets | June 2008 |
| Agency Management of Parliamentary Workflow | May 2008 |
| Public Sector Internal Audit | |
| An Investment in Assurance and Business Improvement | Sep 2007 |
| Fairness and Transparency in Purchasing Decisions | |
| Probity in Australian Government Procurement | Aug 2007 |
| Administering Regulation | Mar 2007 |
| Developing and Managing Contracts | |
| Getting the Right Outcome, Paying the Right Price | Feb 2007 |
| Implementation of Programme and Policy Initiatives: | |
| Making implementation matter | Oct 2006 |
| Legal Services Arrangements in Australian Government Agencies | Aug 2006 |
| Preparation of Financial Statements by Public Sector Entities | Apr 2006 |
| Administration of Fringe Benefits Tax | Feb 2006 |
| User-Friendly Forms | |
| Key Principles and Practices to Effectively Design and Communicate Australian Government Forms | Jan 2006 |
| Public Sector Audit Committees | Feb 2005 |
| Fraud Control in Australian Government Agencies | Aug 2004 |
| Security and Control Update for SAP R/3 | June 2004 |
| Better Practice in Annual Performance Reporting | Apr 2004 |
| Management of Scientific Research and Development Projects in Commonwealth Agencies | Dec 2003 |
| Public Sector Governance | July 2003 |
| Goods and Services Tax (GST) Administration | May 2003 |

| | |
|--|-----------|
| Building Capability—A framework for managing learning and development in the APS | Apr 2003 |
| Administration of Grants | May 2002 |
| Performance Information in Portfolio Budget Statements | May 2002 |
| Some Better Practice Principles for Developing Policy Advice | Nov 2001 |
| Rehabilitation: Managing Return to Work | June 2001 |
| Building a Better Financial Management Framework | Nov 1999 |
| Building Better Financial Management Support | Nov 1999 |
| Commonwealth Agency Energy Management | June 1999 |
| Security and Control for SAP R/3 | Oct 1998 |
| Controlling Performance and Outcomes | Dec 1997 |
| Protective Security Principles (in Audit Report No.21 1997–98) | Dec 1997 |