The Auditor-General
Audit Report No.9 2003–04
Performance Audit

Business Continuity Management and Emergency Management in Centrelink

Centrelink

Australian National Audit Office

© Commonwealth
of Australia 2003

ISSN 1036–7632

ISBN 0 642 80735 3

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 available from the Department of Communications, Information Technology and the Arts.

Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Intellectual Property Branch, Department of Communications, Information Technology and the Arts, GPO Box 2154
Canberra ACT 2601 or posted at

http://www.dcita.gov.au/cca

Australian National
Audit Office

Canberra ACT
22 October 2003

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*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit and the accompanying brochure. The report is titled *Business Continuity Management and Emergency Management in Centrelink.*

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—http://www.anao.gov.au.

Yours sincerely

Oliver Winder
Acting 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

Andrew Morris
Paul O'Connor
Anne Martin
Fran Holbert

Contents

Abbreviations

ACG	Area Command Group
ACT	Australian Capital Territory
ANAO	Australian National Audit Office
ASO	Area Support Office
BC	Business Continuity
BCM	Business Continuity Management
BCP	Business Continuity Plan
BCU	Business Continuity Unit
BIA	Business Impact Analysis
BPG	Better Practice Guide
BRT	Business Recovery Team
BSR	Business Services and Resources Pty. Ltd.
CCA	Call Centre Automation
CCT	Crisis Command Team
CEO	Chief Executive Officer
CNOC	Centrelink Network Operations Centre
CobiT	Control Objectives for Information and Related Technology
COMDISPLAN	Commonwealth Disaster Plan
CPO	Centrelink Projects Office
CSC	Customer Service Centre
CSF	Critical Success Factor
DAPS	Disaster Assistance Payments System
DRP	Disaster Recovery Plan
EM	Emergency Management
EMA	Emergency Management Australia
EMLO	Emergency Management Liaison Officer
EMP	Emergency Management Plan
FaCS	Department of Family and Community Services
FAO/COS	Family Assistance Office/Childcare Operator System

HR	Human Resource
ISIS	Income Security Integrated System
IT	Information Technology
I&T	Information and Technology (Centrelink term which encompasses information and communications technology)
ITIL	Information Technology Infrastructure Library
ITSCM	Information Technology Service Continuity Management
ITSM	Information Technology Service Management
JLL	Jones Lang LaSalle
KAES	Knowledge and Enabling Services
KGI	Key Goal Indicator
KPI	Key Performance Indicator
MAO	Maximum Acceptable Outage
NCCC	National Crisis Command Centre
NSO	National Support Office
SLDC	Single Logical Data Centre
TRIM	Tower Records Information Management System
Y2K	Year 2000 computer code error

Glossary

Where possible, definitions have been sourced from the ANAO's Better Practice Guide on Business Continuity Management and the Australian and New Zealand Standard on Risk Management (AS/NZ 4360).

Business Continuity Management (BCM)	The framework of controls implemented, and steps undertaken, by an organisation to manage its business continuity risks. The primary objective of these controls is to ensure the uninterrupted availability of its key business resources that support key (or critical) business processes.
Business Continuity Plan (BCP)	A collection of documents that outline the organisation's preferred approach to dealing with interruptions to key business processes.
Business Impact Analysis (BIA)	The BIA is undertaken for all key business processes and establishes the recovery priorities, should processes be disrupted or lost.
Business interruption event/outage	A business continuity risk event that has a business interruption consequence, causing a disruption to, or loss of, key business processes for a period of time that is unacceptable to the organisation.
Business Resumption Teams	Business group or service area teams responsible for the implementation of BCPs and recovery of business processes, following an incident.
Contingency processing or treatments	See interim processing.
Continuity treatment	Treatments designed to minimise the effects of disruptions to each key business process.
Crisis	An outage that exceeds the Maximum Acceptable Outage (MAO).
Crisis Command Centre	An actual or virtual centre that allows effective coordination and direction of a response to a crisis or incident.
Crisis response	The use of procedures to ensure that immediate actions are taken and issues escalated appropriately to the crisis leadership.
Crisis management	The process used to escalate, manage, resolve and communicate issues related to a crisis.

Critical (National) Infrastructure	Critical infrastructure is defined by the Commonwealth Attorney General's Department as 'that infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on social or economic well-being or affect national security or defence.'
Emergency management	A range of controls and procedures to manage risks to the business associated with community emergencies. It involves developing and maintaining arrangements to prevent or mitigate, prepare for, respond to, and recover from community emergencies.
Event log	Documents the details of an outage. It should be used to review the adequacy of existing controls and identify areas for improvement.
Interim processing	Interim processing or contingency measures that enable business processes to continue, prior to the restoration and resumption of primary/normal business processes.
Key business processes	Key business processes are those processes essential to the delivery of outputs and achievement of business objectives. Business activities and resources are the essential elements that combine to make up each key business process.
Maximum Acceptable Outage (MAO)	The MAO is the time it will take before a business interruption event threatens an organisation's achievement of its business objectives. The MAO defines the maximum time an organisation can survive without key business functions before business continuity plans and recovery procedures have been completely implemented.
Recovery Director	Directs the various recovery and management teams and reports directly to senior management.
Resources	Resources are the means that support delivery of an identifiable output or result. Resources may be money, physical assets or, most importantly, people. Without resources, activities (and therefore processes) would fail.
Resumption planning	Planning for the resumption of services and associated functions following a disruption.
Risk event	Any non-trivial event that affects the ability of an organisation to achieve its business objectives.
Risk management	The systematic application of management policies, procedures and practices to the tasks of identifying, analysing, evaluating, treating and monitoring risk.

Risk treatment	Appropriate intervention strategies for dealing with risk. Treatments are designed to limit the likelihood or impact of the event on the resource at risk. These strategies may include administrative or security procedures, back up and restoration procedures, or training and awareness programs for staff.
'The Plan'	Centrelink's mainframe and data centre technology disaster recovery plan.

Summary and Recommendations

Summary

Background

1. Centrelink delivers the Government's social policy agenda and other programs. In 2001–02, it paid around $55 billion to over 6.3 million customers. Business Continuity Management (BCM) strategies and plans are essential to ensure the agency can continue to deliver these important programs in the event of a crisis.

2. The Government has required Centrelink to play an increasing role in responding to major emergencies affecting Australians (such as the 2002 Bali terrorist bombings). Centrelink's emergency management (EM) performance is therefore of great importance to the Australian community and the Parliament.

3. The primary objective of the audit was to assess whether Centrelink has effective BCM and/or associated risk management procedures and plans in place that: minimise the likelihood of a significant business outage; and, in the event of such an outage, minimise disruption of critical services to customers. The audit also assessed whether Centrelink services satisfy special demands in times of emergency.

4. Accordingly, the ANAO examined Centrelink's frameworks, approaches, strategies, plans, capabilities and recent performance in both BCM and EM.

Key audit findings

Centrelink's BCM framework, elements and main approaches (Chapters 2 and 3)

5. The ANAO found that Centrelink's BCM framework effectively addresses the main elements of business continuity outlined in the better practice literature[1], namely crisis response, crisis management, interim processing and business process recovery. For example, Centrelink's crisis management organisational structure is logical, as it is based on a Crisis Command Centre structure, includes appropriate managers from Centrelink's network, specifies appropriate Business Resumption Teams, and clearly defines the roles and responsibilities of the key business continuity participants. The Crisis Command Centre structure and Business Resumption Teams also generally work well in practice.

---

[1] Such as the ANAO 2000, *Business Continuity Management, Keeping the Wheels in Motion*, Better Practice Guide, January; and Business Continuity Institute, *Evaluation Criteria for Business Continuity Plans.*

6. Centrelink has recently established a Business Continuity and Emergency Management team, and an IT Service Continuity Management team. This new structure should improve the alignment of BCM and EM in Centrelink. In implementing these changes, the ANAO cautions that Centrelink must clearly distinguish the objectives and operating requirements of BCM and EM. The new structure also potentially allows a unit to have a widely recognised and accepted role to co-ordinate and oversight BCM in Centrelink. However, as these changes are very recent, and roles have not yet been fully determined, the ANAO emphasises the need for a single unit to have a clear and unambiguous oversight responsibility for BCM across the whole organisation, even if this change would require the unit to oversight associated information and technology activities undertaken by other units.

7. The Business Continuity and Emergency Management team provides advice to other parts of Centrelink, and has recently compiled a database of business continuity plans and emergency plans, which it will analyse to improve central oversight and disseminate better practices. However, the ANAO found that Centrelink could enhance central oversight of, and guidance to many staff and managers in its network on, BCM and EM. To clearly and comprehensively outline its approach to BCM, and to improve communication of prime BCM objectives, methods and responsibilities, the ANAO also found that Centrelink should develop, and appropriately distribute, an overarching BCM document.

8. Most of Centrelink's BCM related plans and processes incorporated a risk management process consistent with that used for broader risk management in Centrelink. The ANAO found risk management and BCM to be well aligned at the operational level, although there is scope for further improvement through enhancing the consistency of business continuity plans and underlying risk management methodologies. There is also scope to upgrade communication between managers with overarching responsibility for BCM and risk management, to further enhance BCM in Centrelink.

9. Centrelink's BCM framework is underpinned by organisational processes consistent with the ANAO's Better Practice Guide on BCM[2] that focus on: project initiation; identifying critical business processes; designing and implementing treatments; rehearsal; and training.

Identifying and addressing critical business processes (Chapters 4 and 5)

10. An important element of this audit was to establish whether Centrelink's business continuity strategies and plans covered all critical processes, which

[2] ibid.

would ensure that all services could be recovered within a timeframe that would enable Centrelink to meet its specified business objectives. Centrelink uses two main mechanisms to identify key business processes and undertake Business Impact Analysis, namely Business Criticality Reviews, and continuity elements required to be incorporated into new projects.

11. The ANAO found that the 2002 Business Criticality Review provided a reasonable approach to identifying key business processes and undertaking a Business Impact Analysis. However, the review should have considered a number of business processes that were omitted, including data and telecommunication systems, and some information and technology (I&T) applications and infrastructure. The review could also have considered the impact of an incident affecting an Area Support Office. Centrelink has advised that a Business Criticality Review to be undertaken in 2003–04 will address these concerns.

12. The ANAO considers that Centrelink's project management process provides an effective framework for treating both business continuity and risk for new projects. However, the ANAO found that a lack of central recording and oversight of the business continuity elements of new project plans contributed to a lack of effectiveness of the project management process to adequately address business continuity.

13. Centrelink's business continuity capability is strongly bolstered by the nature of its business, especially the delivery of services to customers throughout its network. For example, if Centrelink were to lose a Customer Service Centre or Call Centre, it can generally quite readily service customers at alternative sites. This flexibility provides extensive built-in redundancies and makes many business processes less 'critical' than they may at first appear. Many of Centrelink's in-house business support processes also sustain its capacity to manage crises, including the existence of substantial capabilities in corporate communication, social workers, people management, and building management. Centrelink is also able to 'fly-in' technology and other resources from the National Support Office to the network.

Information technology and telecommunications (Chapter 5)

14. Centrelink's I&T infrastructure and applications (especially its mainframe processing of customer entitlements) and telecommunications constitute its most critical processes.

15. At the time of audit fieldwork, the ANAO found that Centrelink's I&T framework had a number of shortcomings but was generally consistent with established BCM practices. The ANAO notes that Centrelink has recently

embraced an Information Technology Infrastructure Library (ITIL) framework. IT Service Continuity Management (ITSCM) is a component of ITIL. Fully implementing this ITSCM component should substantially assist Centrelink to improve I&T business continuity management.

16. The ANAO noted that Centrelink has two data centres, in separate locations, which provide back-up capability for mainframe processing. This capability is likely to be substantially enhanced by the establishment of a proposed single logical data centre, comprising inter-operations of both data centre facilities. At the time of drafting the audit report, Centrelink had begun to formally consider the consequences of simultaneous devastation of both data centres, and its off-site backup storage facility.

17. Centrelink has a number of risk exposures in its I&T applications, hardware and system software, especially in regard to its mid-range equipment and network environments. The ANAO considers that Centrelink should extend its risk-based analysis of hardware and system software to make it comprehensive and consolidated. Centrelink has undertaken to re-assess the recovery times of its various I&T platforms and to address risks that expose them to system failure.

18. The ANAO observed that Centrelink's principal applications were not consistently supported by appropriate levels of documentation. Documentation was frequently out-of-date, incomplete and/or relatively inaccessible.

19. Telecommunications is also a critical dependency for Centrelink, as it enables Centrelink to transmit both data and voice, required to conduct business. The ANAO found that Centrelink's data network provides the required resilience, redundancy and flexibility to ensure high availability, and hence business continuity. Similarly, the ANAO found that Centrelink's voice telecommunications network, Centrelink Call, has taken effective steps to ensure business continuity and resumption. However, the ANAO suggests that Centrelink Call more closely examine its interactions with other Centrelink I&T continuity processes and plans, including third party suppliers, to ensure that recovery expectations are capable of being achieved during a major outage.

Adequacy of BCM strategies and plans, including maintenance and rehearsal (Chapters 2, 4, 5, and 6)

20. Business continuity plans (BCPs) and associated plans are an important element of virtually all BCM strategies. The ANAO found that Centrelink's BCPs and associated plans were consistent with theory and practice outlined in core BCM literature, including the ANAO better practice guide. However, the ANAO identified excessive variation in the structure, contents and coverage of plans used across the network. As well, these plans often do not differentiate between

obligations to respond to local community emergencies and the need to respond to a crisis that disrupts Centrelink's own operations. The ANAO also suggests that Centrelink review its I&T continuity plans. Such a review should include those for the mainframe environment, which are narrowly defined.

21. Centrelink has recognised these limitations and is planning to address them through the BC and EM Framework project currently underway, and the introduction of ITIL, respectively.

22. Maintenance of plans involves updating them on a regular and timely basis to ensure, for example, that contact details of key personnel are correct and to incorporate improvements. While some parts of Centrelink's network regularly update plans, limitations in the higher-level management of BCM (as noted in paragraph 6) precluded Centrelink from being able to provide a high level of assurance of BCPs being maintained on a systematic and regular basis.

23. Business continuity should be treated as an ongoing process, rather than a one-off project. Centrelink is aware of the need for rehearsal as part of this continuous process, and in recent years has undertaken two major simulations involving the National Support Office, to rehearse its response to major crises. However, there have been no such exercises in the wider Centrelink network. Moreover, there is little evidence that staff in the Centrelink network regularly rehearse their roles, or that any other form of training for crisis response or business continuity has been undertaken on a formal and on-going basis. Again, Centrelink is addressing this issue through the BC and EM Framework project.

Capability of Centrelink staff to ensure continuity (Chapters 4, 5, and 6)

24. The primary objective of BCM is to provide a high level of assurance that an organisation can respond to a crisis. While a major focus is often on frameworks and plans, as the ANAO Better Practice Guide states, 'people are often overlooked as the most critical resource in ensuring continuity of business'.[3]

25. Centrelink has recognised the importance of its staff in ensuring business continuity, and has included in its framework and plans: human resource management issues including occupational health and safety; protocols for communication; treatments for any psychological effects on staff; and support for the recovery team.

26. During fieldwork, the ANAO observed Centrelink's response to the loss of the Warrnambool Customer Service Centre (CSC) due to fire. This event highlighted the ability, commitment, skills and knowledge of Centrelink staff to

[3] ibid.

undertake contingency processing and restore prime processing. The fire also demonstrated the high level of senior management support for such recovery efforts, the capacity of the recovery team members, and the effectiveness of interaction between all levels of Centrelink in a crisis.

27. The skills noted above are vital to any business continuity response. The ANAO notes the views of managers and staff at the Warrnambool CSC, and at the associated Victoria West Area Support Office, that other Centrelink offices would most likely be as successful as Warrnambool in responding to such an outage. This is due to the consistency of staff skills and commitment throughout the network, as well as other inherent strengths, such as those discussed in paragraph 13 above.

28. However, to further improve the capacity of staff to contribute to BC (and EM), the ANAO found that Centrelink needed to implement a more structured process to develop a competency and learning framework to train staff. The ANAO notes that Centrelink is addressing this through a Training and Communications Strategy, involving the Centrelink Virtual College, as part of the BC and EM Framework Project.

Emergency management in Centrelink (Chapter 7)

29. Centrelink has a legislated obligation to deliver special and emergency services to the Australian community as directed by the Government. The frequency and complexity of these services have been increasing in recent years, requiring Centrelink to more clearly establish its roles and responsibilities, and manage stakeholder expectations.

30. The ANAO found that Centrelink's current EM framework clearly articulated internal roles and responsibilities. However, the ANAO notes Centrelink's current project to more closely align its EM and BCM roles. The project will also address a number of improvements identified by the audit related to resourcing and equipping the National Crisis Command Centre.

31. Another important aspect of Centrelink's EM framework is the effectiveness of links between the agency and other EM stakeholders. The ANAO found that Centrelink's Area Support Offices had effective liaison links in place with their State and Territory counterparts. However, the ANAO considers that greater coordination and monitoring of this effort at the national level would ensure consistent coverage of, and knowledge about, Centrelink's emergency response roles and responsibilities among its own staff, as well as among other EM stakeholders across Australia.

Performance of BCM and EM in Centrelink (Chapter 2)

32. The audit also examined Centrelink's recent performance in BCM and EM, on the basis that good past performance may reflect effective BCM and EM frameworks and supporting processes, which may in turn indicate (but not guarantee) the likelihood of continued good performance, and vice versa.

33. While the ANAO could not obtain clear and comprehensive performance information, available evidence generally supported Centrelink's claim of an excellent record in BCM—that is, in providing continuous service to customers and in quickly restoring critical business services after an interruption.

34. Similarly, available evidence, while not comprehensive, indicated that Centrelink has delivered its EM roles and responsibilities to the high standards expected by stakeholders, including Centrelink customers, the Parliament and the Australian community. Stakeholder satisfaction ultimately depends predominantly on Centrelink delivering emergency payments on a timely basis to eligible customers, consistent with relevant policies and legislation.

Overall audit conclusion

35. Centrelink has comprehensive and detailed BCM and associated risk management frameworks, policies and plans that generally provide appropriate preventive controls to minimise the likelihood of outages to many of its critical business processes. As well, they provide effective corrective treatments to minimise disruptions of services to customers where these business processes are interrupted. It also has skilled staff, committed to the continuity of essential services to customers.

36. Centrelink has demonstrated its capacity to deliver its critical business processes by maintaining continuity of customer payments. Its BCM capability has proven to be effective in overcoming the loss of network offices, such as CSCs and Call Centres.

37. Notwithstanding this good performance and inherent strengths, Centrelink has a number of continuity risks. In particular:

- some elements of its I&T environment do not have sufficient continuity controls and treatments, and in light of experiences with the ACT firestorm in January 2003, it is apparent that Centrelink has not adequately addressed risks associated with simultaneous catastrophic events to its data centres and off-site backup storage facility;
- the existing framework for BCM provides insufficient assurance as to the state of BCM preparedness throughout its service delivery network; and
- there are inadequacies in plan maintenance, rehearsal and staff training.

38. Centrelink noted many of these shortcomings during audit fieldwork, and is in the process of implementing strategies and practices to improve its BCM capacity. Importantly, Centrelink's planned implementation of the IT Service Continuity Management component of the ITIL framework should assist the agency to provide a more comprehensive, consistent and coherent approach to I&T BCM.

39. Centrelink has been able to satisfy increasing requirements to assist victims of community emergencies, despite some limitations in its EM framework and policies. This performance was based on flexible but robust systems to approve, deliver and record payments, mechanisms to liaise with other emergency service providers, and the efforts of skilled and committed staff. Opportunities for improvements identified in this audit, and in Centrelink's BC and EM framework project, should further improve the efficiency and effectiveness of Centrelink's EM response.

Recommendations

40. The ANAO made 11 recommendations to further improve Centrelink's BCM and EM capacity. Centrelink has agreed to all of the recommendations and, at the time of report tabling, had begun to address all of them.

Agency response

41. A proposed report was issued to Centrelink. Centrelink advised the ANAO of its response to the audit as follows:

> Centrelink has welcomed this audit and we have taken the opportunity to participate fully, gaining many benefits in the process. We have particularly appreciated the efforts and consultative approach of the ANAO audit team.
>
> Centrelink has a proud record in Business Continuity and Emergency Management reflecting its role as an efficient and flexible agency for delivery of Australian Government services. Centrelink's role in times of crisis for our community, such as the Bali bombings, the Katherine floods and the Ansett collapse has earned praise throughout our community and furthered our reputation of excellence in emergency response. Coincidentally, during the period the audit was conducted, our Warnambool office was completely destroyed by fire, without disruption of services to our customers.
>
> The January 2003 Canberra bushfires further highlighted Centrelink's ability in crisis response. The outstanding response to the Canberra community, even when many of our staff were personally affected is testament to our capability. During the bushfire emergency, our normal services were maintained and we were able to mobilise additional staff and resources to provide extra support to the

community through effective co-operation with the Australian Capital Territory government. Despite the exceptional and unusual ferocity of the Canberra fires, Centrelink's I&T infrastructure was able to continue uninterrupted service delivery for our customers throughout Australia. The McLeod Inquiry into the Operational Response to the January 2003 Bushfires indicated that 'Although it was probably the most severe fire experienced in the region in the last 100 years, the emergence of large destructive fires in the region, from time to time, is by no means unique.' These events have prompted a review of the risks faced by our data centres and off-site backup storage facilities. As our experience of the bushfires has shown, Centrelink's robust network and dedicated staff have allowed us to continue to provide effective service even when the organisation itself was affected.

Centrelink considers itself a leader in the field of Business Continuity and Emergency Management within the Commonwealth Public Sector. Centrelink is clearly a key player in the whole-of-government response to emergencies in the community with representation on key committees. Centrelink also plays a significant role in the application of Commonwealth remedies for Emergency Management Australia, the Department of the Prime Minister and Cabinet, the Department of Family and Community Services, the Department of Agriculture, Fisheries and Forestry and the Department of Transport and Regional Services. The level of inclusion and consultation from those agencies is a strong indication of our performance and credibility in the Commonwealth emergency management arena.

It is also important to note that the Government's continued confidence in Centrelink has been demonstrated by its significant commitment to Centrelink's IT Refresh program. This program will further our capability to deliver services on behalf of the Australian Government, including bolstering business continuity arrangements. The forthcoming implementation of Centrelink's recently revised Business Continuity and Emergency Management framework will provide improved integration, communication and consistency across our service delivery network. It will also facilitate continuity plan rehearsal, testing and refinement.

Recommendations

Set out below are the ANAO's recommendations and Centrelink's abbreviated responses. Centrelink's more detailed responses are shown in the body of the report immediately after each recommendation.

Recommendation No. 1 Para. 2.21

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.

Centrelink response: Agreed.

Recommendation No. 2 Para. 2.26

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.

Centrelink response: Agreed.

Recommendation No. 3 Para. 4.23

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 coverage 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.

Centrelink response: Agreed.

Recommendation No. 4 Para. 4.42

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.

Centrelink response: Agreed.

Recommendation No. 5 Para. 4.68

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.

Centrelink response: Agreed.

Recommendation No. 6 Para. 5.29

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.

Centrelink response: Agreed.

Recommendation No. 7 Para. 5.43

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.

Centrelink response: Agreed.

Recommendation No. 8 Para. 5.60

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 backup storage facility;

(b) consider the limitations associated with the location of the off-site backup storage facility; and

(c) periodically, at least annually, assess the content, environmental protection and security aspects of off-site backup storage.

Centrelink response: Agreed.

Recommendation No. 9 Para. 6.51

The ANAO *recommends* that:

(a) 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

(b) 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.

Centrelink response: Agreed.

Recommendation No. 10 Para. 7.33

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.

Centrelink response: Agreed.

Recommendation No. 11 Para. 7.39

The ANAO *recommends* that Centrelink monitor and review its emergency stakeholder liaison and response planning at a national level, and implement relevant findings and recommendations, to ensure effective and consistent special and community emergency responses by Centrelink at the national, State/Territory and local levels.

Centrelink response: Agreed.

Audit Findings and Conclusions

1. Introduction

This chapter provides background information on business continuity management and emergency management in Centrelink. It explains the approach, objective and methodology of the audit and describes the structure of the report.

Importance of business continuity management in Centrelink

1.1 Centrelink was established in 1997 as a statutory authority within the Family and Community Services (FaCS) portfolio.[4] Centrelink's prime responsibility is to deliver the Government's social policy agenda, mainly through its Business Partnership Agreement with FaCS. It also provides many other services, and in 2001–02 delivered around 140 products and services on behalf of 20 Commonwealth and State client agencies to about 6.3 million customers, involving total annual expenditure of approximately $55 billion. Centrelink has over 24 000 staff and delivers services through a network that in early 2003 comprised 15 Area Support Offices, 312 Customer Service Centres and 27 Call Centres located across Australia.

1.2 The importance of Centrelink's responsibilities, in terms of the value of expenditure, the numbers of Australians involved and their criticality to many recipients[5], demands that Centrelink delivers timely and reliable services.[6] This delivery must be underpinned by robust systems and practices that reduce risks of interruptions to payments and ensure timely alternative treatments when critical business systems fail, as well as appropriate restoration and resumption of those systems.

1.3 Centrelink takes seriously the need to safeguard its critical systems and has an extensive business continuity framework built around: information, technology and communication systems; its existing distributed service delivery network; the skills and knowledge of its people; and specific plans and staff training.

---

[4] Centrelink operates under the *Commonwealth Services Delivery Act 1997* (CSDA Act) that gives it responsibility for the provision of Commonwealth services in accordance with service agreements. As a mainstream Australian Public Service organisation, Centrelink is also subject to the *Financial Management and Administration Act 1997* and is staffed under the *Public Service Act 1999*.

[5] Centrelink customers include retired people, families, sole parents, people looking for work, people with disabilities, carers, indigenous people and people from diverse cultural and linguistic backgrounds.

[6] Under its current Business Assurance Framework, Centrelink aims for 95 per cent correct payments, whereby a payment is correct if Centrelink makes correct decisions about processes within its control, that is: the right person is paid; under the right program; at the right rate; for the right dates.

Better practice business continuity management and emergency management

1.4 The principles and processes for developing and implementing business continuity management (BCM) are well established. For example, the Business Continuity Institute in the United Kingdom and DRI International in the United States are two high profile agencies that publish guidelines on BCM approaches and practices.[7] These and other guidelines provided the basis for the ANAO's Better Practice Guide on BCM (the ANAO BPG), published in January 2000.[8] Recently, Standards Australia published new guidelines titled HB 221:2003 Business Continuity Management.[9] The guide outlines nine simple steps, from commencement and inter-dependency requirements through to testing and activation.

1.5 The audit has used the ANAO BPG as the basis for measuring Centrelink's performance against better practice BCM, albeit supplemented by subsequent developments in theory and better practice. This approach is appropriate as Centrelink extensively used the ANAO BPG in developing and maintaining its BCM capacity. Figure 1.1 outlines the basic approach to BCM outlined in the ANAO BPG.

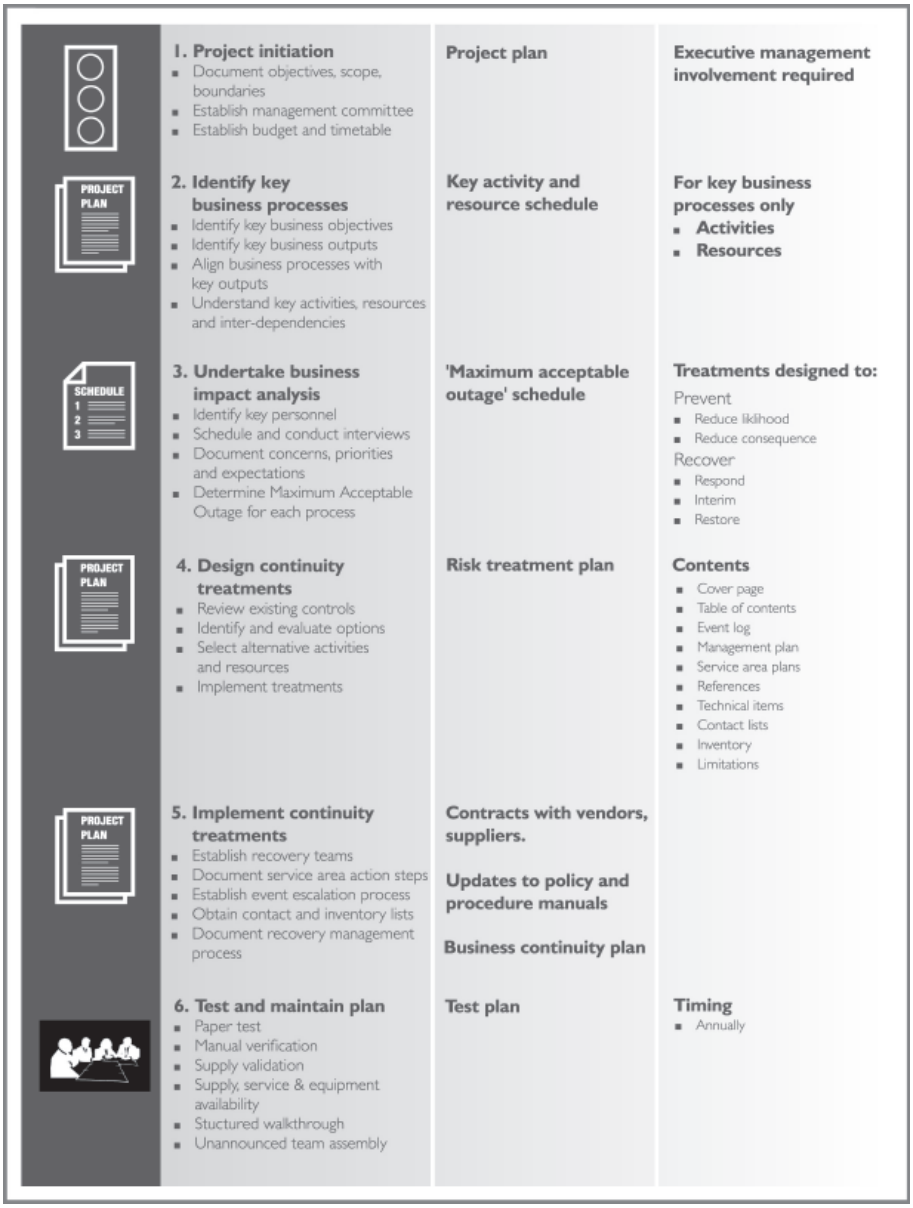
---

7 For example, Business Continuity Institute and DRI International 1997, *Professional Practices for Business Continuity Planners*.

8 ANAO 2000, op. cit.

9 These can be accessed at <www.standards.com.au>.

Figure 1.1
Framework for BCM according to ANAO Better Practice Guide



Source: ANAO 2000, *Business Continuity Management, Keeping the Wheels in Motion*, Better Practice Guide, January.

1.6 BCM is intimately linked to risk management. Most of the relevant literature advocates that BCM incorporate treatments or controls to mitigate the effect of events that may interrupt critical business processes. In this context, BCM delivers contingency treatments to continue essential business services, and to recover and restore full function once an outage event has occurred,

irrespective of the cause and impact of the outage. Separating business continuity from the risk management process, risks information asymmetries that may either lead to a duplication of effort, or more concerning, to critical aspects of the control and recovery process being overlooked.

1.7 The audit identified better practice emergency management (EM) from a number of sources including workshops and publications by Emergency Management Australia[10], industry seminars, general research, as well as input from expert business continuity consultants and practitioners (see Chapter 7).

Defining business continuity management and emergency management in Centrelink

Business continuity management

1.8 The ANAO BPG defines business continuity (BC) to be 'the uninterrupted availability of all key resources to support essential business processes'. Centrelink has a compatible understanding of BC, defining it as the capacity to 'maintain availability of services to customers when a disaster or emergency impacts upon our service delivery capacity'.[11]

1.9 BCM processes underpin Centrelink's approach to safeguarding the continuity of its critical systems. Centrelink considers BCM to be 'a form of risk management' provided through a formal framework that 'deals with the preparation of strategies and contingency plans to ensure that continuity of services to customers can be maintained in an emergency or disaster situation'.[12] In concert with its risk management approach, Centrelink's BC framework aims to prepare strategies and contingency plans that will:

- identify and assess risks which could disrupt services and functions;
- predict likely problems; and
- minimise their impact should the latter occur.[13]

1.10 Figure 1.2 below explains the terminology that Centrelink typically uses to describe key elements of its BC (internal business processes) and EM (external community) activities. At the present time, Centrelink sometimes uses multiple terms to refer to these activities, especially interchanging EM with either disaster response or community emergency response. The ANAO has used single terms in this report for consistency and ease of understanding.

---

[10] Emergency Management Australia is the Australian Government's operational and advisory agency for emergency response, coordination, management, and recovery. Emergency Management Australia is located within the Attorney General's portfolio.

[11] <centrenet/homepage/nso/bc-em/index.htm>

[12] <centrenet/homepage/nso/bc-em/faqs.htm, p. 2.>

[13] ibid., p. 2.

1.11 Centrelink has advised that it plans to update this terminology to ensure greater consistency. The ANAO notes that this may require Centrelink to develop its own terminology. Given that Centrelink has significant BC and EM activities, it will probably not be possible for it to select terminology that is entirely consistent with terminology from core BCM and EM literature.[14] Nevertheless, Centrelink should aim to achieve the maximum possible consistency, for training and educational purposes.

Figure 1.2
Centrelink and ANAO terminology for elements related to BC and EM

Element of BCM	*Description*
Centrelink Terminology	
Business continuity management	Co-ordinating the development of 'back-up' plans that ensure that Centrelink can maintain availability of services when an emergency or disaster strikes. These plans are brought into effect whenever normal business processes are interrupted.
Disaster recovery	The 'clean-up' process during and after an emergency or disaster that aims to return things to normal as quickly as possible.
Emergency management	Is about developing and providing capability for Centrelink to respond to the wider community needs in the event of a national disaster or emergency. As such, it has an external focus.
ANAO Terminology	
Crisis	An interruption to a critical business process that exceeds the maximum acceptable outage.
Critical business process	Those business processes essential to delivery of outputs and achievement of business objectives.
Maximum acceptable outage	The maximum time an agency can survive without key business processes.
Emergency	An event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated approach.

Source: Centrenet/homepage/nso/bc-em/faqs.htm and ANAO 2000, *Business Continuity Management, Keeping the Wheels in Motion*, Better Practice Guide, January.

1.12 Chapter 2 describes and assesses Centrelink's BCM framework and its implementation.

Emergency management

1.13 Due to the nature and scale of its payments to Australian citizens, the existence of its extensive branch office network and heightened expectations of government service delivery, Centrelink is playing an increasingly important role in responding to wider community needs in the event of a national emergency (such as the 2002 Bali terrorist bombings). This assistance to

[14] Such as the ANAO's BPG on BCM or guidance issued by Emergency Management Australia.

individuals in emergencies generally takes two forms: monetary, such as the delivery of special or ex-gratia payments to victims; and general welfare, including counselling services provided by social workers.

1.14 These emergencies are external to Centrelink and generally do not involve the loss of Centrelink business functions. They differ from BC problems involving the loss of Centrelink's internal processes and services. However, there is sometimes considerable interaction between Centrelink staff who deliver internal processes and services and those who provide external services in response to emergencies.

1.15 Centrelink's EM strategies aim to ensure that it can service its customers and affected communities in an emergency. Centrelink's performance in dealing with emergencies is of great importance to the wider community and to the Government and the Parliament. Accordingly, community perceptions of Centrelink and its reputation are strongly influenced by the way Centrelink responds to emergencies.

1.16 Chapter 7 describes and assesses Centrelink's EM framework and its implementation.

Audit approach

1.17 The ANAO has not previously fully and explicitly audited BCM in Centrelink. However, the ANAO briefly examined elements of Centrelink's BC in Audit Report No.39, 2000–01, *Information and Technology in Centrelink* and Audit Report No.41, 1999–2000, *Commonwealth Emergency Management Arrangements*.

1.18 The objectives of the current audit were to assess whether:

- Centrelink has effective BCM and/or associated risk management procedures and plans in place that:
  - minimise the likelihood of a significant business outage[15]; and
  - in the event of a significant business outage, minimise disruption of critical services to customers; and that
- Centrelink services satisfy special demands in times of emergency.

1.19 The audit's examination of Centrelink risk management focused on its alignment with BCM, mainly to ensure that critical business processes had appropriate controls as well as BC treatments. The ANAO did not separately

[15] A significant business outage occurs when an interruption to a critical business function exceeds a specified maximum acceptable outage.

examine Centrelink's risk management framework, methodology and application, in this audit.

1.20 As BCM, by its nature, is embodied within a framework encompassing the full breadth of an organisation, this audit examined key business processes used by Centrelink to deliver and maintain continuity of services. In so doing, the audit examined key National Support Office functions and tested BCM arrangements across Centrelink's network. The audit also examined Centrelink's holistic approach to BCM, including the organisational structure of BCM and related activities in Centrelink and the integration of business continuity plans and procedures with other key planning and operational activities.

1.21 The audit examined Centrelink's responses to external emergencies as these were often related in concept and application to responses to internal crises. In this respect, the audit focused on Centrelink's policies and processes in place to satisfy its Whole-of-Government role in EM at national, state and local levels. This module of the audit involved discussions with Commonwealth and State-level EM organisations.

Audit methodology

1.22 The audit methodology included:

- determining better practice BCM and EM procedures;
- reviewing Centrelink's BCM policies and procedures and their alignment with risk management planning;
- interviews with Centrelink managers, key National Support Office staff and relevant Area Support Office, Call Centre and Customer Service Centre staff in the Australian Capital Territory, New South Wales, the Northern Territory, Queensland, Victoria and Western Australia with responsibility for BCM and EM;
- focus group discussions with some Centrelink staff;
- analysis of key Centrelink documentation, files and intranet; and
- discussions with key community and government stakeholders throughout Australia.

1.23 Appendix 1 reports the audit criteria.

1.24 Fieldwork was conducted primarily from September 2002 to March 2003. Centrelink was implementing substantial changes to the governance and administration of BCM and EM throughout this period. The audit has reflected many of these changes, noting their partial implementation at the time of

fieldwork and, where possible, commenting on the appropriateness of proposed reforms.

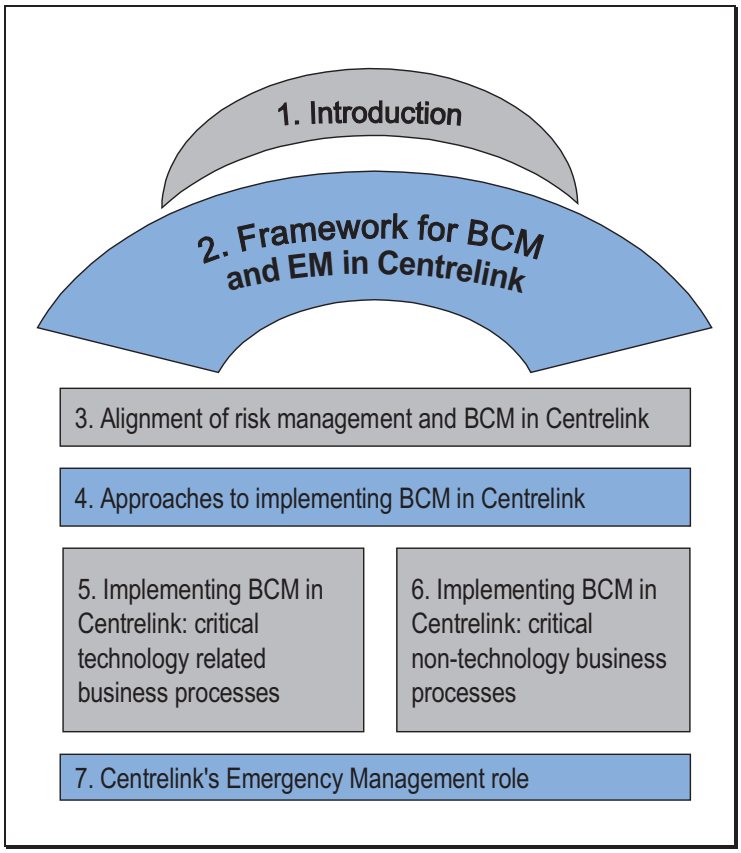
1.25 The ANAO engaged Business Services and Resources Pty Ltd (BSR) to assist with the analysis of evidence gathered throughout the audit. BSR has developed, implemented and audited BCM procedures and plans for organisations with similar characteristics to Centrelink.

1.26 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of $445 000.

Structure of the report

1.27 This report contains seven chapters, as outlined in Figure 1.3.

Figure 1.3
Structure of chapters



2. Framework for BCM and EM in Centrelink

This chapter discusses the framework for BCM and EM in Centrelink. Following a brief discussion of the history of BCM and EM in Centrelink, it examines Centrelink's framework and overarching structures for managing BCM and EM.

Background

2.1 An effective framework for BCM and EM can provide a high level of assurance that an organisation is able to quickly and effectively recover from, or respond to, internal and external crises, respectively. Such a framework provides accountability and alignment through effective management and governance structures; facilitates the development of appropriate plans and strategies; and provides for and monitors appropriate training, rehearsal and plan maintenance.

2.2 While BCM and EM are separate disciplines, they overlap in a number of significant ways within Centrelink, including:

- for those crises that are both internal and external (eg, Katherine Floods—which damaged the Centrelink office and devastated the community, see paragraph 7.14);
- the same person generally having responsibility for both BCM and EM in Centrelink's Area and local offices; and
- that the Crisis Command Centre and broader Crisis Management policies apply to both internal and external crises (that is, to BCM and EM).

2.3 This overlap compels Centrelink to establish a framework that promotes a high level of alignment between BCM and EM. At the same time, the framework must ensure that Centrelink staff clearly understand and operationalise the different objectives and activities of BCM and EM.

2.4 In this context, the framework for BCM and EM in Centrelink has four main components:

- overarching structures for managing BCM and EM;
- risk management processes underpinning BCM and EM;
- strategies, policies and plans underpinning BC; and
- strategies, policies and plans to respond to broader community emergencies.

History and recent performance of BCM and EM in Centrelink

2.5 Historically, Centrelink has focused on the delivery of mainframe based information technology and communication systems. In doing so, it initially concentrated on mainframe disaster recovery planning rather than the development of more general BC strategies and business resumption plans. However, in 1998, the threat presented by the Year 2000 (Y2K) computer code error forced Centrelink to take a more holistic approach to BC planning, and led to the establishment of an organisational framework and plans designed to address a broad range of potential problems. These frameworks and plans were generally consistent with those advocated in core BCM literature.

Centrelink's BCM performance

2.6 Centrelink maintains that it has an excellent record in BCM. That is, it provides continuous service to customers, and is able to quickly restore critical business services when an interruption occurs. Many partial performance indicators, especially regarding information and communications technology (I&T) availability and the nature and duration of outages in area and local offices, support this claim. However, the ANAO could not obtain from Centrelink clear and comprehensive performance information about these fundamental elements of BCM. As a result, we cannot provide unqualified assurance about past performance levels.

2.7 While recognising that Centrelink currently collects a range of performance information that feeds into processes to improve BCM strategies and plans, the ANAO suggests that Centrelink further consolidates and analyses data about outages to business processes, and develops specific BC performance indicators. These performance indicators should then form the basis of, and be consistently used in, internal management processes, and external reporting to FaCS and other stakeholders.

2.8 Specific BCM performance indicators could relate to:

- the timeliness of assessed payments to recipients;
- the availability of Centrelink service delivery channels (that provide information about benefits); and
- the timeliness of restoring critical business processes (including through alternative treatments) when an interruption occurs, especially the proportion restored within the assessed maximum acceptable outage timeframe.

Centrelink's EM performance

2.9 Chapter 7 highlights Centrelink's record of good performance in responding to community emergencies, such as the Katherine Floods of 1998 and the 2002 Bali terrorist bombings. It also explains that Centrelink's role in responding to community emergencies has expanded rapidly in recent years, that is, it has been responding both more frequently and more extensively.

Overarching structures for BCM and EM in Centrelink

2.10 As outlined in Chapter 1, Centrelink is a large organisation, with an extensive network. This network is managed by a National Support Office (NSO) and 15 Area Support Offices (ASO), which support the 312 Customer Service Centres (CSCs) and many other delivery agents.

2.11 Area Managers are responsible to the Centrelink Executive (particularly, to the Chief Executive Officer (CEO)) rather than being directly accountable to the NSO. Similarly, National Managers of particular programs or business support activities form the Guiding Coalition[16], and are accountable to the CEO and the Board of Management. This governance structure underpins the accountability regime for BC in Centrelink.

2.12 At the outset of the audit, Centrelink had separate units responsible for BC and EM, respectively. However, during the time of audit fieldwork, Centrelink undertook a project to develop an integrated BC and EM framework, and to achieve other related objectives. The project was completed in June 2003. It is currently being evaluated by Centrelink's Business Improvement Committee to determine funding and implementation details.

2.13 As a result of work for this project, Centrelink has recently established a Business Continuity and Emergency Management team within the Service Integration Shop. The team, as the name implies, is responsible for the management and co-ordination of BCM and EM. However, there is also a separate IT Service Continuity Management team, with responsibilities for I&T continuity issues.

2.14 The ANAO supports these structural changes as they should improve alignment between BCM and EM in Centrelink. However, as these changes are very recent, the ANAO has not been able to establish the extent to which they have improved alignment between BCM and EM in Centrelink. The ANAO cautions that, in implementing these changes, Centrelink must clearly distinguish the objectives and operating requirements of BCM and EM.

---

[16] The Guiding Coalition is Centrelink's internal corporate board, comprising all of Centrelink's Senior Executive Service officers.

2.15 To further support the management of BCM and EM, the ANAO suggests that Centrelink examine higher-level responsibility arrangements for BCM, EM and risk management. It should also consider mechanisms to better align these responsibilities.

2.16 The ANAO also supports these structural changes, as they apparently allow a single unit to have a widely recognised and accepted role to co-ordinate and oversight BCM across the organisation, outside a technology line area. The ANAO emphasises the need for a unit to have a clear and unambiguous oversight responsibility for BCM, even if this requires it to oversight I&T BCM activities undertaken by a separate unit.

More comprehensive overarching management of BCM and EM within Centrelink

2.17 The ANAO is aware of better practices in BCM, where organisations have clear formal systems for central oversight and analysis of all BCM plans and strategies. This better practice typically requires that all responsible units regularly submit BCM plans (for example annually) that have been reviewed, and where necessary updated. This provides an assurance (including evidence) that all units have satisfied recommended minimum standards, especially regarding plan maintenance, training and rehearsal. These organisations often compare unit plans internally for benchmarking purposes, to improve quality by disseminating better practices, and to report on performance.[17]

2.18 Centrelink does not presently have a central area providing this level of guidance and support for BCM or EM. Recent organisational changes have prepared the Business Continuity and Emergency Management team for this role. However, it currently does not recommend minimum standards for plan maintenance, rehearsal and training for all relevant areas of Centrelink; monitor and report performance against such standards; or regularly and formally analyse centrally collected information to control quality and disseminate better practices.

2.19 The ANAO considers that implementing 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. Such a system would also raise the profile of BCM and EM in Centrelink.

2.20 The ANAO recognises that Centrelink's distributed network model (which involves Area Managers who, as stated earlier, are not subject to formal direction

[17] Performance measures often include the percentage of areas or entities that satisfy the specified BCM requirements (i.e. have updated and revised plans, and have undertaken the agreed training and rehearsal).

from the NSO, and report directly to the CEO) has implications for the implementation of overarching management of BCM and EM within the agency. In this circumstance, it would be more appropriate for the NSO to recommend that ASOs, CSCs and Call Centres adhere to standards for BCM and EM, rather than directing them to implement the standards.

Recommendation No.1

2.21 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.

Centrelink response

2.22 **Agreed. Action Commenced**. Centrelink has developed strategies for plan maintenance and rehearsal. Centrelink has developed training to provide appropriately accredited staff as per Recommendation No.5. Centrelink acknowledges the importance of monitoring and reporting performance against prescribed standards and will develop mechanisms to do so. Regular analysis will be undertaken to assist in quality control. Centrelink is satisfied that its recently revised Business Continuity and Emergency Management framework provides clarity of responsibilities and an effective organisational construct for the direction of enterprise-wide activities and responses when circumstances dictate.

Overarching document on BCM in Centrelink

2.23 In undertaking research for this audit, the ANAO had some difficulty in quickly obtaining information outlining comprehensively but succinctly Centrelink's BCM framework and processes.

2.24 The ANAO found that much of this information was contained in a number of separate documents. However, Centrelink was initially unable to

provide clear information about which documents contained relevant BCM information, whether the documents were comprehensive, and whether they were up-to-date.

2.25 The ANAO is aware that a number of other organisations have developed a single overarching BCM document that comprehensively outlines the organisation's approach to BCM. These organisations regularly update the document to ensure that there is certainty about its currency. Overarching BCM documents are also used for staff awareness and training, to inform stakeholders and for other purposes including audit and for briefing new senior managers.

Recommendation No.2

2.26 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.

Centrelink response

2.27 **Agreed. Action Commenced**. The current Business Continuity and Emergency Management project objectives include:

- clearly defined disaster and emergency management processes supported by an integrated framework that is consistent with Centrelink's National Plans. This framework provides a guide and templates for the preparation,

testing and maintenance of business continuity and emergency management plans;

- introduction of corporate policy, controls, procedures and associated guidelines consistent with ANAO recommendations for Business Continuity Management; and
- linkage of Business Continuity Plans, Disaster and Emergency Management Plans and procedures for National Support Office, Area Offices and Customer Support Centres.

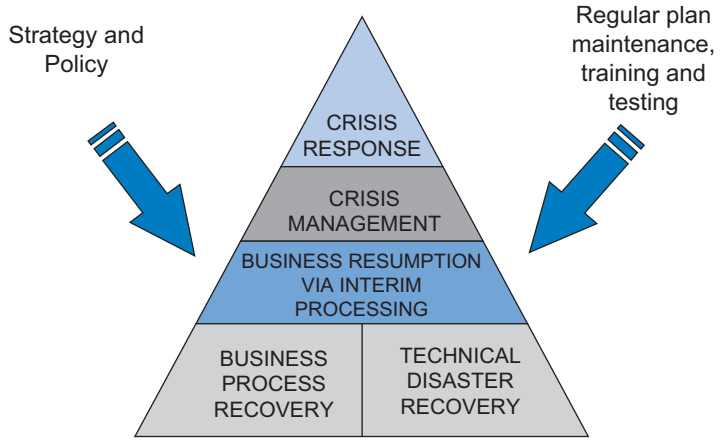
Layers of BCM in Centrelink

2.28 BCM in Centrelink is a broad concept, encompassing:

- an initial response to crises;
- a framework for managing crises;
- alternative treatment methods if critical business systems are interrupted (BC involving interim response); and
- the recovery of critical business systems (business process restoration).

2.29 Accordingly, Centrelink's BCM framework addresses all the main elements of BC outlined in the better practice literature, as illustrated in Figure 2.1 and discussed below.

Figure 2.1
Relationships between elements of effective BC arrangements



Source: Adapted from diagram provided by Business Services and Resources to ANAO in 2003.

Crisis Response

2.30 An important element of crisis response[18] is the use of procedures to ensure that issues are escalated appropriately, and that the crisis leadership is notified promptly. Centrelink has a Business Disruption Notification Guide that 'sets out the problem escalation procedures to be used in response to incidents that disrupt Centrelink's business.'[19] It provides guidance to staff on the nature and likely seriousness of a disruption, which determines what actions should be taken, and especially who should be notified.

2.31 The ANAO found that this guide provided a sensible approach to notification and escalation of business disruption, as it clearly identifies the various levels of escalation, the conditions that apply to each level, and who should be notified.

2.32 Centrelink is often required to address immediate crisis response through evacuation procedures, as well as liaison with community emergency service providers following an evacuation. During fieldwork for this audit, the ANAO observed incident and evacuation procedures at different points in the network. Responsibility for alarm and evacuation testing rests with site managers. Technical testing of fire and personal safety alarms and other safety equipment is a landlord responsibility and is scheduled and monitored by the leased property manager. The exception to this practice is Tuggeranong Office Park, where Centrelink takes direct responsibility for testing and maintenance, conducted on the agency's behalf by a contractor.

Crisis Management

2.33 Crisis Management in Centrelink is based around:

- Crisis Management Team notification procedures (discussed above);
- the Business Resumption organisational structure, including:
  - — the Crisis Command Centre structure and operation; and
  - — the operation of and interaction between Centrelink Business Resumption Teams; and
- Crisis Plans and associated implementation actions.

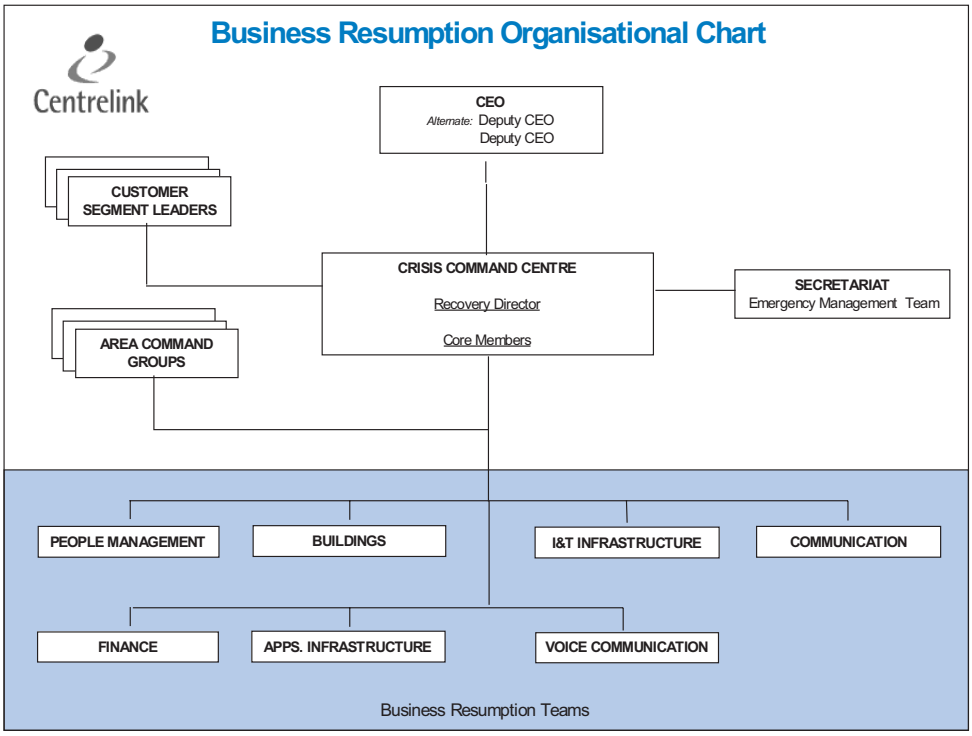
2.34 The main governance structure for managing internal crises in Centrelink is established through the interaction of Centrelink's Crisis Command Centre and the Business Resumption Teams, as illustrated in Figure 2.2.

---

[18] This is often referred to as 'emergency response', but here the term 'crisis response' has been used to avoid confusion with 'community emergency response', and for consistency throughout the audit report.

[19] <http://centrenet/homepage/nso/iandt/security/buscont/framework.htm>.

Figure 2.2
Centrelink's Business Resumption Organisational Chart



Source: Centrelink 2003. (Names and locations not identified by ANAO for privacy and security reasons).

2.35 The Crisis Command Centre consists of key executive personnel who will be involved in critical business decisions when a business disruption event occurs. Business Resumption Teams have a dual role. They have a planning and preparation role, being responsible for the development and implementation of BC strategies in readiness for a disaster; and a crisis management/business resumption role, being responsible for the invocation of the BC strategies they have developed.

2.36 The ANAO found that this structure provides an effective framework for managing crises, because it:

- is based around a Crisis Command Centre structure that empowers a Recovery Director to manage the response to a crisis, with input from the appropriate high level executives, including the CEO and Deputy CEOs;
- includes the appropriate managers from Centrelink's network;
- specifies appropriate Business Resumption Teams—the main business enablers that may be needed to recover from a crisis; and

- clearly defines the roles and responsibilities of the key BC participants in responding to and managing a crisis.

2.37 The ANAO observed good co-operation and interaction between all levels of Centrelink during a crisis. This interaction is specified in the framework, including the Crisis Plans, and appears to work well in practice—as evidenced in Centrelink's response to the Warrnambool CSC fire (see Appendix 2).

2.38 However, the audit identified a number of shortcomings with the Crisis Command Centre, in particular that: both primary and alternate Crisis Command Centres are not currently outfitted for their intended use; and documentation boxes for Business Resumption Teams are not located in the Crisis Command Centres or with the teams.

Business resumption through interim processing

2.39 A critical layer of better BCM practice involves business resumption strategies and plans. These typically involve interim process or contingency measures that enable business processes to continue, prior to the restoration and resumption of primary business processes. Centrelink addresses these business resumption strategies mainly through its BC and related plans in the NSO and throughout the network. These are discussed in subsequent chapters, especially Chapter 4.

2.40 Centrelink generally has an adequate framework to implement business resumption strategies. Particular strengths of Centrelink's approach include:

- the flexibility of the network to cover losses of individual offices (that is, if a CSC or Call Centre is lost, business can generally be quickly diverted to neighbouring or other similar offices);
- the effectiveness of flying-in technology and other resources from the NSO and/or an ASO to any point in the network;
- business owners of the critical business processes having developed, and being responsible for, business resumption measures; and
- the skills, knowledge and commitment of staff.

2.41 However, Centrelink's major limitations in business resumption (through interim processing) include:

- insufficient rehearsal of BCM strategies and plans (see paragraphs 4.48 to 4.55);
- inadequate formal training of key staff (see paragraphs 4.60 to 4.69);

- a bottom-up approach to plan development (that is, filling in template plans, with insufficient scrutiny of whether they have been fully tailored for each circumstance (see paragraph 4.39); and
- a lack of preparation for unlikely but potentially severe crises (see paragraphs 5.58 to 5.62).

Business process restoration, including technology disaster recovery

2.42 The continued functioning of Centrelink's I&T hardware and applications is critical to virtually all its key business functions. Thus, it is a key element of Centrelink's BC strategies. Centrelink has a range of disaster recovery procedures that provide hardware backup, environmental backup, data backup and recovery procedures to be invoked in the case of a crisis. Chapter 5 examines these procedures, and identifies a number of shortcomings.

2.43 The ANAO concludes that Centrelink generally has an appropriate framework for BCM and EM and has apparently been successful to date in delivering services continually and responding to emergencies. The ANAO considers, however, that despite reforms to BCM and EM structures and practices, there is scope to further improve governance and accountability arrangements for BCM and EM.

3. Alignment of Risk Management and BCM in Centrelink

This chapter discusses the alignment of risk management and BCM in Centrelink. It focuses on the effectiveness of processes to ensure that risk management contributes to achieving BCM objectives.

Background

3.1 Risk management and BCM are essential parts of good corporate governance. Risk management processes influence the strategic direction of the organisation. BCM ensures that essential functions of the organisation can be continued. These two disciplines should be implemented as ongoing processes, or programs, within an organisation—rather than treated as 'projects' that are done once and then forgotten.

3.2 Although the two disciplines have clear points of contact, at the operational level they can operate with minimum overlap. However, there needs to be sufficient cooperation and information flows between risk management and BCM to ensure that they achieve their respective objectives.

3.3 This chapter focuses on how effectively risk management contributes to achieving the objectives of BCM in Centrelink, as indicated in Figure 3.1. However, it first briefly outlines better practice risk management, the nature of interaction between BCM and risk management, and risk management in Centrelink.

Figure 3.1

Potential benefits from aligning Centrelink's risk management and BCM efforts

Contribution of risk management to achieving BCM objective [A]	*Implication for BCM*
Provides risk management approaches to be used in BCM.	• Ensures BCM uses a similar risk approach to that used in risk management, to achieve consistency and to reflect better practice.
Provides a top-down approach to complement the BCM bottom-up approach.	• Ensures pro-active controls (often reducing likelihood of events via risk management) and corrective controls (often reducing consequences of events via BCM) are complementary. • Risk management and BCM each identify the same critical business functions. • Risk management adopts similar risk treatments to BCM.
Provides processes for treating risks in new projects thereby contributing to BCM.	• Processes for establishing new projects treat risk and BCM simultaneously and consistently.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) The prime objective of BCM is to ensure that essential functions of the organisation can be continued.

Better practice risk management and its interaction with BCM

Better practice risk management

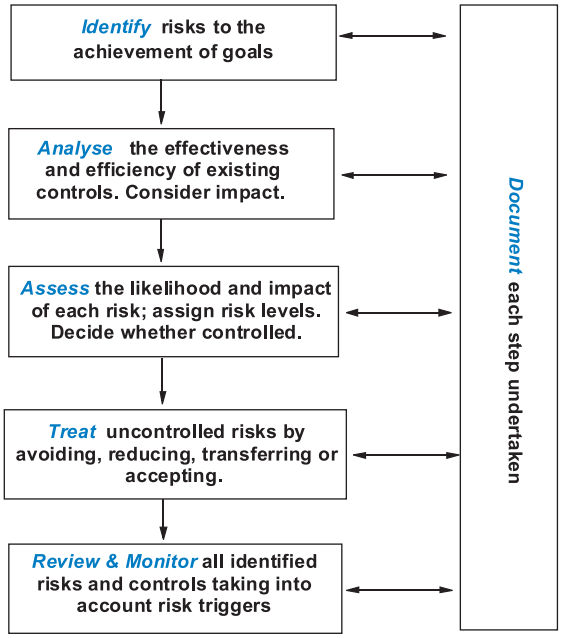
3.4 Standards Australia's AS/NZS 4360 outlines widely accepted better practice approaches to risk management. Centrelink has adopted this framework and methodology (see Figure 3.2).

3.5 AS/NZS 4360 considers risk to be an 'event that could impact on the achievement of goals ... Anticipating these events, including assessing their likelihood and impact, and doing something about it, is risk management.'[20]

3.6 AS/NZS 4360 proposes a risk management framework, where risks are identified, analysed and evaluated. At some point in the process the organisation must decide if a risk is acceptable. If not, then various risk treatment options can be applied, including:

- avoid the risk;
- transfer the risk (in full or in part);
- reduce the risk likelihood; and/or
- reduce the risk consequences.

Figure 3.2
Centrelink's Risk Management Guidelines



Source: Centrelink, Business Assurance, Risk Management Guidelines, 2003.

Nature of interaction between BCM and risk management

3.7 A holistic BCM approach will include treatments to reduce the likelihood of a crisis, as well as its impact. However, if risk management treatments have adequately reduced the likelihood of risk events occurring, then effective BCM can simply focus on mitigating impacts, including those of worst-case scenarios.

3.8 In any case, one of the most important aspects of the alignment of risk management and BCM is to ensure that for each critical business process, preventive controls have been considered (and often implemented) that recognise, and are consistent with, corrective controls, and vice versa.

3.9 Often the BCM process will need to include strategies to address risks and their potential impact that have not been identified by the normal risk management processes. The BCM process will also need to address risks which have been accepted as very low probability by the risk management process but which, if realised, have a high potential impact.[21]

---

[20] Standards Australia 1999, Australian/New Zealand Standard AS/NZS 4360:1999 *Risk Management*.

[21] BCM can be used in conjunction with 'Emergency Risk Management' (ERM), which aims to measure and address these types of 'low incidence–catastrophic consequence' risks. ERM theory has been developed by Emergency Management Australia and is used extensively by emergency management response and recovery stakeholders across Australia.

3.10 Subsequent to the terrorist attacks of 11 September 2001, many organisations now consider possible extreme events in their BCM planning, especially if they are emerging risks. However, this does not appear to be the case at Centrelink, which still does not typically consider, and develop strategies to cater for, extreme events. For example, Centrelink's BCM approach does not currently address the potential for the simultaneous destruction or damaging of both of its data centres (see Chapter 5).

Risk management in Centrelink

3.11 Risk management forms part of Centrelink's Quality Assurance Framework, and is an integral part of planning and operations in Centrelink. Centrelink has a *Risk Management Policy* and *Risk Management Guidelines*, which provide a structured approach to risk management in Centrelink, consistent with AS/NZS 4360.

3.12 As part of its strategic planning, and outlined in *Centrelink's Future Directions 2003-06*, Centrelink identified a number of strategic risks to achieving its mission and goals. One of these strategic risks was failure to 'maintain business continuity'. Treatments for strategic risks are outlined in Centrelink's Business Plans.

3.13 Centrelink's latest Business Plan, *Business Plan, 2003–2004,* reports initiatives to deliver the Plan for five specified goals. Associated implementation actions can, with varying levels of difficulty, be linked to Centrelink's strategic risks. The Business Plan is linked with other documents and plans, including Business Improvement Plans, which can include strategies to address BC risks.

3.14 However, Centrelink's *Business Plan, 2003–2004* does not clearly outline how Centrelink would address the strategic risk of failure to 'maintain business continuity'. The ANAO suggests that subsequent Business Plans provide clearer guidance about how Centrelink is addressing this strategic risk.

Alignment of risk management and BCM in Centrelink

3.15 This section examines processes to align BCM and risk management in Centrelink, according to the criteria outlined in Figure 3.1, namely:

- the use of common risk methodologies in BCM and risk management;
- how BCM and risk management complement each other, especially to ensure that preventive controls consider and align with corrective controls; and
- the use of consistent and coordinated processes to treat risks and BCM in new projects.

Common risk methodologies for BCM and broader risk management

3.16 As explained earlier in this chapter, Centrelink implements a better practice risk management methodology, based on AS/NZS 4360 and described in formal risk management documents. This methodology has been supplemented by Centrelink's Risk and Business Assurance Branch (responsible for risk management in Centrelink) delivering many risk management workshops throughout Centrelink to increase the consistency of applying risk management across the organisation.

3.17 Centrelink applies this methodology to a range of risk strategies and documents including the strategic planning process, risk management plans, project plans and Business Improvement Plans.

3.18 The ANAO found that most BCM related plans and processes incorporated a risk management process consistent with that used for broader risk management in Centrelink, based on AS/NZS 4360. This included consistent risk treatments in many BCPs.

3.19 However, the ANAO notes that:

- there is a wide divergence in the nature of BCPs and related plans used in Centrelink's network (see Chapter 2), partly stemming from a lack of consistency of risk methodologies applied throughout the network; and
- some BCPs and related plans focus too much on applying a standard risk management approach, rather than concentrating on BCM specific aspects such as crisis management, establishing interim processing arrangements, and recovery of critical operations.

3.20 The ANAO notes that Centrelink is in the process of standardising risk management methodologies throughout its network, based on risk management criteria developed by the Risk and Business Assurance Branch. Furthermore, the BC and EM framework project will consider improving the quality and consistency of BCPs and related templates, including by examining risk management approaches.

3.21 The ANAO suggests that the BC and EM framework project (see paragraph 2.12) or alternative projects, also examine and if considered appropriate, develop strategies to improve the consistency of risk management approaches between BCM and broader risk management in Centrelink. This could include teams acknowledging the status of BCM planning in their general business plans and risk management plans.

Complementarity of BCM and risk management

3.22 BCM and risk management need to complement each other so that risk treatments provided through risk management processes and plans are consistent with those provided through BCM. In particular, it is important that preventive treatments for risks identified through risk management processes align with corrective treatments that are also often a part of BCM.

3.23 To examine the complementarity of BCM and risk management in Centrelink, this audit focussed on:

- alignment of risk management processes and BCM treatment processes at the business unit level;
- the extent of interaction between key managers responsible for central oversight of risk management and of BCM; and
- the extent to which risk management processes identified and addressed risks associated with the critical business processes subject to BCM treatments.

Alignment of BCM and risk management at the operational level

3.24 Accountability arrangements in Centrelink deem National Managers to be responsible for both risk management and BCM. Accordingly, each National Manager is responsible for Business Improvement Planning, which is the prime mechanism for managing risk. They are also responsible for maintaining BCPs and training key staff, which are prime means of ensuring BC.

3.25 The ANAO considers this to be an effective means of co-ordinating risk management and BCM at the operational level. It helps to ensure consistency of approaches between the two disciplines for each individual business function. It also helps to ensure that preventive controls developed as part of risk management have compatible corrective controls developed via BCM.

Alignment of BCM and risk management at the overarching level

3.26 During fieldwork, the ANAO noted a relatively low level of interaction between managers of key units with overarching responsibility for BCM (especially the then Business Continuity Unit) and those with overarching responsibility for risk management (the Risk and Business Assurance Branch). This is partly explained by the governance arrangement that holds National Managers responsible for both BCM and risk management.

3.27 There is scope to improve the level of interaction between managers of risk management and BC/EM, in order to co-ordinate efforts to improve performance. A particular opportunity to do this should arise soon, as both the

Risk and Business Assurance Branch and the central unit responsible for BCM (the Business Continuity and Emergency Management team) plan to analyse risk management and BC plans they now collect throughout Centrelink, to disseminate better practices and generally improve overall quality.

Consistency of BCM and risk management identification of critical business functions

3.28 Centrelink has used Business Criticality Reviews to identify and treat critical business processes as part of BCM (see Chapter 4). However, Centrelink's Risk and Business Assurance Branch has not explicitly identified and given particular attention to risk management of critical business processes.[22]

3.29 In this circumstance, Centrelink's risk management approach to identifying critical business functions was consistent with that undertaken for BCM. By the same token, it also did not assist BCM efforts.

Processes to treat risks and BCM in new projects

3.30 Centrelink has established a project management process that requires all new projects to have a BC section in the Project Management Plan, unless there are no grounds why it is needed (see discussion in paragraphs 4.17 to 4.24). The Project Management Plan also requires the Business Manager to complete a Risk Management Plan, in accordance with Centrelink Risk Management procedures.

3.31 The ANAO considers this to provide an effective framework for treating both BC and risk in new projects. However, the ANAO notes that a lack of central recording and oversight of the BC elements of new project management plans casts some doubt on the effectiveness of this process to adequately address BC issues of new projects.

3.32 The ANAO concluded that risk management and BCM in Centrelink are well aligned at the operational level, although there is scope for further improvement. There is also scope to improve communication between managers with overarching responsibility for BCM and risk management. This would improve BCM in Centrelink by reducing the higher-level 'silo' approach to BCM and risk management and re-inforcing the top-down and bottom-up approaches to both risk management and BCM.

---

[22] Instead, the Risk and Business Assurance Branch has recently focused on disseminating better risk management practices throughout the network.

4. Approaches to Implementing BCM in Centrelink

This chapter discusses the approaches used to implement the main elements of BCM throughout Centrelink.

Introduction

4.1 The framework for BCM in Centrelink, reported in Chapters 2 and 3, requires appropriate organisational processes to deliver desired outcomes.[23] Strategic choices and policy design can ensure that a BC culture is encouraged and supported within an organisation. Plans provide a basis for successful responses to disruptions, but need to be supplemented by rehearsal and training, and the knowledge, skills, judgement and involvement of appropriate staff. Better practice BCM must also focus on entire business processes, be business driven (i.e. linked to critical services) and be supported by senior management.

4.2 To examine the main processes required to deliver Centrelink's BCM framework, the ANAO assessed Centrelink's current practices and performance against the guidelines in the ANAO's Better Practice Guide on BCM[24] (see Figure 1.1 of Chapter 1 for a summary), focusing on:

- project initiation;
- identifying critical business processes and undertaking a business impact analysis;
- designing treatments;
- implementing treatments (especially plans);
- rehearsal; and
- training and awareness.

4.3 As Centrelink has maintained a consistent approach, and the audit has consistent findings for many elements of BCM, this chapter discusses findings broadly for Centrelink as a whole. Subsequent chapters examine continuity strategies for individual business enablers in Centrelink.

---

[23] Most importantly, the continuation of critical business processes quickly enough to ensure business objectives are not compromised.

[24] ANAO, op. cit.

Project initiation

4.4 The ANAO BPG emphasised that all projects establishing business continuity plans or strategies should be managed according to good project management principles. In particular, the BPG provided a checklist for project initiation that would provide a basis for audit, outlined in Figure 4.1 below. The ANAO BPG added that 'business continuity projects should be prepared by managers who understand the business and reflect the organisation's approach to risk management.'[25]

Figure 4.1
Checklist for the development of a BC project plan

- Document the project's objectives.
- Define and document the project's scope and limitations.
- Explain any assumptions made.
- Assign responsibility for project tasks.
- Present the budget, including staff resources, required for the project.
- Set project timeframes and deliverables for tasks.
- Plan is formally approved by Chief Executive and/or appropriate management committees.

Source: ANAO 2000, *Business Continuity Management, Keeping the Wheels in Motion*, Better Practice Guide, p.35, January.

4.5 The impetus for the development of the BC strategies and plans that form the basis for Centrelink's current approaches were preparations for Y2K. As part of the effort to address the risks presented by Y2K, a concerted and co-ordinated effort was made over a relatively short space of time to develop and implement BC strategies and plans throughout Centrelink's network.

4.6 While the ANAO encountered some difficulty in accessing and reviewing all relevant files and documentation, mainly due to incomplete records and delays in identifying staff with required corporate knowledge, information provided by Centrelink indicated that there was a clear management structure for the Y2K preparation process. A high level and broad ranging steering committee was formed, which involved relevant Centrelink staff and also drew on the advice of consultants with expertise in BCM. This steering committee used the Business Continuity Unit (BCU) for many of the project management

[25] ibid., p. 31.

and secretarial tasks. As it was an integral part of the high profile Y2K effort, the project attracted high-level support. The BC elements had clear outputs, milestones, roles, responsibilities and costings.

4.7 Throughout 1999, in preparation for Y2K, the BCU worked with Centrelink Business Resumption Teams and Area Support Offices (ASOs) to develop and implement Business Continuity Plans (BCPs). For example, Area planning workshops were held and continuity plan templates and rollover checklists provided. Additionally, a consultant ran a major crisis management simulation (Exercise Brolga) in September 1999. As a result of that exercise, and subsequent follow-up discussions with key participants, the consultant worked with Centrelink staff to develop draft crisis plans for each of the Business Resumption Teams and for the Crisis Command Centre. The consultant and Centrelink staff also refined the roles and responsibilities of key personnel in the Areas and teams.

4.8 The ANAO considers that Centrelink planning of projects to initiate these key BC projects, including BCPs, was undertaken according to the principles of good project management.

Identify critical business processes and undertake a Business Impact Analysis

4.9 An effective BC regime must have strategies and plans in place to respond to outages in all business processes critical to delivering outputs and achieving other business objectives. Accordingly, an important element of this audit was to establish whether Centrelink's BC strategies and plans covered all its critical processes and would therefore ensure that all services could be recovered sufficiently quickly to enable Centrelink to meet its specified business objectives and performance targets.

4.10 To ensure sufficiently comprehensive coverage of BC within an organisation, it is necessary to identify all key business processes, then analyse the impact of their interruption in order to establish the maximum length of time they can be interrupted before business objectives are comprised—the maximum acceptable outage. These two steps are often referred to as 'key business process identification' and 'Business Impact Analysis' (BIA).[26] Figure 4.2 provides checklists for identifying critical business processes and undertaking a BIA.

[26] See for example, ibid., pp. 32–38.

Figure 4.2

Checklists for the identification of critical business processes and undertaking a Business Impact Analysis

Key Business Process Identification

- Document and confirm organisational objectives and outputs.
- List key business processes (and associated activities and resources) that underpin achievement of objectives and delivery of outputs.
- Interview managers responsible for key business processes.
- Effectively use and communicate this information in other stages of project development.

Business Impact Analysis

- Evaluate the impact of the loss of a process on the organisation.
- Identify critical success factors that ensure the process meets the organisation's objectives.
- Identify interim processing procedures to be adopted during the recovery phase.
- Quantify the minimum resource requirements necessary to perform the activity.
- Evaluate the adequacy of current BC measures in place.

Source: ANAO 2000, *Business Continuity Management, Keeping the Wheels in Motion*, Better Practice Guide, p. 37, January.

4.11 Centrelink has established two main mechanisms to identify key business processes and undertake a BIA, namely Business Criticality Reviews and continuity requirements to be addressed when planning new projects.

Business Criticality Reviews

4.12 To date, three Business Criticality Reviews have been undertaken in Centrelink—two by a consultant, in 1997[27] and 1998, and another by Centrelink staff, refining the earlier methodology, released in March 2002.

4.13 The ANAO found that the 2002 Business Criticality Review document, and the process used for its development, represented a reasonable approach to key business process identification and BIA, as it generally satisfied the criteria outlined in Figure 4.2. In particular, it addressed some of the more difficult aspects of this process including: establishing activities and resources critical to key

[27] In 1997, the former Department of Social Security was responsible for the business processes now operated by Centrelink.

business processes; detailing interdependence between activities and resources; providing an agreed priority ranking of the critical processes and systems; and establishing maximum acceptable outages for each key process. Importantly, the review consulted extensively throughout the network—involving 270 staff in 44 locations.

4.14 However, a number of issues that should have been included in the business criticality development process were not, including:

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

4.15 Centrelink has recognised these shortcomings in the criticality review processes. It has advised the ANAO that it will undertake another Business Criticality Review in 2003–04, which will consider data and telecommunications systems. This project will also check whether maximum acceptable outages are realistic.

4.16 The ANAO supports Centrelink's intention to undertake a further Business Criticality Review in 2003–04, and notes that it should address the limitations of the current Business Criticality Review document, outlined above.

Business Process Identification and BIA Components of New Project Planning

4.17 Existing business processes have been subject to the Business Criticality Review, which, with the exceptions outlined above, provides adequate identification of critical processes and BIAs.

4.18 To ensure new projects have adequate BCM treatments, Centrelink has established a project management process that requires the completion of a BC section in the Project Management Plan for all new projects, unless there are no grounds why it is needed. The Project Management Plan also requires the Business Manager to complete a Risk Management Plan, in accordance with Centrelink Risk Management procedures.

4.19 Completion of the BC section in the Project Management Plan involves the identification of the mission critical business elements, and determination of what the impact would be upon Centrelink's goals if these elements were disrupted or lost. Risk assessments are then to be conducted to identify threats to these processes.[28]

---

[28] <http://centrenet/homepage/nso/iandt/security/buscont/howto.htm>.

4.20 The ANAO considers that this is an effective process for treating BC, as it requires all projects that involve critical business processes to complete BC strategies, prior to project approval. It also allows the Risk Management Plan for a project to be aligned to the risk treatments contained in the BCP.

4.21 Given the ANAO's broad agreement with the framework for treating BC in the project management process, the ANAO undertook a brief analysis to gauge the extent to which this process was implemented in practice. The results are reported in detail in Appendix 3. In brief, they indicated that:

- BCPs had been prepared for only a small number of established projects;
- the BCU adopted a passive approach to collecting BCPs, as it maintained only a small number of plans for projects;
- the BCU acknowledged its lack of authority to question or overrule the decision of project managers regarding the need to prepare a BCP; and
- the Centrelink Projects Office did not have readily accessible automated or hard copy records of plans; including copies of BCPs.

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

Recommendation No.3

4.23 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 coverage 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.

Centrelink response

4.24 **Agreed.** All new, approved and funded projects will be required to identify and address business continuity issues arising from those projects and this information will be drawn together to provide a comprehensive view.

Design treatments

4.25 The literature on BCM[29] typically devotes considerable attention to designing continuity treatments, prior to implementation. Treatment design involves identifying and evaluating treatment options to reduce the impacts of losing critical business processes, implementing alternative interim processes and restoring normal operations. These options need to be compared focusing on resource inputs, costs, risks and, ultimately, recovery timeframes compared to the maximum acceptable outage.

4.26 As discussed in paragraphs 4.6 and 4.7, Centrelink undertook a comprehensive program in 1999 to develop its BCPs and other treatments. The program involved extensive participation of staff across the network, advice from expert consultants, a major simulation exercise and the development of a BC template approach across the network (designed to be implemented by individual units according to circumstances).

4.27 The ANAO concluded that this process provided a sound approach to designing BC treatments, which Centrelink has since supplemented by introducing requirements to address BC in new projects.

Implement treatments—BCPs and related plans

4.28 BCPs and related plans are an important element of virtually all BC management strategies. However, it is important not to focus too much on the plans themselves, at the cost of other elements of the strategy, especially rehearsal and training. After all, the primary objective of undertaking BC planning is to provide a high level of assurance that an organisation can respond to a crisis, rather than to develop appropriate documented plans.

4.29 The ANAO BPG on BCM indicates that plans need to be developed as part of the broader risk management framework, and be consistent with structures that address the various phases of recovery, including crisis response and management, business resumption through interim processing and business process recovery.

4.30 The ANAO found that Centrelink's BC related plans cover, and are generally well aligned to, these recovery phases. These plans also generally incorporate risk management approaches. However, as discussed in Chapter 3, there is scope to improve the integration of BC related risk management efforts with broader risk management in Centrelink.

---

[29] Such as ANAO, op. cit, p. 39.

4.31 Figure 4.3 describes the many types of plans underpinning Centrelink's BC strategies and responses.

Figure 4.3

Centrelink's current BCPs and related documents

Type of plan	*Description*
Crisis Command Centre and Business Resumption Team Crisis Plans.	Checklists and information for each of the Crisis Command Centre members and resumption teams, which are normally invoked in the event of an emergency that has a large impact on Centrelink or its customers.
BCPs.	Have an internal focus and document risk minimisation strategies and alternative strategies for continuing business if a risk is manifested. These plans are brought into effect whenever normal business processes are interrupted.
Site BCPs.	Used primarily by Customer Service Centres and Call Centres for addressing disruptions to onsite services/ facilities.
System BCPs.	Used primarily by Project Managers for emerging projects and systems/applications intended to deliver new functionality or service.
I&T Disaster Recovery Plans.	Used for developing I&T Platform Disaster Recovery Plans. Examples of I&T platforms include mainframe, COLFrame, mid-range, network servers, intranet, internet.
Evacuation Plans.	Local plans in place for each office.

Source: Centrenet/homepage/nso/bc-em/index.htm

4.32 The ANAO examined these plans and related documents against guidance provided by the ANAO BPG and similar core literature, including the criteria outlined in Figure 4.4 below.

Figure 4.4

Checklists for developing BCPs and related documents

- Roles and responsibilities of key continuity players are clearly identified and co-ordinated.
- Communications and information channels are adequate, including throughout the various levels of Centrelink—NSO, ASO and CSCs.
- BCPs are comprehensive yet concise and easy to access.
- BCPs include or reference associated risk mitigation processes.
- Limitations of BCPs are clearly spelt out.
- Plans have appropriate version control and event logs and are up-to-date.
- Disaster escalation procedures exist and are well known.

Source: Based on ANAO 2000, *Business Continuity Management*, *Keeping the Wheels in Motion*, Better Practice Guide, January.

4.33 The methodology for testing these plans involved an examination of:

- core templates used, especially for crisis plans and BCPs;
- selected plans to gauge how they are implemented in practice, and particularly how they are tailored to cope with specific circumstances; and
- coverage of plans across the network and the business processes they are designed to cover.

4.34 The ANAO found that Centrelink's BCPs and associated plans were formulated to be consistent with the methodology and principles of core BCM literature[30], including the ANAO BPG. Typically, plans separately cover Crisis Plans—to organise the governance and management of the crisis—and BCPs, that outline alternative strategies for continuing business after an interruption.

ANAO analysis of common Centrelink continuity plans: Crisis Plans, BCPs and Emergency Management Plans

4.35 The ANAO found that Centrelink's plans at the NSO level generally adhered to the criteria outlined in Figure 4.4, reflecting the appropriateness of the template approach developed by the agency in conjunction with its consultants. This particularly was the case for Crisis Plans for each of the national Business Resumption Teams and for the National Crisis Command Centre.

[30] Core BCM literature is described in Chapter 1 at paragraph 1.4.

4.36 However, the ANAO identified considerable variation in the plans used across the wider network, especially for ASOs and CSCs. These plans had a range of formats, names and purposes. As Centrelink generally implements recovery strategies that include 'flying squads' who depart from the NSO to assist local recovery efforts, the ANAO would expect to see a greater degree of consistency between plans, to assist staff to understand more easily what is required of them.

4.37 The ANAO also found that many of the local plans (ASO and CSC) do not differentiate between their obligations under a local community emergency plan, and the need to respond to disruptions to their own operations. This was the case even though many offices have had recent experience of both types of disruption. Many of the local office plans examined by ANAO really only focused on Centrelink's response to broader community emergency needs.

4.38 Furthermore, the majority of local BCPs do not clearly articulate the roles and responsibilities of a crisis management team, nor do they generally outline how the NSO, Area and local staff will work together in response to a crisis. This contrasts with NSO practices, where a detailed Crisis Management Team is usually established and where plans differentiate between managing the crisis and recovering the business. The ANAO considers that Centrelink's local plans could be improved by adopting a similar approach to that used by the NSO.

4.39 In general, local plans display the normal failure of 'bottom up' documentation[31], that is, a lack of cohesion and common direction. They are often not clearly tailored to individual sites, with many sites simply adopting the core template risk ratings and continuity treatments, regardless of their particular circumstances.

4.40 Centrelink has recognised these limitations and is planning to address them through the BC and EM Framework project currently underway. In particular, the project will aim to improve local plans by providing a single template to improve consistency, streamline the contents, and clearly distinguish between the 'internal' BC treatments and 'external' emergency treatments. The project also aims to improve the linkages between Area plans and NSO plans.

4.41 As discussed in Chapter 2, Centrelink is also planning to analyse local office plans, using benchmarking and other techniques to disseminate better practices and provide other advice to improve the effectiveness of these plans.

---

[31] This style of implementation is characterised by head offices sending out standard template documents for remote offices to complete, and is based on a premise that a standard plan is better than none. This choice of method is curious given that NSO have taken the opposite approach, where having appropriately trained people is considered more significant than having a detailed plan.

Recommendation No.4

4.42 The ANAO recommends that 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.

Centrelink response

4.43 **Agreed. Action commenced.** Centrelink is currently revising business continuity plan templates in line with this recommendation.

Coverage of Centrelink network with BCPs and related plans

4.44 As part of audit fieldwork, the ANAO sought data to estimate the percentage of Centrelink's network that had provided BCPs or related plans to the BCU. This was used as a best estimate of the percentage of ASOs, CSCs and Call Centres that had such plans (see Figure 4.5).

4.45 Figure 4.5 indicates that virtually all Centrelink's network had some form of continuity or community emergency plan. However, the data also supports the ANAO's recommendation that Centrelink streamline the BCP and EMP templates and clearly differentiate between responses to internal and external crises, as many sites in Centrelink's network clearly do not adequately distinguish between the two.

Figure 4.5

Coverage of Centrelink network offices with BCPs or community emergency plans

Type of plan	*Number*	*Percentage of all sites*
BCP	219	64
Community Emergency Management Plan (EMP)	235	69
Either a BCP or EMP	334	97

Source: Information provided by Centrelink, March 2003.

4.46 The ANAO noted that the number of offices submitting plans increased rapidly throughout fieldwork for the audit. Together with an examination of many of these plans, this raised concerns that plans had been quickly developed from the templates, rather than fully adapted for local conditions.

Other Plans

4.47 Figure 4.5 also identifies other continuity related plans used in Centrelink, such as I&T Disaster recovery plans and evacuation plans. I&T Disaster Recovery Plans are discussed in greater detail in Chapter 5. Evacuation plans were discussed in Chapter 2. These chapters noted general satisfaction with evacuation plans and their integration with BC related plans but some scope for improvement in I&T Disaster Recovery Plans.

Rehearse and maintain plans and related strategies

4.48 Better practice demands BC to be a process not a project. That is, a continuous process providing continuous improvement, rather than a project done once and put on the shelf. Major components of this continuous process are rehearsal[32] and plan maintenance.

Rehearsal

4.49 The ANAO BPG states that 'testing and maintenance of the recovery process documented in the BCP will provide management assurance that the plan is effective—that is, it will ensure continuity of business should key functions be lost.'[33] The BPG also states that 'the major components of the BCP should be tested annually and updated based on the results of each test. It is important each component be individually tested'. It describes several types of tests, as outlined in Figure 4.6.

4.50 Centrelink is aware of the need for rehearsal and in advice to managers responsible for BCM, states 'once your BCP has been implemented, it is essential that it be regularly tested (to incorporate changes to the business environment) in order for it to remain valid.'[34] The advice to managers adds that tests can be done virtually or as a real live simulation and should focus on the validity and effectiveness of the plans. This advice emphasises that 'as a training tool, tests provide plan familiarisation, enhanced co-ordination and co-operation and communication as well as familiarisation with individual roles and responsibilities.'[35]

---

[32] The term 'rehearsal' is often used in the business continuity lexicon rather than 'testing'. Rehearsal conveys the idea of undertaking a simulation in order to learn from any identified shortcomings and to apply these lessons in a dynamic way. Testing suggests the simulation produces elements that were either successes or failures, which is unnecessarily negative and static.

[33] ANAO, op. cit., p. 62.

[34] <http://centrenet/homepage/nso/bc-em/plans.htm>.

[35] ibid.

Figure 4.6

Types of rehearsals for BCPs

Type of rehearsal	*Nature*	*Purpose*
Paper.	Calculates resources requirements.	Ensures sufficient resources available when BCP activated.
Manual verification.	Checks that all required resources are correctly stored off-site.	Ensures the required recovery material is available as stated in the BCP.
Supply validation.	Compares the list of supplies used during a test to the items documented in the BCP.	Validates all supplies required will be available in the event of a disaster.
Supplies, equipment and services.	Contact vendors to ensure that all information is accurate.	Ensures vendor information is accurate.
Structured walk-through.	Simulated disaster scenario.	Ensures the BCP procedures are adequate.
Unannounced recovery team assembly.	Contacts team members on the notification contract list.	Ensures timely mobilisation is possible.

Source: ANAO 2000, *Business Continuity Management, Keeping the Wheels in Motion*, Better Practice Guide, January, pp 62–63.

4.51 In recent years, Centrelink has undertaken two major simulations to rehearse, at the NSO level, its response to major disasters. These were 'Exercise Brolga' in September 1999 and 'Exercise Gravity' in November 2001. The ANAO found that both these simulations were useful exercises that provided valuable lessons to enable Centrelink to improve its BC capabilities.

4.52 The ANAO notes that there have been no such major training exercises involving Centrelink's ASOs and CSCs, even though Centrelink has had intentions to undertake such rehearsals for a number of years. More significantly, there was little evidence that staff in the Centrelink network regularly rehearse their roles, or that any other form of training for crisis response or BC has been undertaken on a formal and on-going basis. While some BCPs stipulate review periods, the ANAO was unable to establish whether any such reviews have taken place.

4.53 Centrelink recognises that it needs to increase its rehearsal of BCPs and related strategies. A proposed output from the BC and EM Framework project is a rehearsal regime for key plan components. Furthermore, the Business Continuity and Emergency Management Team intends to facilitate and manage crisis exercises with ASOs and CSCs that will rehearse both BCM and EM.

4.54 Centrelink has indicated that the BCM and EM rehearsal program to be developed as a result of the BCM and EM Framework project will adopt a risk management approach that may include a series of test programs with options it described as hypothetical, component, module and full.

4.55 The ANAO supports these elements of Centrelink's BC and EM Framework Project and suggests that the project, or a suitable alternative, is developed to overcome the limitations of BCM and EM rehearsal indicated earlier in this section.

Maintenance

4.56 Plan maintenance is separate to rehearsal, and involves updating BCPs and related plans on a regular, timely basis to ensure that contact details of key personnel are correct, and to incorporate any improvements, including advice from the NSO, lessons learnt from other parts of the Centrelink network, and changes to internal work practices.

4.57 Fieldwork undertaken by the ANAO indicated that some parts of Centrelink's network regularly update their plans. For example, Centrelink's offices in cyclone prone areas in Far North Queensland and Northern Australia typically update and review their plans prior to the onset of the cyclone season. Offices visited in other Areas also reported regular updating of contact lists to ensure that appropriate officers can be mobilised quickly in an emergency.

4.58 However, as discussed in Chapter 2, the ANAO identified a number of limitations in the higher-level management of BCM that precluded it from being able to provide a high level of assurance that maintenance of BCPs is undertaken on a systematic basis. In particular, there was no central guidance about the recommended level of maintenance (and rehearsal) of BCPs in the network or at the NSO, nor any analysis of whether it had taken place. This issue is dealt with in Recommendation No.1, which Centrelink is addressing, as part of its BC and EM Framework project.

Training and awareness

4.59 The literature on BCM and EM highlights the need to train key staff and to ensure sufficient organisational awareness about BCM requirements. For example, the Business Continuity Institute recommends that organisations prepare a program to enhance the skills required to develop, implement, maintain, and execute a BCP, and to create corporate awareness of BCPs more generally.[36]

[36] Business Continuity Institute, *Evaluation Criteria for Business Continuity Plans.*

Training

4.60 The Business Continuity Institute also advocates the development of a formal training program based upon common training approaches.[37] This can include the steps outlined in Figure 4.7.

Figure 4.7
Elements of formal training for BCM and EM

- Establish objectives and components of the training program.
- Identify functional training approaches.
- Identify personnel suitable for training using a needs analysis that compares present skills with required capabilities.
- Develop a training methodology.
- Acquire or develop training aids.
- Identify external training opportunities.
- Monitor the usefulness of training and use resultant information to continually improve the service provided.

Source: Business Continuity Institute, *Evaluation Criteria for Business Continuity Plans*, and general ANAO research.

4.61 The ANAO found that Centrelink does not have a formal approach to training staff in BCM and EM. Instead, Centrelink typically has an ad-hoc approach to such training.

4.62 Key Centrelink staff, particularly in IT Service Continuity Management and the Service Integration Shop, typically do receive appropriate training, including attendance at external courses such as those run by the Emergency Management Australia Institute and Survive Australia. However, the timing of this training is often later than optimal to maximise the benefits to staff and Centrelink.

4.63 As indicated earlier, a number of staff in the NSO have also attended major crisis simulations, and these provide valuable training. The process of updating and maintaining BCPs also provides on-the-job training, as do the general day-to-day activities of staff. The latter is often very relevant to many staff with BCM responsibilities, including those NSO staff on Business Resumption Teams.

4.64 The BC and EM homepages on Centrelink's intranet, Centrenet, also help with training and awareness, as they provide guidance to NSO and network staff about many facets of BCM and EM. This homepage is presently being

[37] ibid.

upgraded, with a repository of plans being populated rapidly, and information provided about developments to align IT Service Continuity Management and the Service Integration Shop as part of the new Framework Project. The individual homepages of CSCs and ASOs are also increasingly including BCM and EM strategies and plans. The ANAO supports this approach as it provides greater accessibility to plans and raises staff awareness about the existence and importance of these items.

4.65 As with many of the related elements of BCM and EM, such as rehearsal, plan maintenance and enhancements to the overarching management and quality control system, Centrelink has acknowledged the need to improve its approach to training staff in BCM and EM.

4.66 The current I&T Business Continuity Work Plan cites the option to develop BC training modules in liaison with the Virtual College. In addition, the BC and EM Framework Project specifies a training program that would:

- train Crisis Command Centre members and Business Resumption Teams;
- train Area and network staff involved in BC and EM response and recovery;
- provide training material for managers/staff involved in delivering ex-gratia payments; and
- develop generic detailed procedures, protocols, task cards and training packages for processing centre staff, including material for the Disaster Assistance Payments System (DAPS) and components.

4.67 The ANAO supports Centrelink's proposals to enhance its training of staff undertaking BCM and EM tasks, according to the broad parameters outlined in the BC and EM Framework Project and on the BC and EM homepage on Centrenet. The ANAO adds that Centrelink should examine, with a view to enhancing, information about BCM and EM provided in Induction Training Programs to new Centrelink Senior Managers and Executive level staff.

Recommendation No.5

4.68 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.

Centrelink response

4.69 Agreed. Action commenced. Centrelink has developed a training and exercise strategy for Business Continuity and Emergency Management in Centrelink. With the implementation of this strategy, Centrelink is confident that relevant staff will be appropriately trained and accredited for special and community response roles.

Awareness

4.70 One of the recommendations from Exercise Gravity was to undertake a publicity campaign to raise staff awareness of a number of elements of the BCM and EM framework including the Business Disruption Notification Guide, the Crisis Management Framework and the Disaster Response and Recovery Plan. This had not been done at the time of audit fieldwork to March 2003. The BC and EM Framework Project intends to consider this recommendation.

BC with external providers of critical services and commodities

4.71 Centrelink makes extensive use of external providers to deliver services and commodities that enable critical business processes within Centrelink, particularly I&T hardware, and voice communications and data connectivity-related products (see Chapter 5).

4.72 It is important that Centrelink's BCM approach focuses on the continuation of business critical processes, so to be effective, the BCM process needs to include an understanding of the minimum level of resources required from external providers of critical products and services. To do so, Centrelink needs to assess the risks of these critical external providers not being able to efficiently deliver the services for which they are responsible. This assessment requires understanding of the BC and disaster recovery capabilities of these service providers. The more central an external provider is to the delivery of a critical business function, the more crucial it is that their actual BC capability be understood. As in all aspects of BCM, it is the proven capability, rather than unproven claims, that needs to be understood.

4.73 Centrelink is a major Australian client for a number of very large companies. Centrelink is also a major user of the Model 204 Database Management System/development environment. Centrelink's choice of large, well-resourced external service providers, and the fact that Centrelink is a major client, may assist Centrelink to achieve priority restoration and maintenance of equipment and services if they were to fail. However, these attributes are not

sufficient in themselves to provide strong assurance about the capability of these critical external providers to support BC in Centrelink.

4.74 Taking regard of the issues discussed in paragraph 4.73, and based on observations from audit fieldwork, the ANAO considers that there are a number of areas where Centrelink should further investigate the scope, and take action if required, to minimise the risks of relying on external suppliers of critical equipment and services. These could include:

- checking whether supplier response times for required maintenance calls are actually achievable, compared to those specified in existing contracts and service level agreements;
- checking the physical capability of external equipment suppliers to deliver hardware in a crisis;
- checking on the level of technical disaster recovery capability specified in I&T related contracts;
- determining the ability of critical external suppliers to maintain their staff skills and expertise if a crisis were to affect their operations; and
- ensuring that key external personnel, vendors, suppliers of critical goods and services, and business partners are readily contactable in a crisis.

4.75 In regard to the above issues, Centrelink advised the ANAO that in order to spread its risk of reliance on individual providers, the agency has been adopting a contract panel strategy (that is, a number of suppliers are contracted to a panel to supply the same or similar services). However, this strategy has not yet been fully implemented across the full range of Centrelink's externally procured services and commodities. Centrelink also advised that the agency will commence analysing its supply chain in order to identify any externally supplied critical services or commodities that may require detailed BC risk assessments and treatments.

5. Implementing BCM in Centrelink: Critical Technology Related Business Processes

This chapter examines BCM of the critical technology business enablers in Centrelink.

Background

5.1 This chapter examines BCM approaches, practices and performance in Centrelink's critical technology business enablers, namely:

- I&T infrastructure and applications;
- telecommunications; and
- voice communications.

I&T infrastructure and applications

Overview of I&T infrastructure and applications

5.2 I&T serves a vital function at Centrelink. Most of Centrelink's outputs and activities depend on the robust and sustained delivery of I&T services. In 2001–02, expenditure for I&T exceeded $30 million and software assets accounted for more than $194 million.[38] Centrelink develops and manages I&T infrastructure internally but externally sources hardware supply and maintenance.

5.3 Centrelink presently operates two data processing centres, with its premier and secondary facilities both located in Canberra. Other strategic facilities include the Centrelink Network Operating Centre (CNOC), an off-site backup storage facility and an IT Support Centre. In addition, distributed computer facilities are situated at various locations throughout Australia, including the NSO in Canberra and ASOs and CSCs in major metropolitan areas and in regional and remote regions.

5.4 Figure 5.1 lists the principal components of Centrelink's hardware and system software environment.

[38] Centrelink 2002, *Annual Report 2001–02*, p. 236.

Figure 5.1

Principal Components of Centrelink's Hardware and System Software Environment

- Mainframes, mid-range (E10K), Infolink equipment, desktop PCs.
- COLFrame—a middleware framework that supports the development of Centrelink's business applications.
- Network servers, notes servers and communication platforms at the NSO, ASOs and CSCs.
- Intranet and Internet.
- Operating systems.
- Gateway security, logical security, physical security.

Source: Centrelink 2002, *I&T Platform Recovery Times*, 3 April; additional information provided by Centrelink, 2003.

5.5 Figure 5.2 identifies Centrelink's principal applications and its database management system.

Figure 5.2

Principal Applications/Databases and Definitions

Principal Applications/Database	Definitions
ISIS (Income Security Integrated System)	Provides the fundamental framework, upon which the benefit-specific processes are built. Assesses customers for payments and updates user circumstances.
Model 204	A database management system storing all ISIS customer information.
FAO/COS	An application supporting family assistance and childcare.
EDGE	An integrated expert system and decision-making tool used in Centrelink offices throughout Australia to connect customers with Centrelink payments and services.
MAPSTAT	A national 'street' directory, allowing staff to identify the location of offices and respective details. Used extensively within Call Centres to direct customers to their closest office.
Online Services for Customers	Provides the ability for all customers to access their Centrelink information via the Internet. Previously known as Customer Services Online, or 'CSO'.
Centrepay	A voluntary direct deduction service available for customers for payment of ongoing expenses.
Infolink	An automated package, which includes financial accounting, human resources reporting/recording, payroll.

Source: Information provided by Centrelink, 2003.

5.6 Of all these applications, Centrelink considers ISIS and its supporting Model 204 database as most critical to its operations, as they process customer payments.

Audit methodology to analyse I&T infrastructure and applications

5.7 To review BCM of Centrelink's I&T infrastructure and applications, the ANAO:

- drew on better practice outlined in the ANAO BPG[39];
- used the *Control Objectives for Information and Related Technology* (CobiT)[40];
- used ISO/IEC 17799 *(IT Code of Practice for Information Security Management)*;[41]
- examined Centrelink's I&T infrastructure (for example, its two data centres, CNOC and the off-site back-up storage facility), and gained an understanding of its principal applications (e.g. ISIS); and
- interviewed a wide range of Centrelink I&T management and staff, reviewed appropriate documentation (both hardcopy and Intranet), and performed appropriate testing.

5.8 The ANAO's approach to reviewing BCM of Centrelink's I&T infrastructure and applications, therefore, represented an amalgam of the guidelines and processes recommended by CobiT, the ANAO in its BPG, and,

---

[39] ANAO, op. cit.

[40] CobiT is an open standard for control over information technology, developed and promoted by the IT Governance Institute and endorsed by the Information Systems Audit and Control Association (ISACA). According to the IT Governance Institute, *(CobiT Management Guidelines, Executive Summary, Third Edition, July 2000),* 'CobiT assists management in determining and monitoring the appropriate level of IT security and control for an organisation. In addition, CobiT provides management with tools to assess and measure an organisation's IT environment. The framework identifies specific IT processes, a high-level approach to control over these processes, detailed control objectives, audit guidelines and management guidelines, the latter of which includes maturity models of best practice. CobiT also presents an IT governance management guideline and maturity model and explains how IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives'.

[41] Developed by the International Organisation for Standardisation.

to a lesser extent, other literature such as the IT Infrastructure Library (ITIL), which complements IT Service Management (ITSM).[42]

5.9 However, the ANAO's approach concentrated on applying the control objectives outlined in CobiT Section DS4 *'Ensure Continuous Service'*, which addresses BC (see Appendix 4 for details). The IT process of ensuring continuous service has the business goal of ensuring 'IT services are available as required and ensuring a minimum business impact in the event of major disruption.'[43] Control over the IT process is enabled by 'having an operational and tested IT continuity plan, which is in line with the overall business continuity plan and its related business requirements.'[44]

5.10 In some instances, the ANAO found an overlap with non-I&T aspects of its analysis of BC in Centrelink and, to reduce repetition, did not repeat these findings in detail in this chapter.

Analysis of I&T infrastructure and applications

I&T continuity framework

5.11 The ANAO recognises that Centrelink has recently embraced ITSM and its supporting ITIL framework. IT Service Continuity Management is a process within the ITIL framework, with the objectives stated in Figure 5.3 below.

---

[42] ITSM is primarily known as the process—and service-focused approach to IT Management. ITSM aims to provide effective and efficient process-driven IT management, to ensure quality IT services are provided to end-users. ITSM is a means to enable an IT group to provide reliable information systems to meet the requirements of business processes, thus enabling the organisation to meet its business objectives. As a framework for the management of IT infrastructure, ITIL primarily describes what must be included in ITSM to provide IT services of the required quality. ITIL provides good practice processes on how to manage IT service delivery. Whereas CobiT serves as a control and measurement mechanism, ITIL offers standards for operational and tactical management of service delivery. ITIL describes how these processes can be optimised and how the coordination between them can be improved. Available best practice comprises integrated guidance from the Office of Government Commerce (OGC) and the British Standards Institution (BSI). This information was drawn from: *The IT Service Management Forum (itSMF), IT Service Management: An Introduction, First Edition, May 2002; The Art of Service Pty. Ltd., Foundation Certificate in IT Service Management with ITIL, 2003;and itSMF, IT Service Management (A Pocket Guide), Version 2.1.a, 2001.* As mentioned in paragraph 5.11, Centrelink has recently commenced implementation of an ITSM framework.

[43] IT Governance Institute, *CobiT Management Guidelines*, DS4: *Ensure Continuous Service*, Third Edition, July 2000, p. 68.

[44] ibid.

Figure 5.3

Objectives for IT Service Continuity Management within the ITIL Framework

To support the overall BCM process by ensuring that the required IT technical and services facilities can be recovered within required and agreed business time scales.

IT Service Continuity Management is concerned with managing an organisation's ability to continue to provide a predetermined and agreed level of IT services to support the minimum business requirements, following an interruption to the business. This includes:

- ensuring business survival by reducing the impact of a disaster or major failure;
- reducing the vulnerability and risk to the business by effective risk analysis and risk management;
- preventing the loss of customer and user confidence; and
- producing IT recovery plans that are integrated with and fully support the organisation's overall BCP.

Source: IT Service Management Forum (itSMF), 2001.

5.12 The ANAO acknowledges Centrelink's intent to implement ITIL over time but emphasises that it will be some time before the IT service continuity management component will be implemented. Fully implementing this component should substantially assist in improving Centrelink's framework for IT service continuity management.

5.13 At the time of audit fieldwork, the ANAO found that although there were a number of shortcomings, the I&T framework adopted by Centrelink was generally consistent with the establishment of a BCM process, as outlined in CobiT and ISO/IEC 17799.

5.14 The main strengths of Centrelink's I&T continuity framework[45] were that it:

- required I&T managers to be accountable to their business process owners for continuity;
- was well integrated into Centrelink's broader BC approach;
- involved the main layers of BC—crisis response, crisis management, interim processing and recovery/restoration;

[45] Refer to Appendix 4, CobiT Control Objective DS4.1, *IT Continuity Framework*.

- defined the roles and responsibilities of those involved in I&T BC; and
- required documented continuity plans and approval procedures.

5.15 However, the existing framework does not appear to have been linked to an overall risk identification[46] and assessment of events that could cause interruptions to key business processes (notwithstanding reference to AS/NZS 4360[47] in various BC templates). This lack of linkage supports the finding in Chapter 3 (see paragraph 3.21), which identified the need to improve the consistency of risk management approaches between BCM and broader risk management at Centrelink.

5.16 The existing framework also does not:

- fully and comprehensively identify and prioritise critical I&T resources for continuity treatments and recovery;
- include an overarching document that describes the I&T continuity approach; or
- provide a clear and up-to-date link between continuity and existing system capability and specification.

5.17 These issues are discussed below.

Identify and prioritise critical I&T processes

5.18 As discussed in Chapter 1 (see paragraph 1.5), better practice BC requires that all critical business processes be identified and subject to continuity treatments. Similarly, CobiT[48] gives consideration to critical IT resources, so that critical resource elements are available and correctly prioritised to enable business functions to continue operating efficiently and effectively. Critical resources include critical applications, programs, third party services, operating systems, personnel and supplies, data files and time frames required for recovery.

5.19 In the course of its audit work, the ANAO identified two documents which addressed the criticality of Centrelink's I&T:

- *Centrelink's Critical Business Processes*[49]—which provides a table of processes and support, the latter reflecting undefined applications; and
- *Business Criticality Review* (Draft, March 2002)—tables in the document delineate IT products, including applications for mainframe production, network and standard desktop configuration products.

---

[46] ibid.

[47] AS/NZS 4360 is discussed at paragraphs 3.4 to 3.6.

[48] Refer to Appendix 4, CobiT Control Objective DS4.10, *Critical IT Resources*.

[49] Not dated nor author identified.

5.20 The ANAO found that, as reflected in these documents, the relationships between I&T applications/products, their priorities, business functions and responsibility centres have not been well defined in Centrelink. Moreover, it is not clear whether all critical I&T applications and infrastructure have been identified and subject to appropriate continuity strategies, plans and other treatments. As a result, in the event of a disaster, Centrelink is presented with the risk that its business-critical IT resources would not be available or coordinated in a defined, effective or timely manner. In addition, IT personnel might recover items based on their personal understanding of what is most important, rather than items pre-designated as critical to business process recovery.

5.21 As discussed in Chapter 4 (see paragraph 4.15), Centrelink plans to update its Criticality Review as part of the BC and EM Framework Project. Furthermore, Centrelink has advised that relationships between business processes and I&T services, applications and IT infrastructure components will be clarified as part of the implementation of ITIL.

5.22 The ANAO supports these developments but emphasises that these, or alternative projects, need to ensure that critical data and operations are identified, documented, prioritised and approved by the business process owners, in cooperation with I&T management.

Overarching I&T continuity document

5.23 To assist resource allocation at the crisis recovery and crisis management phases, priorities for continuity treatments for critical resources should be clearly outlined in an overarching document that explains I&T approaches to BC.

5.24 Centrelink does not have such an integrated document for either I&T or for the entire organisation generally.[50] The ANAO considers that Centrelink should produce an overarching I&T continuity document, that contributes to an organisation-wide continuity document, as outlined in Recommendation No.2 in Chapter 2 (paragraph 2.26).

5.25 Such a document could also describe how Centrelink would minimise continuity requirements for I&T resources, as illustrated by CobiT Control Objective DS4.4.[51]

Link between existing system specification and continuity

5.26 Effective I&T BC (including interim processing and recovery) requires a thorough understanding of current I&T specifications. To achieve this

---

[50] Refer to Appendix 4, CobiT Control Objective DS4.2, *IT Continuity Plan Strategy and Philosophy*.

[51] Refer to Appendix 4, CobiT Control Objective DS4.4, *Minimising IT Continuity Requirements*.

understanding, the development of, or changes to, applications must incorporate on-going revision of system and user documentation to ensure that it accurately reflects a current and complete representation of existing applications.

5.27 The ANAO observed that Centrelink documentation supporting principal applications was largely incomplete, inconsistently defined, improperly dated and relatively inaccessible. Centrelink's Intranet provides only limited descriptions of the applications. Proper documentation of applications does not exist with respect to continuity of operations. Furthermore, there is often little explanation of the relationship between applications and business functions.

5.28 Without such documentation, a risk exists that incorrect understanding of I&T applications will compromise continuity and capacity to recover quickly from interruptions.

Recommendation No.6

5.29 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.

Centrelink response

5.30 **Agreed. Action commenced.** Centrelink is in the process of documenting the services that are provided by IT as part of the IT Service Management project. The IT Refresh project (7.2 Service Management Processes and Tools) will assist in mapping the relationship between IT Services and Business Services. Continuity arrangements will become more formalised through an improved change control process, as part of Centrelink's IT Service Management implementation. Centrelink is in the process of updating major system documentation, initially for the Families Assistance Office system. Much of this documentation applies to common functions shared by core systems.

I&T continuity plans

5.31 Centrelink maintains different types of I&T-related BCPs, as listed in Figure 5.4.

Figure 5.4

Centrelink's main types of I&T BCPs and related plans

- I&T project continuity plans (including I&T applications).
- Disaster recovery plans by platform (reflecting hardware and systems software).
- Crisis plans (checklists for I&T infrastructure and I&T applications infrastructure).
- Site continuity plans (incorporating I&T considerations).

Source: Information provided by Centrelink, 2003.

5.32 To examine the adequacy and effectiveness of these plans, the ANAO examined;

- their content and format; and
- coverage of continuity plans for critical I&T applications and infrastructure.

Adequacy of content of Centrelink's I&T BCPs and related plans

5.33 Centrelink has site BCPs (and emergency management plans) for its many ASOs, CSCs and some Call Centres. These generally involve NSO 'flying-in' I&T solutions to extended outages. Chapter 4 explains that while these plans are generally sound, the core templates need to be streamlined and quality control undertaken on their implementation (see paragraphs 4.28 to 4.43).

5.34 The ANAO reviewed the BCPs for a number of Centrelink projects using CobiT criteria, which is a recognised basis for sound practice. The ANAO found that these BCPs did not necessarily address all aspects of CobiT criteria for content and format[52]

5.35 Consistent with the previous discussion of critical processes and resources, the ANAO suggests that Centrelink review its I&T continuity plans to ensure they contain critical information and procedures for response and recovery, safeguarding and reconstructing sites, coordination with public authorities, and communication with key resources. In accordance with accepted standards, Centrelink should consider including wrap-up procedures for assessing the adequacy and currency of the plans.[53]

---

[52] Refer to Appendix 4, CobiT Control Objective DS4.3, *IT Continuity Plan Contents*.

[53] Refer to Appendix 4, CobiT Control Objective DS4.13, *Wrap-Up Procedures*.

5.36 Centrelink has advised that, consistent with the ITIL framework, it intends to review continuity plans in 2003–04, including testing to ensure the adequacy of the plans (see 5.43 below).

Coverage of continuity plans for critical I&T applications and infrastructure

5.37 Better practice emphasises that all critical I&T infrastructure and applications be clearly identified and defined, and continuity plans be instituted to support them.[54] This can be done either separately, or jointly for a number of applications/platforms, depending on the degree of inter-connection.

5.38 Centrelink's *Business Criticality Review* emphasises that 'the current mainframe systems that support the programs have evolved into a highly integrated critical mass'.[55] Centrelink does not clearly distinguish or document its applications or maintain separate continuity plans for ISIS, let alone other major applications.

5.39 The ANAO considers that Centrelink needs to extend the criticality analysis to all important applications and then implement appropriate continuity and recovery plans. These would be prepared for discrete units, but may be addressed at the platform level (for example, mainframe, mid-range, internet, network) or at the application level.

5.40 The ANAO examined the treatment of BC for many of Centrelink's I&T projects. The results are discussed in Chapter 4 (see paragraphs 4.17 to 4.24) and Appendix 3. They highlight some shortcomings in the monitoring of BC elements of these plans by the relevant central units in Centrelink.

5.41 The ANAO found that plans for the mainframe environment are narrowly defined. This especially relates to the *'Centrelink Business Disruption Data Centre Technical Recovery Manual* ('The Plan'). The ANAO notes that 'The Plan' is not a BCP but describes itself as '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.'

5.42 Based on fieldwork observations and documentary review, the ANAO also considers that Centrelink has not adequately addressed BC for its mid-range equipment[56] and network environments. In recent years, the platforms for operations have changed, with emphasis directed towards growing mid-range and network environments.

---

[54] Refer to ANAO, op. cit., p. 42: 'Distributed handling and processing of information inherently spreads the business continuity risk across an organisation. However, as part of a comprehensive BCP, plans should be developed for each of these systems and recognise any interdependencies between them.'

[55] Centrelink's *Business Criticality Review*, p. 44, 2002.

[56] Detail on Centrelink's mid-range equipment is provided at paragraph 5.4. Mid range equipment supports management and busines administration rather than processing customer records.

Recommendation No.7

5.43 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.

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

Centrelink response

5.45 **Agreed. Action commenced**. Centrelink has contracted IBM to review and subsequently test mainframe disaster recovery procedures at the Data Centres. Centrelink teams will work to develop business continuity plans and disaster recovery plans as described in the recommendation. A number of projects are currently underway for major applications to take advantage of the continuity benefits of the Single Logical Data Centre configuration

Maintaining and rehearsing I&T continuity plans

5.46 Better practice[57] requires a BC framework that encourages and supports comprehensive rehearsal and maintenance of BCPs. Similar standards also apply to IT continuity plans.[58]

5.47 Chapter 2 (see paragraphs 2.17 to 2.20) reports that Centrelink does not provide a comprehensive quality control and assurance function for the preparation, submission, maintenance and rehearsal of BCPs, and accordingly makes a recommendation on quality control (Recommendation No. 1 at paragraph 2.21). These shortcomings also apply to I&T continuity plans and strategies.

5.48 The ANAO further observed that I&T rehearsals:

- are often stage-managed, narrowly defined and technical in nature;
- are operationally based, rather than business-oriented; and

[57] As discussed in paragraph 1.4.

[58] Refer to Appendix 4, CobiT Control Objective DS4.5, *Maintaining the IT Continuity Plan* and CobiT Control Objective DS4.6, *Testing the IT Continuity Plan*.

- do not reflect principal aspects of the organisation's resources, major applications on various platforms, or the ability to restore respective, actual business functions.

5.49 The maintenance of I&T BCPs is not linked into Centrelink's system development and change control process.[59] Consistent with Recommendation No.6 (at paragraph 5.29), the ANAO considers that Centrelink's system development and change management procedures need to be enhanced and enforced to ensure that essential elements of BC apply throughout the life cycle of an application.

5.50 Centrelink has advised that the introduction of ITIL should assist the agency to achieve a consistent change management process.

Training

5.51 Chapter 4 (see paragraphs 4.59 to 4.67) recognises that Centrelink does not have a formal approach to training management and staff in BCM and recommends that Centrelink develop a structured approach to such training (Recommendation No.5 at paragraph 4.68). This recommendation also applies to training relevant management and staff about I&T continuity plans and strategies.[60]

Risk exposures for I&T applications and infrastructure

5.52 The lack of suitable continuity strategies (including planning, maintenance and rehearsal) has contributed to risk exposures in Centrelink's I&T applications, hardware and system software, especially in regard to its mid-range equipment and network environments.

5.53 For example, a recent Centrelink project draws attention to the exposures presented to I&T.[61] The project plan states:

> I&T has identified a number of system risks that expose Centrelink's I&T systems to failure and adversely impact on the business. These risks have accumulated primarily because investments were not made to scale up existing applications to the wider business use. To assess the potential business impact of these risks, a data collection exercise was conducted with all I&T teams…'

5.54 In April 2002, Centrelink prepared a study, *IT Platform Recovery Times*,[62] which defined its major, non-mainframe platforms and their respective risks/

---

[59] Referred to as *Centrelink Project Lifecycle*, Fourth Edition.

[60] Refer to Appendix 4, CobiT Control Objective DS4.7, *IT Continuity Plan Training*.

[61] Centrelink, *I&T Assets at Risk—Additional Projects, Project Proposal (Summary)*, Project Plan #989.

[62] Centrelink 2002, *I&T Platform Recovery Times*, 3 April (Memorandum from Manager, BCU to Chief Information Officer.

exposures and risk mitigation strategies (see Figure 5.5 below). For each of its platforms (including the data centre platform and the ISIS platform), Centrelink considered the business impact, target recovery times, actual recovery times, recovery points and verification methods.

Figure 5.5

Risk/Exposure for Centrelink Non-Mainframe Platforms

Platform	Risk/Exposure
COLFrame[63]	High
Mid-range (i.e. Enterprise 10000, 'E10K')	High
Network Servers (ASOs, CSCs)	Medium/High
Intranet	Medium/High
Internet	High

Source: *Centrelink 2002, I&T Platform Recovery Times: Current Risks to I&T Recovery: Executive Summary*, 3 April.

5.55 The study revealed that actual recovery times were often considerably longer that targeted recovery times. It concluded that the targeted recovery times, which were generally also the maximum acceptable outage times, were often not justified. For example, for COLFrame, the maximum acceptable outage for EDGE[64] and CCA[65] BCPs was specified as two hours, though actual recovery time was more than 16 hours.[66] Furthermore, the firestorm on 18 January 2003 in the Australian Capital Territory (ACT) heightened doubts about the viability of stated recovery times for various platforms.

5.56 The ANAO noted that this April 2002 document has not been updated to reflect subsequent major events involving I&T, especially the movement of the second data centre from Sydney to Canberra.

5.57 Overall, the ANAO considers that Centrelink should extend its risk-based analysis of hardware and system software to make it comprehensive and consolidated. Centrelink should also re-assess the recovery times of its various I&T platforms. Centrelink has advised that this reassessment will follow a forthcoming revision of its Business Criticality Review.[67]

---

63 Colframe is described at Figure 5.1.

64 EDGE is described in Figure 5.2.

65 CCA: Call Centre Automation.

66 Furthermore, Centrelink 2002 *Data Centre Relocation Backout and Recovery Plan*, 9 October, stated that 'recovery from a disaster at either data centre will result in the loss of up to one hour's ISIS data and time frame of up to 24 hours to restore it at the other site'. A recent Service Incident Review, dated 6–7 February 2003, indicated a software error in an analysis tool, which took 24 hours to diagnose, and resulted in significant disruptions to I&T services over a two-day period.

67 Centrelink has also initiated a project to address risks that expose I&T systems to failure and adversely impact on business.

Loss of both data centres and off-site backup storage

5.58 The 2003 ACT firestorm highlighted the possibility of total devastation of both data centres and its off-site backup storage facility in Canberra as real risks to be considered by Centrelink.[68] However, according to 'The Plan', Centrelink has only considered partial and total loss of the mainframe/Unix hardware at one data centre as well as partial and total loss of data communications at one data centre. Centrelink has not formally considered the consequences of total devastation of its two data centres and its off-site backup storage facility.[69]

5.59 With regard to control procedures over its off-site backup storage facility, Centrelink does not periodically assess the contents, environmental protection and security aspects. Independent reviews would provide Centrelink with additional assurance about the continuity capabilities of its off-site backup storage facility.

Recommendation No.8

5.60 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 backup storage facility;

(b) consider the limitations associated with the location of the off-site backup storage facility; and

(c) periodically, at least annually, assess the content, environmental protection and security aspects of off-site backup storage.

Centrelink response

5.61 Agreed. Risk assessment scheduled for completion in the 2003/04 financial year. Centrelink facilities withstood the January 2003 Canberra bushfires, without impact on delivery of customer services. However, Centrelink will reassess the risk of the location of its data centres and off-site backup storage facilities with respect to events of this nature. Depending on the outcome of the risk assessment, consideration will be given to developing contingencies for the loss of these facilities. Centrelink's intention is to engage outside expertise to undertake this work.

---

[68] Standards underlie the need for sufficient backup facilities. Refer to Appendix 4, CobiT Control Objective DS4.11, *Backup Site and Hardware* and DS4.12, *Off-Site Backup Storage*.

[69] 'The Plan' states that 'the loss of both data centres is not catered for by any current Centrelink IT contingency plans and any recovery action would depend on the support available from our current vendors and support contractors.' Centrelink has advised, however, that no formal contract(s) ha(s)ve been established with vendors to provide this support in the event of a disaster.

5.62 Centrelink teams will assess the content of off-site storage facilities through testing data centre disaster recovery procedures. Centrelink will assess environmental protection and security aspects of off-site backup storage as described in the recommendation.

Establishment of a single logical data centre

5.63 Movement of the Sydney Data Centre to Canberra has enabled the possibility of the establishment of a single logical data centre (SLDC), comprising inter-operations of both data centre facilities. Projected benefits of the SLDC are efficiency of operations and respective cost savings. The ANAO notes that BC is a secondary consideration of the SLDC and has been given recent prominence as a project outcome mainly due to this audit, and emerging BC risks for Centrelink.

5.64 The SLDC Project Management Plan[70] states that a 'business continuity plan will be developed as part of the design taking business continuity requirements into account.' However, the High Level Design document[71], presented a restricted, technical analysis (for example, backups) rather than a comprehensive view of BC.

5.65 The ANAO suggests that greater consideration be given to BC aspects of the proposed SLDC. Comprehensive tests should be performed regularly on each of the components of the hardware environment, and plans should be updated to reflect results of its testing.

Conclusion: I&T infrastructure and applications

5.66 Based on the results of audit analysis and respective tests performed, the ANAO considers that, taken as whole, the BCM framework underlying I&T infrastructure and applications at Centrelink has considerable scope for improvement, particularly in the areas of:

- identifying critical resources;
- maintaining documentation for applications;
- developing plans for applications, hardware and system software;
- instituting quality control and training programs for BC; and
- integrating project management and BCPs.

5.67 The ANAO views Centrelink's response to BC for I&T as not yet fully mature. However, implementation of the IT Service Continuity Management

[70] Dated 30 July 2002.

[71] Dated 20 February 2003.

component of the ITIL framework should assist the organisation to provide a comprehensive, consistent and coherent best practice approach to I&T BCM.

5.68 In addition, the ANAO considers that Centrelink would benefit from using CobiT's detailed control objectives, critical success factors, key goal indicators and key performance indicators to evaluate its own progress towards ensuring continuous service (refer to Appendix 4).

Telecommunications

Overview of data connectivity BC issues

5.69 Telecommunications (or 'data connectivity') is a critical dependency for Centrelink, particularly as it affects the agency's ability to transact business on-line and communicate between points of presence.[72] Every application used by Centrelink for internal business automation, or for customer payments and interactions, is carried at some point by the Centrelink data network.

5.70 Centrelink manages its own internal data network, but contracts out data transmission to data network carriers. This approach means that all equipment used for connectivity within Centrelink is managed internally, while all equipment required for data transmission outside Centrelink is managed by a data carrier.[73] The components of the data network managed by Centrelink are overseen by the IT Infrastructure Services group, and are incorporated within the I&T infrastructure BC arrangements outlined earlier in this chapter.

Analysis of BC aspects of the Centrelink data network

5.71 In high availability data networks, BC aspects are often assessed in the context of:

- resilience of the network to withstand daily peaks and seasonal loads;
- redundancy of the network to withstand outages and allow re-routing of transmission backbones; and
- flexibility and responsiveness of the network to support required data volume and response times.

5.72 The ANAO examined the Centrelink data network for each of the above aspects, and checked current BCPs and rehearsal levels.

---

[72] These points of presence can range from large Area Office complexes to CSCs to community agents across Australia.

[73] Telstra carries the bulk of Centrelink's data traffic, although Optus and ICON (Inter Government Communications Network) carry some data between Centrelink's two data centres in Canberra.

5.73 Connectivity within the Centrelink data network is based on a spoke and hub design, which transmits data from CSCs and Call Centres via ASOs to either of the NSO data centres. To ensure appropriate levels of redundancy and resilience, the data network uses a primary high-speed backbone with a standby back-up link[74], albeit at a degraded capacity, if the main backbone is not operating.

5.74 Performance and responsiveness of the data network is monitored by the CNOC, which liaises closely with the IT Support Centre and the data carrier to rectify identified faults and poor network performance. Bandwidth on the data network is purchased on a volume basis under wholesale contracts managed by IT Procurement (a unit within I&T Business Services).

5.75 The ANAO notes that Centrelink has commenced a project to conduct high level re-design of the data network[75] to provide greater network flexibility. This re-design was prompted by a greater demand for communications capacity, due to increases in non-mainframe data traffic, such as Web-based applications; as well as business needs driving more stringent demands on service levels. This project will also examine voice and video transmission over the network, which has to date been used solely for data transmission.[76]

5.76 Apart from general references to restoration of data links in separate BCPs[77], the ANAO did not find any specific overall plan or strategy to restore the complete Centrelink data network and coordinate necessary interaction between internal Centrelink resources and external data carriers.

Conclusion: Telecommunications

5.77 Based on the above analysis and observations, the ANAO concluded that Centrelink's data network provides the required resilience, redundancy and flexibility to ensure high availability, and hence BC. The ANAO considers, however, that there is scope for the critical dependency of the data network to be more clearly articulated and more closely aligned to the agency's overall BC planning approach. The ANAO further considers that, due to the converging nature of the technologies being considered for the refreshed data network design, more detailed business impact analysis and continuity treatment planning should be conducted in conjunction with Centrelink's relevant BC units.

---

[74] The primary transmission protocol is a frame relay backbone, with an ISDN dial-in back-up link.

[75] *Data Network Re-design Project CR2222, Project Plan, Version 3*, dated 19 March, 2003.

[76] The project aims to provide communications infrastructure for Centrelink's needs over the next 10 years by implementing 'data aggregation points' co-located with available high capacity communication bearers such as fibre optic cable. This design will refresh the 'spoked hub' approach of the existing data network to focus the hubs on available data transmission capacity rather than geographic locations of ASOs.

[77] Including p. 18 of 'The Plan', which documents manual interventions to restore data links between data centres and ASOs. These contingency procedures do not, however, specify notification, escalation and recovery procedures for the Centrelink data network as a total network.

Voice Communications

Overview of voice communications crisis response in Centrelink

5.78 Centrelink's voice network is delivered via a national outsourced services contract and allows deployment of the following telephony-related resources:

- internal abbreviated dialling system for every Centrelink handset (Spectrum);
- internal help desks (used by Centrelink staff for IT and human resource enquiries);
- customer Call Centres (including Interactive Voice Responses and virtual national queuing capability for Centrelink business lines); and
- outbound calls and mobile telephony.

5.79 A significant contract with Telstra delivers inbound call and telephony infrastructure required by the Centrelink Spectrum network (including Call Centres). Non-local outbound calls (except outbound calls from Call Centres) as well as business mobile phone calls are delivered via a contract with AAPT. Both of these major contracts are at various stages of re-tendering.

5.80 The National Contracts Management Unit monitors overall performance of the above contracted services, while technical and business managers from Centrelink Call and Telstra monitor operational delivery of inbound calls to the Call Centres.

5.81 In addition to monitoring and managing the telephony load within the national Call Centre network, Centrelink Call is responsible for the BC of Centrelink's 'by phone' service channel and provides a voice communications Business Resumption Team. Figure 5.6 specifies the terms of reference of this Business Resumption Team.

Table 5.6

Voice Communications Business Resumption Team: Terms of Reference

- Determine customer service impact.
- Determine communications strategy.
- Organise staff and roster.
- Communicate with customers.
- Broadcast status updates to customers.
- Activate the outbound call facility.
- Liaise with customers, Recovery Director, Communications and Marketing.
- Monitor customer comments.

Source: Centrelink Business Disruption Notification Guide.

Core continuity requirements: analysis of capability of voice communications in Centrelink

5.82 To audit the effectiveness of Centrelink's voice communications capability to respond to a crisis, the ANAO examined its framework, strategies, plans, capability and recent performance against the following:

- project initiation;
- identifying critical processes and undertaking Business Impact Analysis;
- designing and implementing treatments;
- rehearsal and plan maintenance; and
- training and awareness.

5.83 The ANAO generally found Centrelink to have satisfied these criteria, as reported in Figure 5.7.

Figure 5.7

Voice Communications: audit findings against core aspects of BC

Stage of BC	*ANAO rating* [A]	*Comment on capability*
Project initiation	Adequate	• Part of broader Centrelink Y2K preparations in 1999.
Identifying critical processes and undertaking Business Impact Analysis	Adequate	• Centrelink Call has identified critical systems required to maintain service to customers and developed a detailed BCP that articulates the business impact of system outages and actions needed in order to restore services.
Designing and implementing treatments	Adequate	• Voice Communication Crisis Plan appropriate and well cross-referenced. • Treatments are detailed and achievable, covering technical and wide area outages. • Rectification of technical outages well documented within escalation procedures.
Rehearsal and plan maintenance	Adequate	• Sufficient rehearsal through day-to-day activities and NSO involvement in major simulations. • BCP was up-to-date for audit.
Training and awareness	Adequate	• Highly trained staff, especially NSO and generally, as required, in the network. • Appropriate staff aware of Voice Communications role in a crisis.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) Rating: Adequate, Requires Improvement, Inadequate.

Specific continuity requirements: Centrelink's performance in providing voice communication responses to crises

5.84 In addition to satisfying the core BC requirements outlined in Figure 5.7 above, an effective voice communications continuity response typically requires:

- human resource procedures to support the business function;
- vendor and carrier negotiations for service level agreements;
- alternative path designs and switching services redundancy;
- back-up software and equipment; and
- Uninterruptible Power Supply and monitoring to help reduce system loss.

5.85 During fieldwork, the ANAO found that the above specific continuity requirements were included in detailed technical and business procedures, which had been developed, implemented and tested by Centrelink Call. In particular, due to the geographically dispersed nature of the Centrelink Call Centres and mixed business lines within each Call Centre, redundancy of capacity can be

achieved by centrally re-allocating calls within the virtual national queue system.[78]

5.86 The ANAO also found that use of a managed voice service to underpin the voice communications technical capability has transferred much of the technology-related risk to its contractor—Telstra—and that treatments to control and mitigate these risks had been documented in detailed risk plans for various components of the outsource contract.

5.87 The ANAO also observed that many of the actions required to rectify an outage were reliant on other plans, such as 'The Plan' discussed in this chapter (see paragraph 5.41), or an external supplier, such as Telstra. This reliance or dependency therefore requires ongoing examination by Centrelink Call to ensure that recovery expectations are actually capable of being achieved during a major or wide area outage.

5.88 Notwithstanding the above, operational resilience and flexibility has allowed Centrelink Call to provide 'hot-lines' for customers to use during special community or emergency incidents such as the 2001 NSW bushfires, the 2001 Ansett collapse, or the 2002 Bali terrorist bombings.[79] This capability is based on the close technical and business links with Telstra forged during day-to day operations.

Conclusion: voice communications

5.89 Overall, the ANAO concluded that Centrelink Call is a responsive service channel for Centrelink and its customers, which has taken effective steps to ensure business continuity and resumption. The ANAO found that the Voice Communications Crisis Plan was sound and integrated well with the Centrelink Call BCP and Notification Guide.

---

[78] This call routing flexibility does have an impact on client service, however, as the total number of available call centre agents is reduced, triggering a 'call block', which is used to abate lengthy wait times by blocking customer access to the call queue via a 'busy' signal.

[79] Centrelink's role in the response to the Bali bombings included setting up an international toll-free number for Australians in Indonesia to contact Centrelink for crisis assistance and counselling.

6. Implementing BCM in Centrelink: Critical Non-technology Business Processes

This chapter examines BCM of the main non-technology business enablers in Centrelink, as well as the coverage of BCM and EM throughout the network.

Background

6.1 Chapter 4 reviewed common approaches to BCM and EM throughout Centrelink's network and across its business enablers. This chapter examines BCM approaches, practices and performance in Centrelink's non-technology business enablers, or Business Resumption Teams, namely:

- Communication;
- People Management;
- Finance;
- Corporate Records;
- Buildings; and
- Network.

6.2 The ANAO has considered the BCM of these business enablers on a similar basis to that outlined in Chapter 4. That is, by examining:

- project initiation;
- identifying critical processes and undertaking Business Impact Analysis;
- designing and implementing treatments;
- rehearsal and plan maintenance; and
- training and awareness.

6.3 However, the chapter does not dwell on the general messages reported in earlier chapters. Rather, the focus in this chapter is on the key findings applicable to each of the business enablers.

Communication

Overview of Communication crisis response in Centrelink

6.4 Communication is one of Centrelink's Business Resumption Teams. As with all Centrelink's Business Resumption Teams, the leader of the Communication Business Resumption Team is the National Manager of the corresponding function in Centrelink, in this instance, the Communication and Marketing Branch.

6.5 The Communication Team's continuity roles and responsibilities primarily include channelling and coordinating all formal communications with external and internal stakeholders about developments and implications of crises and similar events affecting Centrelink. The Communication Team also interacts with the People Management Team to keep Centrelink staff informed of developments in crisis response policies and procedures including by providing updated content for the Intranet.

6.6 Similar to other Centrelink Business Resumption Teams, the skills, knowledge and contacts required for BC actions related to communication and marketing are similar to, and draw heavily from, those applied in day-to-day operations. These day-to-day operations include: responding quickly to emerging issues potentially affecting Centrelink (targets are 15 minutes response to standard issues and 60 minutes to complex issues); dealing with the media, the chief executive and senior management; and co-ordinating communication and marketing across the network.

Core continuity requirements: analysis of capability of Communication in Centrelink

6.7 To audit the effectiveness of Centrelink's communications capability to respond to a crisis, the ANAO examined its framework, strategies, plans, capability and recent performance against the parameters outlined in paragraph 6.2.

6.8 The ANAO generally found Centrelink to have satisfied the criteria associated with each of these stages of BCM, as reported in Figure 6.1 below.

Figure 6.1

Communication: Audit findings against core aspects of BC

Stage of BC	*ANAO rating* [A]	*Comment on capability*
Project initiation	Adequate	• Part of broader Centrelink Y2K preparations in 1999.
Identifying critical processes and undertaking Business Impact Analysis	Adequate	• Communication is a supporting process rather than a critical process requiring its own BCM.
Designing and implementing treatments	Requires Improvement	• Communication Crisis Plan appropriate and well cross-referenced within NSO but could refer to integration throughout the network.
Rehearsal and plan maintenance	Adequate	• Sufficient rehearsal through day-to-day activities and NSO involvement in major simulations. • BCP was up-to-date but would benefit from recommended improved Centrelink control framework (see Recommendation No.1 at paragraph 2.21).
Training and awareness	Adequate	• Highly trained staff, especially in the NSO and generally as required in network. • Appropriate staff aware of Communication role in crisis.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) Rating: Adequate, Requires Improvement, Inadequate.

6.9 Many of the aspects of BC that have been identified as warranting considerable attention and improvement throughout Centrelink were much less of an issue for Communication. These include rehearsal, training, and enhancing staff awareness. The nature of the communication service, and the fact that Centrelink has highly trained and experienced staff undertaking these duties on an ongoing basis, reduced the need for Centrelink to pay significant attention to specific BC or EM roles.

6.10 While the Crisis Plans for Communication and for the Media Spokesperson appeared sound, there was scope for relevant formal plans to more clearly specify the nature of co-ordination required between the NSO and the Centrelink network (ASOs, CSCs and Call Centres). This limitation is similar to that in other Centrelink BCPs. Having said that, the interaction between the Communication Team in the NSO and their counterparts in the network appeared to be effective, for example, as evidenced in their response to the Warrnambool CSC fire (see Appendix 2). Furthermore, the NSO's Communication, Media and Marketing team has close and extensive links with all of the State Communication Units that serve the Centrelink network.

Specific continuity requirements: Centrelink's performance in providing communication responses to crises

6.11 In addition to satisfying the core BC requirements outlined above, an effective communications and marketing continuity response typically requires:[80]

- a single media spokesperson;
- well trained media representatives;
- a network of media contacts to utilise in a crisis;
- 'friends'[81] to call on for help if there is an event;
- a positive image in the community and media that may help defend reputation in times of crisis; and
- an understanding of likely media responses to a crisis.

6.12 The ANAO found that Centrelink had these elements in place, which support effective communication with stakeholders during, and subsequent to, a crisis.

6.13 Centrelink does nominate single spokespeople to liase with the media and has guidelines that discourage any other staff from making public comments at any time, unless they have been specifically authorised to do so. Discussions as part of audit fieldwork indicated that Centrelink staff abide by these directions.

6.14 Centrelink prefers to use local people to deal with the local media if possible, as local staff are often more effective in providing messages to local communities about crises or disasters. This was the case for the Warrnambool CSC fire, when the NSO supported the local offices in strategy and the nature and style of presentation, but a local officer was the sole media spokesperson.

6.15 Centrelink runs a continuous marketing campaign to provide good news stories about Centrelink to a network of journalists, in order to build a positive image in the community and media. This ongoing groundwork can assist in times of crisis.

6.16 A mechanism Centrelink uses to achieve fast communication response times is that the National Manager of Communication and Marketing has the authority to issue press releases without the need for clearance from the CEO or operational director. Centrelink's view is that this mechanism expedites the handling of issues and often enables problems to be contained rather than get out of hand.

---

[80] Sourced from a presentation by Jane Jordon of the Jordon Templeman Group, at the *Business Continuity Management Summit*, 23 September 2002, IBC Conferences.

[81] High profile and respected individuals or senior representatives of organisations.

People Management

Overview of People Management crisis response in Centrelink

6.17 People Management is a Business Resumption Team that mainly aims to support other teams in responding to crises affecting Centrelink. The leader of the People Management Business Resumption Team is the National Manager of People Management.

6.18 The People Management Team's main roles are to provide expert human resource (HR) policy guidance and advice to ASOs and Business Resumption Teams during crises, and to keep employees informed of developments. Policy guidance may cover matters such as leave provisions and Occupational Health and Safety issues affecting interim processing arrangements. The People Management Team negotiates with Comcare regarding any relevant workplace safety, rehabilitation and compensation issues, and also liases with unions.

6.19 BC roles and responsibilities of the People Management Team are outlined in the Business Disruption Notification Guide. The ANAO considers that Centrelink should review the Terms of Reference for the People Management Team, to clarify the role of the Human Resource Area Units (for example in safeguarding personnel), and also to acknowledge the People Management Team's liaison role with other Centrelink managers (for example, those who may actually visit injured employees) and with other emergency services involved in crisis response.

6.20 Similar to the Communication Team, the day-to-day operations of members of the People Management Team prepares them well to deal with many crises. In particular, the NSO People Management Team regularly liaises across the network, and within the NSO, in disseminating information about HR guidelines.

Core continuity requirements: analysis of capability of people management in Centrelink

6.21 To audit the effectiveness of Centrelink's people management capability to respond in a crisis, the ANAO examined Centrelink's organisation-wide framework, strategies, plans, capability and recent performance against the core parameters outlined in paragraph 6.2.

6.22 The ANAO found that Centrelink generally met the criteria associated with each of these stages of BCM, as reported in Figure 6.2. However, Centrelink's overall people management capability suffered from some of the more common limitations affecting BC and EM more broadly in Centrelink, especially regarding rehearsal and plan quality.

6.23 While the Crisis Plan for the People Management Team was basically sound, the version provided to the ANAO had minor errors such as incorrect page numbers on the Table of Contents, and other presentation problems. Additionally, it did not: adequately cross reference other necessary resources; discuss liaison protocols with the wider Centrelink network; explain how to delegate certain tasks; or include guidance on liaison with external emergency services.

Figure 6.2

People Management: Audit findings against core aspects of continuity

Stage of BC	*ANAO rating* [A]	*Comment on capability*
Project initiation	Adequate	• Part of broader Centrelink Y2K preparations in 1999.
Identifying critical processes and undertaking Business Impact Analysis	Adequate	• People Management is a supporting process rather than a critical process requiring its own BCM.
Designing and implementing treatments	Requires Improvement	• People Management Crisis Plan appropriate but had minor errors and did not integrate adequately throughout the network.
Rehearsal and plan maintenance	Requires Improvement	• Some rehearsal through day-to-day activities and NSO involvement in major simulations but would benefit from greater rehearsal in the network. • BCP was up-to-date but would benefit from recommended improved Centrelink control framework (see Recommendation No.1 at paragraph 2.21).
Training and awareness	Adequate	• Appropriate staff aware of People Management role in crisis. • Highly trained staff but little exposure to extreme crises, such as those involving a major number of staff injuries.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) Rating: Adequate, Requires Improvement, Inadequate.

Specific continuity requirements: analysis of Centrelink's performance in managing HR in a crisis

6.24 In addition to satisfying the core BC requirements outlined above, the audit focused on the following specific elements of the People Management Business Resumption Team's responsibilities:

- effectiveness of communication between the NSO People Management Team and Human Resource Area Units in response to a crisis;
- capacity to inform staff of crisis developments and responses;

- capacity to continue staff payments; and
- ability to arrange counselling for staff affected by crises.

6.25 The ANAO found that the NSO People Management Team and the Human Resource Area Units had good day-to-day communication networks and relationships, which, as evidenced by the response to the fire that destroyed the Warrnambool CSC, contributed to a strong capability to manage Centrelink staff in crisis situations (see Appendix 2).

6.26 Centrelink can use a number of on-line channels to inform staff about crisis developments. These include Infolink (the HR communication on-line channel), the intranet (Centrenet) and a program called Mapstat (which provides daily information about the status of Centrelink offices, including those affected by interruptions). The ANAO noted the recommendation from Exercise Gravity[82] that Centrelink should provide a 1300 number that staff could call to obtain information about a crisis, if the intranet and other on-line resources were not available. The ANAO understands that this resource has not yet been provided but is being developed as part of the BC and EM project.

6.27 The ANAO briefly examined Centrelink's capacity to ensure continuity of staff payments. Centrelink did not have a separate BCP for this service (Centrepay) as it was considered very unlikely that an event would occur that would prohibit salary payments from occurring for a period of time exceeding the 'maximum acceptable outage'. The ANAO acknowledges this judgement but suggests that Centrelink further consider the underlying assumptions. The ANAO notes that Centrelink has a number of alternative sites for processing staff payments and also has access to back-up tapes that can be used to determine payment levels in a crisis.

6.28 Centrelink has two main facilities to provide staff with access to counselling in response to trauma or other problems associated with a crisis. A panel of Employee Assistance Providers can be used, as well as Centrelink's own social workers and counsellors, which together provide a considerable resource.

Finance

Overview of Finance crisis response in Centrelink

6.29 The Finance Business Resumption Team is primarily responsible for providing timely and controlled access to funds to support business resumption operations. The Team is also responsible for ensuring that customer payments continue.

---

[82] This major crisis simulation exercise was conducted by Centrelink in November 2001.

6.30 The National Manager of Financial Services is responsible for the Finance Business Resumption Team. Financial Services is the business owner of all finance functions in Centrelink, including: Business Systems; Taxation and Financial Policy; Asset and Reporting; Treasury; and Accounts Payable and Receivable.

6.31 As the business owner, Financial Services is therefore responsible for all finance and payments functions in Centrelink. However, most of the operational finance processes are I&T based, and undertaken by Corporate Systems staff. These processes include Infolink (a SAP-based system providing corporate, finance and HR information in Centrelink), and a separate payments system. Both systems are delivered according to agreements negotiated with Financial Services.

Analysis of continuity of Finance in Centrelink

6.32 To audit the effectiveness of Centrelink's finance and payments capability to respond to a crisis, the ANAO examined its framework, strategies, plans, capability and recent performance against the core parameters outlined in paragraph 6.2.

6.33 The ANAO found the Finance Team had adequately structured its BCM approach through: project initiation; identification of critical business processes and acceptable outage times; and designing BCPs related to risk exposures (see Figure 6.3 below).

Figure 6.3

Finance: Audit findings against core aspects of BC

Stage of BC	*ANAO rating* [A]	*Comment on capability*
Project initiation	Adequate	• Part of broader Centrelink Y2K preparations in 1999.
Identifying critical processes and undertaking Business Impact Analysis	Adequate	• Aware of critical business processes, especially I&T (i.e. Infolink and Payments). • Business Impact Analysis undertaken and Maximum Acceptable Outage defined.
Designing and implementing treatments	Adequate	• Financial Services Team Plan adequate and risk analysis undertaken for Corporate Systems.
Rehearsal and plan maintenance	Requires Improvement	• Have not sufficiently rehearsed the loss of Finance systems, e.g. Infolink.
Training and awareness	Requires Improvement	• Highly trained staff but little exposure to extreme crisis scenarios such as those involving a large number of staff injuries. • Need to improve staff awareness of Finance role in crisis.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) Rating: Adequate, Requires Improvement, Inadequate.

6.34 However, the Finance Team acknowledges that it needs to improve training and awareness of staff about BCM, and to incorporate training more formally in BCM arrangements. Finance managers also recognised the need to improve rehearsal and plan maintenance.

6.35 For example, rehearsals could be conducted to test the effectiveness of temporary processing systems, such as a spreadsheet program to be used if Infolink became unavailable for extended periods. While this has never happened, and is considered by Centrelink to be very unlikely, the critical nature of this possibility warrants a formal rehearsal program.

6.36 This requirement for enhanced rehearsal, training and plan maintenance was the main finding from audit work in relation to the Finance Business Resumption Team. The adequacy of BC strategies of the Corporate Systems unit was considered as part of the audit work in relation to Centrelink's I&T, reported in Chapter 5.

Corporate Records

Overview of corporate records crisis response in Centrelink

6.37 The responsibility for management of Centrelink's corporate records lies within a national branch called Knowledge and Enabling Services (KAES). KAES is responsible for the following aspects of corporate records management:

- structured data (physical and/or electronic records covered by the *Archives Act 1983*);
- unstructured data (business analysis and compliance related data sets); and
- the Records Management Unit based at the NSO (which manages paper policy and administration files).

6.38 Although a national off-site records storage project to standardise management, storage and retrieval of records across Centrelink has commenced, at this stage, most Centrelink Areas are still responsible for the paper records produced and stored by their ASO and CSCs.

Analysis of continuity of corporate records management in Centrelink

6.39 To audit the effectiveness of the corporate records management function's capability to respond in a crisis, the ANAO examined its framework, strategies, plans and recent performance against the core parameters outlined in paragraph 6.2.

6.40 The corporate records function in Centrelink was also examined during other recent ANAO audit activity and fieldwork[83], which included review of the impact of a business disruption on the agency's record keeping system.

6.41 The ANAO found that at the time of fieldwork for the current audit, KAES had no documented crisis response role within Centrelink. The ANAO notes that KAES has been included as a Business Resumption Team in recent[84] versions of the BCM framework chart. However no documentation has been provided on the new Business Resumption Team's role and responsibilities.

6.42 The recent yet incomplete development of the corporate records Business Resumption Team role contributed to the limitations in corporate records continuity capability, as outlined in Figure 6.4.

Figure 6.4

Corporate Records: Audit findings against core aspects of BC

Stage of BC	*ANAO rating* [A]	*Comment on capability*
Project initiation	Inadequate	• No evidence of any coordinated BC activity or integration within the BCM framework.
Identifying critical processes and undertaking Business Impact Analysis	Requires Improvement	• BC focus is ad hoc and project, rather than function, based. • Business Impact Analysis conducted as part of BCP for off-site storage shed and national TRIM[85] database.
Designing and implementing treatments	Requires Improvement	• Treatments designed as part of the BCPs for TRIM database and off-site storage. • Australian Archives Better Practice Principles need to be adopted.
Rehearsal and plan maintenance	Requires Improvement	• Have not rehearsed for loss of the NSO Records Management Unit and holdings. • The BCPs for TRIM database and off-site storage sheds have not been rehearsed.
Training and awareness	Inadequate	• Key staff not trained or aware of Business Resumption Team role.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) Rating: Adequate, Requires Improvement, Inadequate.

Specific continuity requirements: Centrelink's performance in providing corporate records responses to crises

6.43 To assess specific BC requirements, the audit focused on the following specific elements of the corporate records business resumption responsibilities:

[83] Centrelink was examined by the ANAO Business Support Process Audit*: Recordkeeping in Large Commonwealth Organisations*, tabled on 24 September 2003.

[84] March 2003.

[85] TRIM = Tower Records Information Management system.

- safeguard vital documents which support critical business processes;
- restore hardcopy and electronic records data;
- minimise impact on public image due to inability to deliver information to stakeholders such as Ministers, the Courts, and the public; and
- ensure legislative requirements are complied with.

6.44 The ANAO found that restoration and back-up of electronic documentation had been incorporated into existing data management and back-up treatments implemented within Centrelink's I&T Infrastructure environment. The ANAO noted, however, that many vital BCM documents (such as BCPs and Site Response Plans) are stored on Centrenet or Local Area Networks with no guaranteed or documented capture by system back-up strategies.

6.45 For hardcopy records data, the ANAO found that at present a number of independent TRIM databases are used across Australia to capture data about paper records stored at the NSO or within the Areas. The roll-out of the Off Site File Storage Project aims to integrate these independent databases into a national TRIM database by inputting records data once paper records have been transferred from ASOs and CSCs into the storage sheds. A BCP has been developed for the Off Site File Storage Project and incorporates fail-over and back-up strategies for the national TRIM database.

6.46 During discussions with Centrelink staff in the course of the audit, the ANAO observed that many of the staff interviewed felt that paper records were less valuable than electronic data and on-line documents stored in customers' mainframe files. Many staff felt that source documents stored on paper files (such as proof of identity documentation and payment application forms) could be readily replaced by customers if the paper file was lost or destroyed.

6.47 Notwithstanding the fact that Centrelink's processes are highly automated, with many decisions documented electronically, customers and other stakeholders, including the Courts, expect that customer files should be complete and readily accessible in paper form if requested (such as under the Commonwealth's *Freedom of Information Act 1982* or subpoena).

6.48 The ANAO considers that the current hybrid system of paper and electronic customer and corporate records has not been assessed in terms of risk of possible damage to Centrelink's public image from adverse media reporting or political interest should complete records became unavailable due to a BC outage.

6.49 Other recent ANAO audit activity, referred to in paragraph 6.40, observed during fieldwork that although Centrelink has undertaken assessments of

business disruption and developed BCPs, little emphasis has been placed on the importance of identifying vital corporate records. Furthermore, the ANAO noted that no arrangements have been made for the recovery or security of paper records held by individual program areas, ASOs and CSCs. The ANAO also noted that current business resumption plans fail to take into account records stored on portable physical media such as disks or CDs.

6.50 During this audit, the ANAO found that, although Centrelink has attempted to improve its internal corporate record keeping practices, in the particular context of BC planning, the agency has not fully adopted better practice as advocated by the National Archives of Australia[86]. This better practice approach[87] provides detailed and practical guidance on disaster preparedness, as well as the identification, protection and salvage of vital corporate records.

Recommendation No.9

6.51 The ANAO recommends that:

(a) 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

(b) 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.

Centrelink response

6.52 **Agreed.** Centrelink recognises identification of vital records is an important issue and considers customer records as the heart of our business. Electronic customer data is regularly backed up and stored at an off-site secure facility. The record keeping system used to administer physical files has failover capability that will be further bolstered by the system configuration that the Single Logical Data Centre will provide. Centrelink has a number of records management units Australia wide. These units have in place security and records protection systems and procedures, with links to relevant Commonwealth archiving bodies in each State. As a matter of course, Centrelink employs its best endeavours to meet Commonwealth Standards where they exist.

---

[86] Incorporating Australian Standard AS4390-1996 Records Management, now also referred to as AS ISO 15489.

[87] The Australian Archives '*Disaster Preparedness Manual for Commonwealth Agencies'* is available on-line at <http://www.naa.gov.au recordkeeping/preservation/disaster/contents.html>.

6.53 Centrelink has recently completed an internal review of information services. This review has led to a realignment of responsibilities which will improve both the quality and management of data, and improve the analysis undertaken. Part of this realignment has been the creation of the Data Shop team, whose key responsibilities include business ownership of records management, being the supplier and manager of Centrelink's data holdings and implementing and mandating content management strategies.

6.54 As part of the IT Refresh project, Centrelink will implement a fully functional and integrated electronic document and records management system. The Data Shop team is currently progressing Centrelink's DIRKS (Design and Implementing Records Keeping System) program.

Buildings

Overview of Buildings crisis response in Centrelink

6.55 Centrelink's Buildings function incorporates the large NSO presence in Canberra and numerous (approx 1000) leased sites across Australia. The National Property and Services Team manages the major NSO complex in Canberra, while the remainder of the sites are managed through a property services contract with Jones Lang LaSalle (JLL).

6.56 The Centrelink network also has Property and Services managers located in each Area, who play an important coordination and reporting role between CSCs, ASOs and the National Property and Services Team.

6.57 Although the National Property and Services Team manage the national contract with JLL, they are not directly involved in Area operational response and rectifications, unless an Area or a national business unit such as Centrelink Call[88] formally escalates the fault or outage to them.

6.58 The Buildings Business Resumption Team's main function is to coordinate external resources required to safeguard Centrelink personnel and provide working access to office premises. Importantly, the Buildings Team is not responsible for undertaking necessary actions, but rather to coordinate outsourced resources to ensure that these actions occur.

6.59 The skills, knowledge and contacts required to perform BC actions related to property management are similar to, and draw heavily from, those required for day-to-day operations. Day-to-day operations may include: site managers responding to, and reporting, building faults (e.g. power outages, storm damage, broken doors and windows, soilage in customer service areas); and Area

[88] Centrelink Call refers to the national management of Centrelink's network of Call Centres.

Managers dealing with more serious building problems, such as air conditioning failure or pervasive workplace odours.

Core continuity requirements: analysis of capability of Buildings in Centrelink

6.60 To audit the effectiveness of Centrelink's Buildings capability to respond to a crisis, the ANAO examined its framework, strategies, plans, capability and recent performance against the parameters outlined in paragraph 6.2.

6.61 The ANAO generally found Centrelink to have met these criteria, as reported in Figure 6.5 below.

Figure 6.5

Buildings: Audit findings against core aspects of BC

Stage of BC	*ANAO rating* [A]	*Comment on capability*
Project initiation	Adequate	• Part of broader Centrelink Y2K preparations in 1999.
Identifying critical processes and undertaking Business Impact Analysis	Adequate	• Buildings is a supporting process rather than a critical process requiring its own BCM. • The escalation workflow is embedded into the external provider's contract and promulgated across Centrelink's network.
Designing and implementing treatments	Adequate	• The Buildings Crisis Plan is appropriate and well cross-referenced within the NSO but could refer to integration throughout the network.
Rehearsal and plan maintenance	Requires Improvement	• Sufficient rehearsal via day-to-day operational activities and NSO involvement in major simulations. • BCP was up-to-date but would benefit from recommended improved Centrelink control framework (see Recommendation No.1 at paragraph 2.21).
Training and awareness	Adequate	• Highly trained staff, especially in the NSO and generally as required in network. • Appropriate staff aware of National Buildings Team role in a crisis.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) Rating: Adequate, Requires Improvement, Inadequate.

6.62 Many of the aspects of BC identified as warranting considerable attention and improvement throughout Centrelink, are relevant for Buildings. These aspects include rehearsal and keeping plans up to date.

6.63 The nature of the Buildings operating environment, and the fact that experienced Centrelink staff undertake these duties on an ongoing basis, reduces the need for Centrelink to pay significant attention to specific BC or EM roles.

6.64 Interaction between the National Buildings Team members and their counterparts in the wider Centrelink network appeared to be effective, as evidenced in their response to the Warrnambool CSC fire (see Appendix 2). The national accountability and service requirements framework of the JLL contract also appeared to work effectively, although no detailed testing was conducted of JLL's performance or ability to meet BC related Key Performance Indicators.[89]

Specific continuity requirements: Centrelink's performance in providing Buildings responses to crises

6.65 In addition to satisfying the core BC requirements outlined above, an effective Buildings BC response typically requires:

- damage assessment, salvage, and restoration of buildings and equipment;
- timely restoration or relocation of the premises housing essential business processes; and
- documented procedures to support building restoration.[90]

6.66 The ANAO found that Centrelink's Buildings Team Crisis Plan effectively addressed all of the above continuity crisis response requirements. However, the crisis response would heavily rely on support from JLL or other specialists within Centrelink, such as those dealing with IT equipment salvage, or insurance and occupational health and safety issues.

6.67 In regard to relocation of business processes due to temporary or extended access disruption at Centrelink sites, the ANAO suggests that it would be prudent for the National Buildings Team and Area Buildings Managers to maintain up to date knowledge of suitable, vacant temporary accommodation, especially in markets where this type of accommodation is scarce. The possibility of establishing arrangements in advance with suppliers to enable rapid re-furnishing, re-cabling and re-equipping of damaged facilities and equipment should also be explored.

6.68 The ANAO found that the building fault escalation flowchart for JLL enabled appropriate trade and repair responses to building and equipment related BC outages.[91] The flowchart also specifies the roles and responsibilities of various stakeholders in such an event, as illustrated by Figure 6.6.

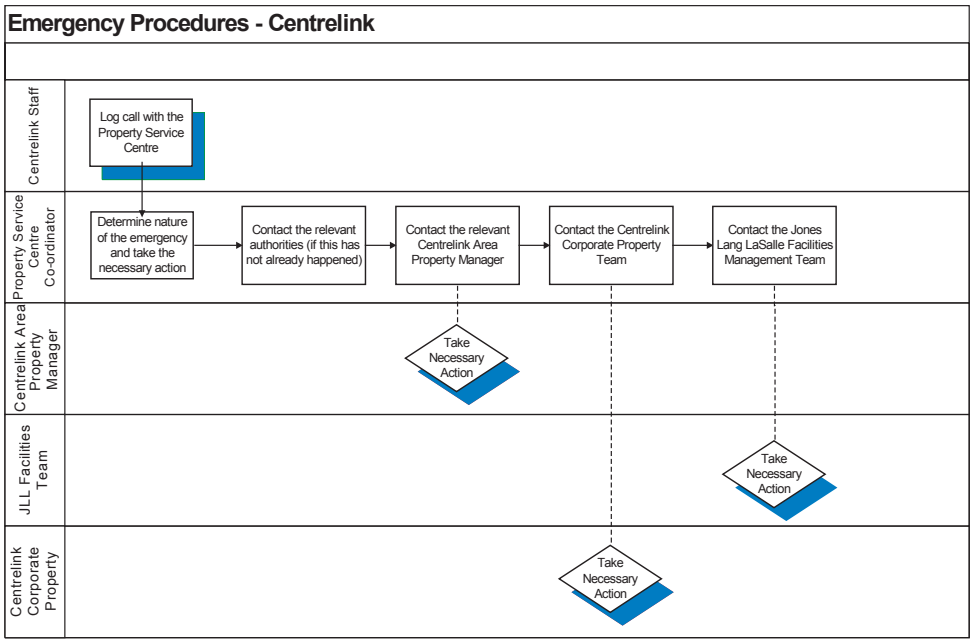
---

[89] Centrelink's contract with JLL expects availability of a 24-hour fault reporting centre and Buildings Management Information System. Lack of availability of these services results in JLL being unable to receive access to a bonus contract pool worth $200 000. Detailed service obligations, workflows, delegations and key performance indicators have been specified in the contract.

[90] op. cit. ANAO 2000, p. 41.

[91] Centrelink uses a Critical, High, Medium, Low scale for building and facilities fault reporting. Detailed definitions of the type of fault that would fit into these categories, agreed response parameters, and performance targets have been negotiated with JLL. An 'approved faults' listing has been promulgated on Centrenet for use across Centrelink.

Figure 6.6
Centrelink Buildings escalation flowchart



Source: Flowchart provided by Centrelink, 2003.

6.69 Notwithstanding that Centrelink's has an adequate buildings business recovery response and escalation process, the ANAO observed that the National Buildings Team did not receive consolidated information on past service outages or utility failures which had affected BC, and which had been reported to the BCU.

6.70 The ANAO observed that in order to profile and mitigate human and natural hazards, Centrelink does liaise with local site managers and maintains premises that conform with relevant building codes and regulations. However, the ANAO considers that this liaison and profiling could be more effective if it was managed by the National Buildings Team, and then linked to analysis of known causes of business outages previously reported within the Network.

Centrelink Network—ASOs, CSCs and Call Centres

BCM framework for Centrelink Network

6.71 As part of the Centrelink BC Framework, each Area Manager is responsible for an Area Command Group (ACG). The ACG typically consists of the Area Manager, Area Business Managers and experienced business and technical staff

from within the Area. The function of the ACG is to coordinate and plan the BC activities in its Area, and to direct any crisis response or business resumption effort. The ACG is also responsible for the dissemination of information throughout the Area, and liaison with the Crisis Command Centre in the NSO.[92]

6.72 As discussed in Chapter 4 (see paragraph 4.36), Centrelink is an organisation that implements recovery strategies that include dispatch of expert 'flying squads' from the NSO to assist local recovery efforts. These flying squads can offer particular expertise in recovery of I&T hardware and system software (including applications and voice and data connectivity); buildings; finance; and, depending on circumstances, crisis response governance. Otherwise, the NSO provides ASOs with support for other business processes including people management; communication with internal and external stakeholders; and records management. Thus, effective coordination between the various levels of Centrelink—the NSO, ASOs, CSCs, and Call Centres—is crucial to achieving successful management of crises.

Analysis of continuity capability of the Centrelink network

6.73 To audit the effectiveness of Centrelink's crisis response capability at Area level, the ANAO examined the Area level framework, strategies, plans, capability and recent performance against the core parameters outlined in paragraph 6.2.

6.74 During fieldwork for this audit, Centrelink's Warrnambool CSC burnt down. As discussed in Appendix 2, Centrelink was very successful in responding to this crisis, with particular strengths being:

- governance of the crisis, involving the 'virtual' Crisis Command Centre and an 'off-line' Area Manager;
- the effective relationship between the three main levels at Centrelink—the NSO, ASOs and CSCs—in co-ordinating the response; and
- the commitment, skills and knowledge of Centrelink staff to undertake contingency processing and restore normal processing.

6.75 Managers and staff at the Warrnambool CSC and the associated Victoria West ASO commented that other regions in Centrelink would probably be as successful as Warrnambool in responding to such an outage, for the reasons outlined in 6.74. This attests to a strong capacity of Centrelink to respond to crises in the network.

6.76 Contrary to this positive observation, the audit identified a number of limitations in BC processes in Centrelink's regional network, as outlined in

[92] <http://centrenet/homepage/nso/iandt/security/buscont/framework.htm>.

Figure 6.7, and discussed in Chapter 2 (see paragraphs 2.10 to 2.16) and Chapter 4 (see paragraphs 4.35 to 4.43).

6.77 Limitations include the need to:

- improve BCPs and EMPs—to streamline and tailor them to reflect local conditions, and to make a clear distinction between BC and EM;
- improve consistency of BCPs and EMPs between regions, and improve linkages between these plans and NSO plans;
- generate crisis plans for ACGs;
- ensure plans are updated and maintained on a regular basis;
- increase the number of rehearsals;
- improve staff training and awareness of BCM and EM; and
- provide guidance on minimum standards for BCM and EM, and on performance monitoring and reporting against those standards.

Figure 6.7

Area response: Audit findings against core aspects of BC

Stage of BC	*ANAO rating* [A]	*Comment on capability*
Project initiation	Adequate	• Part of broader Centrelink Y2K preparations in 1999.
Identifying critical processes & undertaking Business Impact Analysis	Adequate	• ASOs and CSCs aware of critical business processes, often related to customer contact.
Designing and implementing treatments	Requires Improvement	• Need to streamline and improve continuity related plans, including the relationship between crisis control, BCM and EM, and to improve consistency between Areas. • ASOs and CSCs generally use risk approach.
Rehearsal and plan maintenance	Inadequate	• Generally unacceptably low level of rehearsal in the network.
Training and awareness	Requires Improvement	• Scope to improve formal training. • Need to improve staff awareness of BCM and EM in some parts of the network.

Source: ANAO analysis of Centrelink strategies, plans and capability.

Note: (A) Rating: Adequate, Requires Improvement, Inadequate.

6.78 The BC and EM Framework Project currently underway is seeking to address these identified shortcomings. The ANAO considers that it is important that this project deliver timely and effective solutions to these problems. In particular, there is a need for greater rehearsal across the network, including examining responses to extreme situations such as the loss of ASOs.

7. Centrelink's Emergency Management Role

This chapter discusses Centrelink's EM role and examines the framework and processes used to achieve required responses.

Background

7.1 In addition to ensuring the continuity of key business processes needed to deliver core services (as examined in earlier chapters), Centrelink has an obligation to deliver special and emergency services to the Australian community as directed by the Government.[93] As described in Chapter 1 (see paragraph 1.14), these emergencies are external to Centrelink, but can sometimes coincide with the loss of Centrelink business functions.

7.2 While most EM[94] responses generally have similar phases and elements, these can differ significantly, according to individual policy imperatives and the nature of the incident. This requires Centrelink to maintain a broad operational framework that allows flexibility to respond quickly to specific emergency conditions. Importantly, Centrelink must communicate effectively with other policy-making and emergency service organisations.

7.3 In this context, given the possible overlap between operational requirements with elements of BCM, an objective of this audit was to assess whether Centrelink could satisfy stakeholder expectations of its EM role by examining:

- Centrelink's EM roles and responsibilities, and stakeholder expectations of Centrelink in delivering them;
- Centrelink's EM framework (including interaction with internal crisis management processes); and
- the plans, policies and capabilities available to implement Centrelink's EM framework.

7.4 This chapter addresses these issues, after first providing background to this EM role.

---

[93] This obligation is legislated. Centrelink was set up by the *CSDA Act 1997*, an 'Act to establish an agency for the provision of certain Commonwealth services, and for related purposes'. Under the Act, the Government can direct Centrelink to provide certain services, as required.

[94] This paper refers to Centrelink's community emergency management role as 'emergency management' (EM). However, it is known under many terms within Centrelink, including community emergency management, community disaster response, disaster response and special and emergency community response.

Development of the EM role in Centrelink

7.5 Centrelink's antecedent, the former Department of Social Security, developed the National Disaster Response and Recovery Plan after Cyclone Tracy, which devastated Darwin in 1974. This plan took an external view and was aimed at ensuring the department was better prepared to service its customers and affected communities in the event of a similar major (natural) disaster in the future.

7.6 The development, marketing and testing of the National Disaster Response and Recovery Plan was given high priority and extensive resourcing during the 1970-1980s period and is still the basis for plans currently in place at national, Area and local Centrelink sites across Australia.

7.7 Figure 7.1 provides an indicative chronology of major incidents and emergencies and the response role undertaken by Centrelink in the past five years.

Figure 7.1

Community/emergency responses by Centrelink in past five years

Date	Event/Incident	Response by Centrelink
Jan 1998	Cyclones Sid and Katrina.	Centrelink staff presence at the Disaster Relief Centre in Thuringowa.
Jan-Feb 1998	Katherine Floods. (See case study in this chapter at p.118).	Delivery of Prime Minister's special ex-gratia payment ($7.8 million to more than 10 720 persons).
Jul-Oct 1998	Heavy flooding in Northern NSW and Queensland.	Financial and counselling assistance.
Sep 1998	Victorian Gas Crisis.	Delivery of Prime Minister's Emergency Relief Fund.
Feb 1999	Crookwell bushfires.	Delivery of Commonwealth ex-gratia payment to 37 farmers.
Mar 1999	Exmouth and Moora (devastated by Cyclone Vance).	Financial and counselling assistance.
Apr 1999	Outbreak of Newcastle Disease in chickens on the NSW Central Coast.	Commonwealth ex-gratia payment to farmers whose livestock were destroyed and farms quarantined in an effort to eradicate the disease.
Oct 1999	Batlow (fruit growers' annual harvest devastated by frost).	Delivery of Exceptional Circumstances Relief Payment.
Sep 1999 Jun 2000	Evacuation from East Timor due to civil unrest. Evacuation from Solomon Islands due to civil unrest.	Involved in providing financial and welfare assistance to evacuees as part of the joint State and Commonwealth Government Emergency Reception Teams to receive evacuees as they arrived.
Early 2000	Cyclones Steve, Tessa, Vaughan, and Rosita, which caused rain and severe long-term flooding to numerous towns and communities.	Centrelink social worker assistance in many Emergency Relief Centres, as well as processing numerous Crisis, Special Benefit and continuing payment claims.
Mar 2000	Farmers in North-eastern South Australia affected by drought and locust plague.	Delivery of Commonwealth ex-gratia payment to 192 eligible farmers.

Date	Event/Incident	Response by Centrelink
Late 2000 to early 2001	Several incidents of severe flooding of townships and communities throughout southern Queensland and northern NSW.	Centrelink social worker assistance in many Emergency Relief Centres. Delivery of ex-gratia payments (NSW Farmers Flood Assistance Package, Fodder/Pasture Grant).
Feb 2001	Bushfires in the Eyre Peninsula.	Centrelink staff presence at the Port Lincoln Recovery Centre to provide counselling and advice on social security payments.
Sep 2001	Corporate collapse of Ansett Airlines.	Gateway for the delivery of many government payments and services. Responsible for delivery of $4.9 million package of assistance to stranded travellers and newly redundant employees.
Dec 2001 to Jan 2002	NSW Christmas/New Year Bushfires.	Centrelink staff presence at the Recovery Centre to provide counselling and advice on social security payments. Delivery of ex-gratia payments to assist Volunteer Fire-fighters who actively fought fires and therefore suffered a loss of income.
Oct 2002	Bali terrorist bombings. (See case study in this chapter at p.122).	Centrelink acted as the focus point for the Whole-of-Government response to the consequences of the bombing.
Jan 2003	ACT firestorm. (See case study in this chapter at p.122).	Centrelink staff attended evacuation centres across the ACT. National Crisis Command Centre is activated.

Source: Information provided to ANAO by Centrelink, 2003.

7.8 Figure 7.1 highlights the range of emergency responses that Centrelink has contributed to in recent years. These have included:

- drought relief packages;
- sugar and dairy industry restructuring packages;
- 'one-off' special packages (such as those delivered to stranded travellers and redundant employees after the Ansett collapse); and
- disaster and other ex-gratia payments.

7.9 Ex-gratia payments have been delivered in cash—such as the Katherine Floods payments in 1998, or in kind—such as the suite of travel, accommodation, counselling and other arrangements delivered after the 2002 Bali terrorist bombings. These payments have been made on either a grant or reimbursement basis.

7.10 Figure 7.1 also highlights the increasing expectations of the Government and community stakeholders that agencies, including Centrelink, will deliver effective and timely special response packages when required. The ANAO notes that the increase in scope and frequency of this type of response over the past five years is consistent with the changing nature of the delivery of Government services, as well as the growing impact and incidence of natural and man-made hazards on the Australian community.

7.11 In this climate of rising expectations, with increasingly frequent and complex responses required to cope with various special and emergency situations, it is paramount for Centrelink to ensure that it, and its stakeholders, have a clear understanding of Centrelink's roles and responsibilities. It is also crucial for Centrelink to maintain a framework with sufficient flexibility, yet including sufficient accountability mechanisms, to allow it to fulfil these stakeholder expectations.

Centrelink's EM roles and responsibilities

7.12 Centrelink has a variety of legislative and other responsibilities in regard to emergency responses, arising from its status as a:

- member of Commonwealth Counter-Disaster Committee (convened by Emergency Management Australia);
- response agency under the Commonwealth Disaster Plan (COMDISPLAN);
- delivery agency for Special Benefit, Crisis Payment and other special payments made under the *Social Security Act*;
- delivery agency for Disaster Relief Payments, which can be made after a disaster declaration by the Minister for Social Security; and
- delivery agency for ex-gratia payments made under *CSDA Act* arrangements.

7.13 Most of Centrelink's EM roles outlined above involve high-level coordination and policy guidance from client departments, requiring Centrelink to liaise with stakeholders and disseminate information to operational response staff.

7.14 The ANAO notes that many external response scenarios require the use of internal Centrelink resources. By their nature, many external response scenarios would require a higher degree of availability of Centrelink resources than normal operations. For example, after-hours and weekend access to on-line payment and processing systems is often required to support the special or emergency response, as are mobile computing platforms, and disaster payment systems.[95] Centrelink staff can also themselves be affected by the external emergency (such as during the 1998 Katherine floods, and the 2003 ACT firestorm), requiring a flexibility of response from Centrelink's personnel and network to compensate for possible unavailability of affected staff.

---

[95] The Emergency Management Team is responsible for a 'fly away' processing system known as DAPS (Disaster Assistance Payment System). This system can be remotely deployed and run on standalone or mobile computing platforms to enable recording of basic client and payment data. A precursor to this system was first deployed to administer the Katherine Floods ex-gratia payment.

Case study: Katherine floods of 1998

During the late afternoon and evening of 26 January 1998, the Katherine River rose above its 100-year flood mark and severely inundated most of the urban area of Katherine in the Northern Territory.

The Northern Territory Chief Minister declared a State of Disaster on 27 January. The Prime Minster visited the town on 30 January, and announced that the Commonwealth would provide an ex-gratia payment, later known as the 'Commonwealth Emergency Payment for Katherine Floods'. The payment allowed for $1000 per adult and $200 per child for those affected by the flooding. Centrelink was designated as the agency to deliver the payment.

Centrelink staff and facilities in the town were heavily affected by the flood, with the Centrelink CSC's ground floor fully submerged and uninhabitable. Eight staff experienced severe personal losses due to flood damage.

In conjunction with the emergency response apparatus of the Northern Territory Government, Centrelink's Area North office managed the immediate response to the flooding by establishing a crisis team to coordinate recovery efforts in Katherine, as well as a team to oversee and deliver the ex-gratia payment. Resources from adjoining Areas such as Central and Far North Queensland, as well as the NSO were used as required to support the response and recovery.

Centrelink dispersed some $7.8 million to more than 10 000 persons over the period of availability of the ex-gratia payment. Other persons not eligible for the payment were able to access Special Benefit under relaxed eligibility criteria.

Full Centrelink services were restored on 13 February 1998 with the partial re-opening of the Katherine CSC.

Centrelink's performance in fulfilling its EM roles and responsibilities

7.15 In order to satisfy EM expectations of stakeholders, Centrelink needs to clarify, as clearly as possible:

- its roles and responsibilities, at an agency level, in delivering each of the requirements outlined in paragraph 7.12;
- stakeholder expectations about delivery against these roles and responsibilities; and
- integration with other service providers responding to the emergency.

7.16 The ANAO examined Centrelink's performance against these requirements and found that it was mixed.

7.17 To clarify its roles and responsibilities, Centrelink has made some attempts to define generic response scenarios and capture learnings and accountabilities

via proforma Memorandums of Understanding with client and purchasing agencies. However, these attempts have not yet been formalised. The ANAO considers that this is partly due to a lack of coordination among disparate client/purchasing agencies, and some overlap between their existing Business Partnership Agreements with Centrelink and definitions of the scope of response work undertaken by Centrelink.

7.18 The ANAO considers that Centrelink should more actively manage occasions when service delivery risks arising from evolving community responses are transferred from stakeholders to Centrelink. Even though Centrelink cannot control sources of risk, potential impacts upon Centrelink's reputation as a delivery agency can be extreme, particularly due to fluid policy environments and intense political and media scrutiny.

7.19 Regardless of the above issues, Centrelink remains responsible to deliver services to existing Centrelink customers, albeit with some inevitable changes in the mode and type of service offered, due to the nature of the emergency. This responsibility places further demands upon Centrelink to maintain existing internal controls (right person, right payment, at the right rate, from the right date), and deliver additional response-related payments or advice.

7.20 The ANAO notes that Centrelink has made concerted attempts to position itself as a 'premier broker' in the Australian community[96], and has actively offered its human and technical capabilities as a resource to enable the Government to mount effective delivery responses to a variety of scenarios[97]. The ANAO considers that this proactive positioning has further heightened government and community awareness of Centrelink's capabilities, which potentially increases future demand and expectations for operational responses.

7.21 The ANAO concluded that, based on past performance, Centrelink has identified its EM roles and responsibilities and has discharged them to the high standards expected by stakeholders, including its customers, the Parliament and the wider Australian community. Nevertheless, documenting these expectations has often been on an informal or ad hoc basis, with Centrelink only recently commencing a process to formalise core requirements with other key agencies via Memoranda of Understanding.

7.22 Centrelink's integration with community and emergency stakeholders to manage expectations and outcomes also appears to have room for improvement, and is further discussed in the following section.

---

[96] Lesley Tannahill (National Manager Strategic Services, Centrelink), *Towards being the premier broker—joining up Government and reducing complexity*, speech delivered 6–8 August 2000.

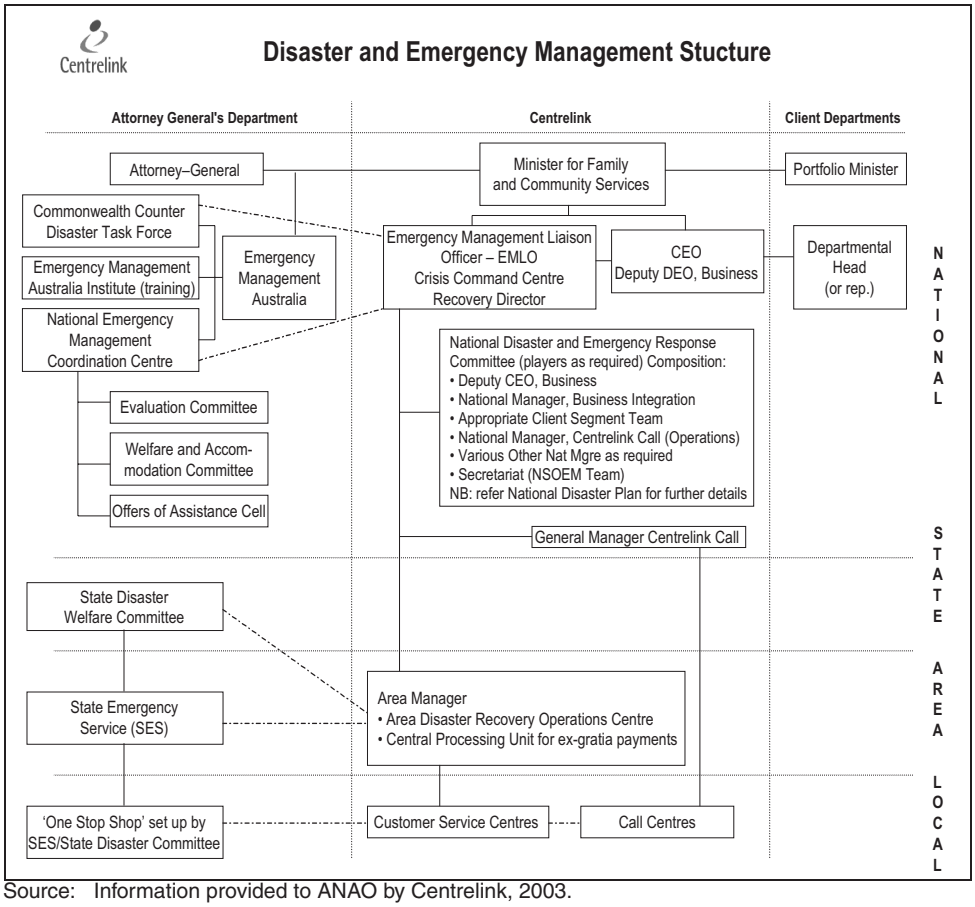
[97] An example of this proactive approach was the offer of the agency's full social worker capacity to help service the Bali bombing survivors, victims and their families by the Centrelink CEO to the Minister for Family and Community Services on 15 October 2002.

Centrelink's EM framework

7.23 Centrelink established an EM framework in the lead up to Y2K. The framework aims to coordinate Centrelink's response role and resources, as well as maintain effective links with other emergency stakeholders at Commonwealth level. An Emergency Management Liaison Officer (EMLO)[98] is responsible for the effective coordination of the disaster management framework and is supported by the Emergency Management Team of the Service Integration Shop.

7.24 Figure 7.2 illustrates Centrelink's current EM framework. To be fully effective, it cannot operate in isolation and relies upon: timely and effective policy advice from FaCS; effective liaison with external stakeholders at various levels; and the availability of Business Resumption Teams, as required, through activation of the BC framework (as discussed in Chapter 2—see paragraphs 2.30 to 2.32).

Figure 7.2
Centrelink's EM framework



Source: Information provided to ANAO by Centrelink, 2003.

[98] At present, the EMLO is also Centrelink's Recovery Director whose role is outlined in Chapter 2 (see paragraph 2.36).

Integration of Centrelink's EM function with BCM and the risk framework

7.25 During the course of this audit, the Specials and Emergencies Team received approval to commence scoping a project to examine the potential of an integrated BC and EM framework that would bring together the agency's internal and external escalation, response and recovery procedures (as discussed in Chapter 2—see paragraphs 2.33 to 2.38). An example of the overlap between the agency's internal and external continuity procedures is the commonality of the National Crisis Command Centre—see Figures 7.2 and 2.2).

7.26 This project aims to document and define existing procedures within Centrelink, capture lessons from previous events and incidents, as well as align with other identified better practices in the public and private sector.[99] Another major aim of the scoping exercise is to identify overlaps and gaps between the existing BCM and EM frameworks. The BCM and EM Framework Project seeks to align Centrelink's enterprise risk framework, internal business outage escalations and procedures, and external emergency recovery role and service obligation.

7.27 The ANAO supports this project, and endorses Centrelink's proposed adoption of better practice models and methodology for management of the risks related to BC and community emergency response and recovery.

Centrelink's EM framework performance

7.28 In order to analyse the adequacy of Centrelink's existing EM and response framework, and Centrelink's performance in implementing it, the ANAO examined the following aspects:

- the appropriateness of Centrelink's EM framework, including internal management structures;
- appropriate liaison and operational links with emergency and community stakeholders at national, State and local levels;
- the adequacy of EM (and related) plans; and
- accreditation and training of response staff.

7.29 The Centrelink EM framework was activated in October 2002 to help coordinate Centrelink's part in the Whole-of-Government response to the 2002 Bali terrorist bombings, and the subsequent medical evacuation and trauma counselling for survivors and their families. The following case study examines Centrelink's role in the emergency response.

---

[99] Identified sources of better practice include the ANAO BPG, Emergency Management Australia, the Business Continuity Institute, DRI international, and Survive.

Case study: Commonwealth response to Bali terrorist bombings

Late on the evening of 12 October 2002, two explosions occurred in the nightclub area of Kuta Beach on the Indonesian island of Bali. Of the 202 people killed as a result of the terrorist attack, 89 were Australians. Some 250 Australians were injured in the blast and medically evacuated to Australia by Royal Australian Air Force and other aircraft. More than 7600 persons were evacuated from the island in the immediate days after the bombing.

As part of a Whole-of-Government response to the incident, Centrelink was tasked to provide a range of assistance including: domestic and international 'free call' hotlines; crisis counselling by Centrelink social workers for victims, their families and friends; and a suite of payments and grants to allow travel for identification and repatriation of remains, re-union travel for injured people in Australia and Bali, assistance with the cost of funerals, assistance with costs to attend funerals or memorials and other costs associated with staying on in Bali due to the explosions.

As delivery agency for this assistance, Centrelink acted as a key focus point for policy and advice from other areas of Government such as the Departments of Prime Minister and Cabinet, Attorney General, Foreign Affairs and Trade, Health and Ageing, and Family and Community Services.

Based on this policy advice and direction, Centrelink developed systems and procedures in order to achieve the required Government response in a timely and effective manner.

Centrelink's role in delivering this assistance, at the time of the audit, was ongoing.

Appropriateness of Centrelink's EM framework

7.30 The ANAO found that Centrelink's current EM framework clearly articulates internal roles and responsibilities, and clearly identifies external liaison links, for national, State, Area and local levels. However, the ANAO notes Centrelink's current project to more closely align its EM and BCM roles (see paragraphs 2.12 to 2.15). By reviewing Centrelink's EM framework and its application in past responses such as some of those listed in Figure 7.1, the ANAO found that the agency has been effective in mounting timely and appropriate responses such as the response made by Centrelink during the ACT firestorm in January 2003.

Case study: Activation of Centrelink Crisis Command Centre during the ACT firestorm in January 2003

Late on the morning of 17 January 2003, a number of bushfires burning out of control converged to form a massive firestorm, directly threatening large areas of Canberra's south-western suburbs.

Due to the extreme weather conditions, ferocity of the fire and direct threat to life and limb, the Chief Minister of the ACT declared a state of emergency early in the afternoon. A number of evacuation centres were set up for people unable to return to their homes due to the fire danger.

Centrelink's Area South West (NSW) became directly involved in the fire response by deploying staff to evacuation centres. Centrelink activated its National Crisis Plan due

to the wide scale of the fire threat, as well as its impact on Centrelink facilities and personnel.

The fire directly threatened Centrelink's National Support Office (NSO) complex in Canberra and a decision was taken by the acting CEO to conduct an emergency shut down of the data centre and evacuation of the building.

Due to evacuation of the building and loss of power, the National Crisis Command Team was unable to meet at either the designated primary or secondary command centres, which are both situated at Centrelink's NSO complex in Canberra.

Once able to convene in ad hoc accommodation at the Centrelink executive suite in Woden, the National Crisis Command Team began coordinating Centrelink's role in the internal and external responses to the firestorm. Within 24 hours of the main firestorm, damage assessment and technical testing had been conducted at the NSO complex in order to re-start equipment in the data centre and provide an 'all-clear' for staff to return to the facility.

The National Crisis Command Centre also coordinated the Human Resource and Communications response in order to assist Centrelink staff and communicate with the public who were affected by the fires. Area South West (NSW), working closely with the NSO, coordinated with the ACT emergency organisations for referral, advice and assistance. The Commonwealth announced no special or ex-gratia payments after the firestorm, although Commonwealth funding was provided to the ACT Government under the existing Natural Disaster Relief Arrangements[100].

The ACT firestorm destroyed more than 500 homes and claimed four lives. Total infrastructure damage and other costs to the ACT and its residents has been estimated in some reports as more than $500 million.

7.31 However, the ANAO did note some issues arising from the coordination and control aspects of the BCM and emergency response framework, as follows:

- the designated National Crisis Command Centre is not fully equipped as per existing Centrelink plans;

[100] The Commonwealth Department of Transport and Regional Services provides financial support for the States and Territories through the Natural Disaster Relief Arrangements (NDRA). These arrangements are designed to reduce the excessive financial burden associated with provision of natural disaster relief and infrastructure restoration by the States. While Commonwealth Government financial assistance is not normally provided until after a natural disaster has occurred, the NDRA framework effectively guarantees that a proportion of the expenditure incurred by States and Territories for the provision of disaster relief will be reimbursed by the Commonwealth Government, subject to the NDRA criteria being met.

- the designated alternate National Crisis Command Centre is in close proximity to the primary National Crisis Command Centre, risking both centres to be rendered unusable by a single event[101];
- documentation boxes and crisis plans for key Business Recovery Teams were not located in the designated National Crisis Command Centre;
- heavy reliance is placed on a small team of staff to fulfil secretariat and coordination roles which can become unsustainable beyond one standard working shift due to fatigue and/or other personal issues for the staff involved; and
- documented escalation and declaration guidelines are not consistently followed.

7.32 Most of these issues were identified in recommendations arising from Centrelink's Exercise Gravity held in 2001, and arose again during the ACT firestorm in January 2003. The ANAO notes that these issues have been included for examination as part of the combined BC and EM Framework project, but still considers that Centrelink needs to take immediate action due to the short warning timeframes that may be expected for any future required special or emergency response.

Recommendation No.10

7.33 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.

Centrelink response

7.34 **Agreed. (a) Completed, (b) Completed, (c) Action Commenced.** Centrelink has ensured National Crisis Command Centres are designated and appropriately equipped as per existing Centrelink plans. Centrelink will ensure documentation boxes for key business resumption teams are available within the National Crisis

[101] This actually did occur when the NSO complex was evacuated at the height of the 2003 ACT firestorm.

Command Centres. Crisis plans will be included following steering committee endorsement. Centrelink will ensure Occupational Health and Safety issues are adequately addressed for National Crisis Command Centre staff.

Effectiveness of liaison and operational links with community emergency stakeholders at national, State and local levels

7.35 Another important aspect of Centrelink's EM framework is the effectiveness of links between the agency and EM stakeholders (refer to Figure 7.2).

7.36 Centrelink's main formal emergency links are with FaCS and Emergency Management Australia. The links with FaCS are mainly at the NSO level and relate to policy advice and direction on the form and scale of the special or emergency response, while the links with Emergency Management Australia enable a more concrete response coordination role at the national, State and local levels.

7.37 During fieldwork for this audit, the ANAO found that ASOs it visited had appropriate liaison links in place with their State/Territory counterparts and had effectively documented expected roles and responsibilities of Centrelink's staff and technical resources. However, as discussed in para 7.45, the ANAO did note that some documentation required updating and better integration with the wider Centrelink BCM and EM framework.

7.38 The ANAO further observed that liaison between Centrelink and its State/Territory emergency counterparts was not consistent throughout Centrelink's Areas. Furthermore, the ANAO observed that the NSO Emergency Management Team did not know what liaison had occurred across various Areas, or what actual Centrelink response commitments or roles had been articulated in State/Territory and local level emergency response plans. The ANAO considers that more support and monitoring within Centrelink at a national level of this stakeholder liaison effort would ensure more consistent planning for, and knowledge about, Centrelink's expected emergency response roles and responsibilities both among Centrelink staff and among community emergency management stakeholders across Australia.

Recommendation No.11

7.39 The ANAO recommends that Centrelink monitor and review its emergency stakeholder liaison and response planning at a national level, and implement relevant findings and recommendations, to ensure effective and consistent special and community emergency responses by Centrelink at the national, State/Territory and local levels.

Centrelink response

7.40 Agreed. Action commenced. Centrelink is in the process of reviewing its emergency stakeholder and response planning and implementing strategies to ensure consistent representation and response at all levels.

Critical infrastructure and liaison with national security agencies

7.41 The current heightened level of security threat environment across Australia has also highlighted the need for Centrelink to enhance links with national security agencies.[102] Centrelink has an Agency Security Advisor, and aims to implement physical, personal and information security policies and procedures in line with the Commonwealth's Protective Security Manual.

7.42 Based on discussions with relevant Centrelink staff, the ANAO found that during the time of audit fieldwork, Centrelink had enhanced its liaison with security agencies about the wider external threat environment, particularly for the critical social and government infrastructure controlled by Centrelink.[103] This liaison has enabled Centrelink to: more effectively interact with relevant security agencies about the wider external threat environment; communicate this threat to appropriate staff within Centrelink; and take steps to implement appropriate protective measures.

Effectiveness of EMPs

7.43 One of the most important aspects of Centrelink's EM framework is the agency's ability to mount effective horizontal and vertical responses, reflecting the scale and nature of the special issue or emergency incident.

7.44 During fieldwork visits to ASOs and CSCs in New South Wales, the Northern Territory, Queensland, Victoria and Western Australia, the ANAO observed that EMPs and related plans were generally of an adequate standard and reflected the main types and scale of emergency responses that Centrelink could be expected to make.

7.45 However, the ANAO noted that emergency response documentation in some sites was out of date or inconsistent. The ANAO also noted a degree of

---

[102] Relevant national security agencies include the Protective Security Coordination Centre, the Australian Security Intelligence Organisation, the Australian Protective Service and the Defence Signals Directorate.

[103] Critical infrastructure is defined by the Commonwealth Attorney General's Department as 'that infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on social or economic well-being or affect national security or defence.' The ANAO assesses that many aspects of Centrelink's services meet this definition of critical infrastructure.

overlap of staff roles and responsibilities between site response procedures[104], site BCPs, and site or Area disaster response and recovery plans.

7.46 The ANAO considers that there is scope for this suite of response documentation to be rationalised, streamlined and cross-referenced into a more readily accessible and standardised format (see Recommendation No.4 at paragraph 4.42 in Chapter 4).

Accreditation and training of emergency response staff

7.47 Training of response staff is widely recognised as a critical aspect of an EM framework to ensure that plans and responses are effectively implemented when required, based on the common sense view that it is too late to start training responders once the response is occurring.

7.48 The ANAO found that Centrelink has conducted crisis simulations (such as Exercises Brolga and Gravity) in recent years for some key senior staff[105], but has not developed an ongoing training program to test and exercise the various elements of a special or emergency response scenario at national, State and local levels.

7.49 Although many Centrelink staff have received on the job training, due to their personal exposure and experience of special and emergency responses, the ANAO found that very few of the staff who would be expected to have a response role had received specific, accredited training for those roles.

7.50 The ANAO notes that a number of accredited, competency-based emergency response and community recovery management courses are offered by the Emergency Management Australia Institute.[106] The ANAO also notes that the Centrelink Virtual College is a Registered Training Organisation and could cooperate with other Registered Training Organisations if relevant training could not be provided from the Centrelink Virtual College's syllabus.

7.51 The ANAO therefore reinforces the requirement for Centrelink to implement a structured process to develop a competency and learning framework as specified in Recommendation No.5 (see paragraph 4.68 in Chapter 4).

---

[104] These procedures usually cover incidents such as violent/aggressive customers and fire or other hazards that require evacuation of the site.

[105] Some Centrelink staff were also involved in Exercise Minotaur, which was run by Agriculture, Fisheries and Forestry Australia in 2002, and simulated and tested a Whole-of-Government response to a major outbreak of foot and mouth disease in Australia.

[106] The Emergency Management Australia Institute is the education and information arm of Emergency Management Australia.

7.52 Overall, the ANAO concluded that, notwithstanding the opportunities for improvements identified in this chapter and proposed in the integrated BC and EM framework project, Centrelink has generally adequate plans and procedures. Moreover, skilled and committed staff have enabled it to effectively implement its special and emergency response role when required at the national, State/Territory and local levels.

Canberra ACT
22 October 2003

Oliver Winder
Acting Auditor-General

Appendices

Appendix 1

Audit Criteria

The ANAO used the criteria below in the audit of BCM and EM in Centrelink.

Figure A1.1
Audit criteria

The criteria for the audit were to establish whether:

- Centrelink's BCM framework is integrated into its risk management framework so that BCM focuses on the main business risks and critical business functions;
- Centrelink's BCM procedures and plans adhere to better practice principles, at the minimum as outlined in the ANAO Better Practice Guide on BCM; and
- Centrelink effectively implements its Whole-of-Government role in continuity/disaster recovery at local, State and national levels.

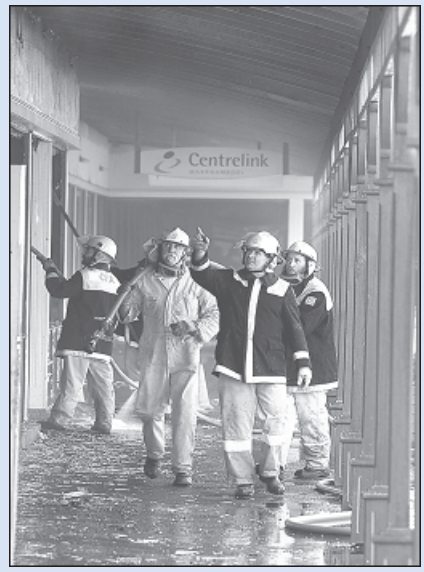
Appendix 2

Case Study of Fire at Warrnambool CSC

Background

During the course of the audit, Centrelink's Warrnambool Customer Service Centre (CSC) was destroyed by fire. The fire, which started on the morning of Sunday 6 October 2002, heavily damaged the low-rise office and retail complex housing the CSC, making continued tenancy impossible and potentially causing major business disruption of Centrelink's service delivery to the local community.

A Centrelink employee working at the site on the Sunday escaped from the building and immediately notified the regional operations manager. Notification of the fire was escalated to the Victoria West Area Manager, then quickly on to Centrelink's National Recovery Director and the Centrelink CEO.



Crisis response

The Area Manager assembled a Crisis Command Team (CCT) at the Area Support Office (ASO) in accordance with the Area Crisis Plan. The National Recovery Director also advised various key National Support Office (NSO) managers of the fire.

The Area CCT met at 3 pm, and received initial damage reports from Centrelink officers at the fire scene. Based on these reports and after consultation with the National Recovery Director, a decision was made to attempt to provide basic services by 8:30 am the next day, which was a Monday and a normal business day.

Recovery actions

A State Emergency Service command and control caravan, temporary signage and office furniture were hastily assembled by local Centrelink staff on the Sunday evening and installed in a car park adjacent to the burnt out CSC. A number of other actions were concurrently commenced by the ASO and NSO including:

- a decision by the Area Manager to go 'off-line' from normal business activities to fully coordinate the recovery effort, and appointment of an acting Area Manager to manage day-to-day business of the Area network;
- despatch from the NSO of pre-configured remote access laptop computers and a network server loaded with the CSC's most recently backed-up data to enable access to the Centrelink mainframe and therefore the ability to process customer information;
- despatch of IT support staff from Adelaide and Canberra to install temporary IT equipment;

- activation of State and national media plans to communicate key messages via local and regional media to local customers about the fire and special temporary processing procedures in place;
- discussions with the Department of Family and Community Service seeking authorisation for temporary telephone lodgement of forms for customers affected by the CSC fire, and subsequent implementation of this interim processing by Centrelink Call;
- rescheduling on the mainframe system of all customer appointments booked for the CSC for the next week, followed up with individual telephone calls to customers by ASO staff;
- booking of Employee Assistance Scheme counsellors to come to the temporary site and conduct incident de-briefing for Centrelink staff, as required; and
- rostering of CSC staff for temporary shop-front duties, and relocation of some specialised processing staff to Portland, Hamilton and Colac.

The temporary facility was opened as scheduled on the Monday morning, and was further upgraded over the next two days by the addition of voice and data lines, a portable power generator and construction huts.

Recovery transition

NSO Buildings Team staff arrived on site within two days in order to liaise with insurance assessors, and check with local realtors for available temporary office space. Under the supervision of the Victorian Country Fire Authority, local Centrelink staff were able to retrieve some personal effects and commence securing customer records and corporate documentation.

After the subsequent hand-over of the CSC site by the fire brigade, and an Occupational Health and Safety inspection, designated teams of Centrelink staff and contractors entered the CSC site and retrieved furniture, office equipment, client and customer records, and salvaged hard disks from computers in order to safeguard customer data.

A small call centre facility, which had been closed down recently by Telstra, was identified as a potential site for relocation of the CSC. Negotiations with Telstra were conducted by senior officers in the NSO, with the premises becoming occupied and operational eight days after the CSC fire.

After 10 days, the ASO CCT was disbanded and the Area Manager returned to normal management duties. In all, the crisis and recovery efforts involved Centrelink officers at the Warrnambool CSC site, adjoining CSCs, the ASO, and the NSO. At the NSO level, the Voice, People Management, I&T Infrastructure, Buildings, and Communication Business Resumption Teams all played a direct role in assisting with the management of the crisis response, and supporting business recovery.

ANAO analysis

The ANAO observed that prompt activation and escalation of existing plans ensured an effective and appropriate use of ASO and NSO resources and expertise. Focused management of staff morale and skills also ensured that maximum staff capability could be brought to bear during the recovery effort.

The ANAO further observed that existing plans provided an appropriate framework and guidance for management of a complex business outage, and articulated the steps needed for a smooth business recovery.

Centrelink learnings

Centrelink commissioned Ernst and Young to conduct a post-incident review of the outage. This post-incident review confirmed the analysis by ANAO that the response and recovery actions were effective and appropriate. The Ernst and Young review identified some areas for improvement of Centrelink's response procedures relating to insurance and costs, human resource management, and occupational health and safety.

Appendix 3

Analysis of the BCM component of Centrelink Project Plans

Given the ANAO's broad approval of the framework for treating business continuity (BC) in the project management process, the ANAO undertook a brief analysis to gauge the extent to which this process was implemented in practice.

From a total population of 97 approved projects undertaken during the 2002-03 financial year, the ANAO selected 25 projects for review (26 per cent of the total approved projects). Of the 25 projects selected, Centrelink's Business Continuity Unit (BCU) advised that five projects did not qualify for planning documents due to the nature of those projects. Thus, testing was directed towards the remaining 20 projects. The projects were principally oriented towards I&T projects.

To determine if Business Continuity Plans (BCPs) were required, the ANAO sought preceding project plans for approved projects. If those project plans specified BCPs were to be developed, the ANAO sought to establish whether they had been undertaken.

The ANAO made a number of observations about the system for maintaining records of project plans and respective BCPs, described in Figure A3.1 below.

Figure A3.1

ANAO Testing of Centrelink Projects Office's Records: General Observations

Audit Expectation/Objective	Result
The ANAO expected that the BCU, which is listed as a stakeholder in the process, would hold project plans and have a record, preferably electronic but at least a hard copy, of the existence and nature of these plans.	This was not the case. The BCU did not hold the project plans or records of the BC sections of the project plans. The BCU advised that it was not responsible for holding project plans, which were reportedly maintained by the Centrelink Projects Office (CPO).
The ANAO then expected that the CPO would have a readily accessible automated record of the project plans (specifically the Project Management Plans).	This was also not the case. While there is a field in the CPO's database linked to preceding project plans, this field had not been populated and so the information was not easily available electronically. As a consequence, it was necessary to extract the entire database for individual projects to locate specific plans. The CPO advised that the automated records are not necessarily comprehensive and the hardcopy of the project plans would be a superior record.

Audit Expectation/Objective	Result
The ANAO then sought access to the hard copy records held by the CPO.	The hardcopy records were often extensive (e.g. six files for one project), but did not necessarily reflect updated project plans and did not contain the BCPs. Not all hardcopy records were readily accessible as older files are retired to the archives for storage. To check if the BCPs for each selected project were completed, the CPO advised that the ANAO would have needed to contact the responsible project officers and ask for the documentation. The BCU performed this task in the latter stages of audit fieldwork.

The ANAO made further observations from its audit testing of the Centrelink Project Office's automated records, outlined in Figure A3.2, below.

Figure A3.2

ANAO Audit Testing of Centrelink Project Planning Documents

The majority of project plans reflected consideration of risks throughout the project life cycle. Of the original 25 projects selected, the CPO's automated records indicated that risk profiles were ranked as low, medium or high–distributed as 24 per cent low, 44 per cent medium and 32 per cent high.
Of the 20 projects available for testing, only 60 per cent of projects had project management plans and/or business cases represented. The lack of these project-planning documents would not promote the generation of the BCPs. The ANAO identified only one instance of a BCP reflected in the CPO's automated records.
Very few project management plans indicated any analysis of the need for BCPs.
Of the 20 projects available for testing, the ANAO sought BCPs from all sources (i.e. automated and hard copy from the BCU, CPO or project managers). Of the 20 projects, only seven projects (35 per cent) had BCPs. For isolated projects, which had no BCPs, alternative plans (i.e. disaster recovery plans, crisis plans) were prepared. Of the sample tested, the BCU only held four of the BCPs. Of all the current Centrelink projects, the BCU held only 10 BCPs.
The BCU adopted a passive approach to collecting BCPs, as it maintained only a small number of plans for projects. The BCU acknowledged its lack of authority to question or overrule the decisions of individual project managers regarding the need to prepare a BCP.
In the majority of cases, the main reference number (PRN#) assigned at the initiation of the project was not carried forward to other respective documents/phases, thus creating confusion in subsequent phases of the project life cycle.

To address these findings, the ANAO included Recommendation No.3 at paragraph 4.23 in Chapter 4.

Appendix 4

CobiT Standards to 'Ensure Continuous Service'

This appendix outlines the control objective, critical success factors, key goal indicators, key performance indicators and detailed control objectives for the IT process, 'Ensure Continuous Service' (DS4). [107]

Control Objective

Control over the IT process, *Ensure Continuous Service*, with the business goal of ensuring 'IT services are available as required and ensuring a minimum business impact in the event of a major disruption' is enabled by 'having an operational and tested IT continuity plan, which is in line with the overall business continuity plan and its related business requirements'.[108]

Critical Success Factors (CSFs)

CSFs define the most important issues or actions for management to achieve control of its IT processes. CSFs must be management-oriented implementation guidelines, and must identify the most important things to do strategically, technically, organisationally or procedurally.[109] Table A4.1 presents the CSFs prescribed by CobiT.[110]

Table A4.1

Critical Success Factors to Ensure Continuous Service (DS4)

Critical Success Factors
• A no-break power system is installed and regularly tested.
• Potential availability risks are proactively detected and addressed.
• Critical infrastructure components are identified and continuously monitored.
• Continuous service provision is a continuum of advance capacity planning, acquisition of high-availability components, needed redundancy, existence of tested contingency plans and the removal of single points of failure.
• Action is taken on the lessons learned from actual downtime incidents and test executions of contingency plans.
• Availability requirements analysis is performed regularly.
• Service level agreements are used to raise awareness and increase cooperation with suppliers for continuity needs.
• The escalation process is clearly understood and based on a classification of availability incidents.
• The business costs of interrupted service are specified and quantified where possible, providing the motivation to develop appropriate plans and arrange for contingency facilities.

[107] IT Governance Institute, CobiT, *Management Guidelines*, Version 3, July 2000, p. 68.

[108] Ibid., p. 68.

[109] ibid., p. 8.

[110] Ibid., p. 68.

Key Goal Indicators (KGIs)

KGIs define measures that tell management, after the fact, whether an IT process has achieved its business requirements, usually expressed in terms of information criteria:

- availability of information needed to support the business needs;
- absence of integrity and confidentiality risks;
- cost-efficiency of processes and operations;
- confirmation of reliability, effectiveness and compliance. [111]

Table A4.2 presents the KGIs prescribed by CobiT.[112]

Table A4.2
Key Goal Indicators for Ensure Continuous Service (DS4)

Key Goal Indicators
• No incidents causing public embarrassment.
• Number of critical business processes relying on IT, that have adequate continuity plans.
• Regular and formal proof that the continuity plans work.
• Reduced downtime.
• Number of critical infrastructure components with automatic availability monitoring.

Key Performance Indicators (KPIs)

KPIs define measures which determine how well the IT process is performing in enabling the goal to be reached; are a lead indicator of whether (or not) a goal will likely be reached; and are good indicators of capabilities, practices and skills.[113] Table A4.3 presents the KPIs prescribed by CobiT.[114]

[111] IT Governance Institute CobiT, *Management Guidelines*, Version 3, July 2000, p. 8.

[112] Ibid., p. 68.

[113] Ibid., p. 8.

[114] Ibid., p. 68.

Table A4.3
Key Performance Indicators for Ensure Continuous Service (DS4)

Key Performance Indicators
• Number of outstanding continuous service issues not resolved or addressed.
• Number and extent of breaches of continuous service, using duration and impact criteria.
• Time lag between organisational change and continuity plan update.
• Time to diagnose an incident and decide on continuity plan execution.
• Time to normalise the service level after execution of the continuity plan.
• Number of proactive availability fixes implemented.
• Lead time to address continuous service shortfalls.
• Frequency of continuous service training provided.
• Frequency of continuous service testing.

Detailed Control Objectives

CobiT's Audit Guidelines outline detailed control objectives, which are consistent with the high-level control objective specified for the designated IT process. Table A4.4 presents control objectives prescribed by CobiT.[115]

Table A4.4
Control Objectives for Ensure Continuous Service (DS4)

Control Objectives for Ensure Continuous Service		
No.	**Title**	**Description**
#4.1	**IT Continuity Framework**	IT management, in cooperation with business process owners, should establish a continuity framework, which defines the roles, responsibilities and the risk-based approach/methodology to be adopted and the rules and structures to document the continuity plan as well as the approval procedures.
#4.2	**IT Continuity Plan Strategy and Philosophy**	Management should ensure that the IT continuity plan is in line with the overall business continuity plan to ensure consistency. Furthermore, the IT continuity plan should take into account the IT long- and short-range plans to ensure consistency.

[115] IT Governance Institute, CobiT, *Audit Guidelines*, '*Detailed Control Objectives',* Version 3.

Control Objectives for Ensure Continuous Service		
No.	**Title**	**Description**
#4.3	**IT Continuity Plan Contents**	IT management should ensure that a written plan is developed, containing the following: • guidelines on how to use the continuity plan; • emergency procedures to ensure the safety of all affected staff members; • response procedures meant to bring the business back to the state it was in before the incident or disaster; • recovery procedures meant to bring the business back to the state it was in before the incident or disaster; • procedures to safeguard and reconstruct the home site; • coordination procedures with pubic authorities; • communication procedures with stakeholders, employees, key customers, critical suppliers, stakeholders and management; and • critical information on continuity teams, affected staff, customers, suppliers, public authorities and media.
#4.4	**Minimising IT Continuity Requirements**	IT management should establish procedures and guidelines for minimising the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.
#4.5	**Maintaining the IT Continuity Plan**	IT management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resource procedures.
#4.6	**Testing the IT Continuity Plan**	To have an effective continuity plan, management needs to assess its adequacy on a regular basis or upon major changes to the business or IT infrastructure. This requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.
#4.7	**IT Continuity Plan Training**	The disaster continuity methodology should ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.
#4.8	**IT Continuity Plan Distribution**	Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorised personnel and should be safeguarded against unauthorised disclosure. Consequently, sections of the plan need to be distributed on a need-to-know basis.
#4.9	**User Department Alternative Processing Backup Procedures**	The continuity methodology should ensure that the user departments establish alternative processing procedures that may be used until the IT function is able to fully restore its services after a disaster or an event.

Control Objectives for Ensure Continuous Service		
No.	**Title**	**Description**
#4.10	**Critical IT Resources**	The continuity plan should identify the critical application programs, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs. Critical data and operations should be identified, documented, prioritised and approved by the business process owners, in cooperation with IT management.
#4.11	**Backup Site and Hardware**	Management should ensure that the continuity methodology incorporates an identification of alternatives regarding the backup site and hardware as well as a final alternative selection. If applicable, a formal contract for these types of services should be concluded.
#4.12	**Off-Site Backup Storage**	Off-site storage of critical backup media, documentation and other IT resources should be established to support recovery and business continuity plans. Business process owners and IT function personnel should be involved in determining what backup resources need to be stored off-site. The off-site storage facility should be environmentally appropriate to the media and other resources stored and should have a level of security commensurate with that needed to protect the backup resources from unauthorised access, theft or damage. IT management should ensure that off-site arrangements are periodically assessed, at least annually, for content, environmental protection and security.
#4.13	**Wrap-Up Procedures**	On successful resumption of the IT function after a disaster, IT management should establish procedures for assessing the adequacy of the plan and update the plan accordingly.

Series Titles

Audit Report No.8 Performance Audit
Commonwealth Management of the Great Barrier Reef Follow-up Audit
The Great Barrier Reef Marine Park Authority

Audit Report No.7 Business Support Process Audit
Recordkeeping in Large Commonwealth Organisations

Audit Report No.6 Performance Audit
APRA's Prudential Supervision of Superannuation Entities
Australian Prudential Regulation Authority

Audit Report No.5 Business Support Process Audit
The Senate Order for Departmental and Agency Contracts (Autumn 2003)

Audit Report No.4 Performance Audit
Management of the Extension Option Review—Plasma Fractionation Agreement
Department of Health and Ageing

Audit Report No.3 Business Support Process Audit
Management of Risk and Insurance

Audit Report No.2 Audit Activity
Audit Activity Report: January to June 2003
Summary of Outcomes

Audit Report No.1 Performance Audit
Administration of Three Key Components of the Agriculture—Advancing Australia (AAA) Package
Department of Agriculture, Fisheries and Forestry—Australia
Centrelink
Australian Taxation Office

Better Practice Guides

Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
AMODEL Illustrative Financial Statements 2003	May 2003
Managing Parliamentary Workflow	Apr 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Internal Budgeting	Feb 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
Life-Cycle Costing	Dec 2001
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	Jun 2001
Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.49 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997

Public Sector Travel	Dec 1997
Audit Committees	Jul 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres & Handbook	Dec 1996
Paying Accounts	Nov 1996
Asset Management & Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996