

The Auditor-General
Audit Report No.16 2008–09
Performance Audit

The Australian Taxation Office's Administration of Business Continuity Management

Australian Taxation Office

Australian National Audit Office

© Commonwealth
of Australia 2008

ISSN 1036-7632

ISBN 0 642 81047 8

COPYRIGHT INFORMATION

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

Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration,
Attorney-General's Department,
Robert Garran Offices,
National Circuit
Barton ACT 2600

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



Canberra ACT
22 December 2008

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the *Australian Taxation Office* 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 *The Australian Taxation Office's Administration of Business Continuity Management*.

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

A handwritten signature in black ink, appearing to read 'Ian McPhee', is positioned above the printed name.

Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

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

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

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

Audit Team
David Crossley

Contents

Abbreviations.....	7
Summary and Recommendations	9
Summary	11
Introduction	11
Audit objective and scope	12
Conclusion	12
Key findings by chapter.....	14
Summary of agency response	19
Recommendations	21
Audit Findings and Conclusions	23
1. Background and Context.....	25
Introduction to business continuity management.....	25
The importance of business continuity management to the Tax Office.....	26
Business continuity management, risk management and business impact analysis	27
Business continuity strategy	31
Business continuity ‘program’ approach	32
Audit objective and scope	34
2. Business Continuity: Better Practices and Benchmarks.....	36
Overview	36
3. Business Continuity Management Framework	41
Business continuity management in the Tax Office.....	41
Corporate Management Practice Statement on emergency control organisation	43
Corporate Management Practice Statement on risk and issues management	46
Corporate Management Practice Statement on business continuity.....	47
4. Implementing the Business Continuity Management Framework	53
The Tax Office’s approach to planning for business continuity management.	53
Linking risk management and business continuity management	54
Maximum acceptable outage.....	56
IT continuity management.....	56
Exercises to test business continuity management arrangements.....	57
Business continuity awareness.....	59
Facilities management and disruptions	60
Resources relevant to business continuity	61

Appendices	67
Appendix 1: Agency Response	69
Appendix 2: Glossary of terms used in relation to this Audit Report	70

Figures

Figure 1.1	Risk management.....	28
Figure 1.2	Business continuity management relationships	30
Figure 1.3	Key components of business continuity management in the Tax Office	32
Figure 2.1	Tax Office key business continuity linkages.....	37
Figure 2.2	Framework for business continuity management depicted in the ANAO <i>Better Practice Guide—Business Continuity Management</i>	39
Figure 3.1	Operation of the business continuity process.....	43
Figure 3.2	Business continuity infrastructure within the Tax Office	51
Figure 4.1	Tax Office business continuity management framework elements	54

Abbreviations

ANAO	Australian National Audit Office
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BSL	Business and Service Lines
CEO	Chief Executive Officer
CMPS	Corporate Management Practice Statement
ECO	Emergency Control Organisation
EMP	Emergency Management Plan
EPC	Emergency Planning Committee
HR	Human Resource
ICT	Information, Communications and Technology
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MAO	Maximum Acceptable Outage
OCG	Office of Government Commerce
PMC	Prime Minister and Cabinet
Tax Office	Australian Taxation Office
SES	Senior Executive Service
Y2K	Year 2000

Summary and Recommendations

Summary

Introduction

1. Government agencies deliver a wide range of programs and services which are critical to the economic and social well-being of our society. Single or multiple events may cause a significant disruption or outage to the 'business as usual' operations of agencies, compromising their ability to function, which could have significant consequences for citizens, businesses and government.
2. In order to respond to such disruptions, agencies need to consider business continuity management (BCM) as an integral part of their organisational risk management framework. BCM planning guides agencies in responding to unplanned disruptions or outages, variously described as an emergency, crisis and/or disaster¹, when normal management practices and procedures may be unable to cope. The primary objective of BCM is to ensure the uninterrupted availability of all key resources required to support essential (or critical) business activities and to return the agency to 'business as usual' within a predefined acceptable time limit (the maximum acceptable outage—MAO) following a disruption.
3. Effective BCM planning is particularly important for agencies such as the Australian Taxation Office (Tax Office). As the main administrator of Australia's tax and superannuation systems, it is critical that the Tax Office has in place an appropriate BCM framework to minimise disruptions to its role as the Government's principal revenue collection agency.
4. As at 30 June 2008 the Tax Office employed 23 303 ongoing and non-ongoing employees and occupied office space in some 70 buildings across Australia. During the year to 30 June 2008, the Tax Office processed more than 32.5 million income tax and Business Activity Statement lodgements, and responded to more than 12 million taxpayer enquiries, in collecting revenues of some \$278.0 billion on behalf of the Government.

¹ A number of other terms are used to describe unplanned disruptions or outages such as: event; incident; business disruption or interruption; and, business interruption event. All terms refer to the same concept.

Audit objective and scope

5. The objective of the audit was to assess the adequacy and effectiveness of the BCM practices and procedures within the Tax Office in preparing for, or responding to, disruptions to 'business as usual' operations.
6. Particular emphasis was given to examining whether the Tax Office:
 - has in place an appropriate framework for the administration of BCM;
 - adheres to sound BCM principles for its plans, practices and procedures; and
 - has appropriate mechanisms to test, evaluate, report and improve on its administration of BCM.
7. The scope of the audit did not include an examination of the continuity planning for business processes between the Tax Office and external agencies such as the Reserve Bank of Australia and Centrelink.

Conclusion

8. As the main administrator of Australia's tax and superannuation systems it is critical that the Tax Office has in place effective BCM practices and procedures to ensure a timely and appropriate response to business disruptions. A significant or long term disruption to 'business as usual' within the Tax Office has the potential to disrupt the collection of taxation revenues. It could also have a significant impact on the efficiency and the effectiveness of the Tax Office in administering and regulating the tax and superannuation systems. This in turn could lead to a loss of reputation, and reduced taxpayer confidence in the self assessment taxation system.
9. The Tax Office has a well developed BCM framework which is integrated into its 'business as usual' operations. Its BCM framework consists of the following four elements:
 - emergency management;
 - crisis management;
 - disaster recovery; and
 - business resumption planning.

10. The Tax Office has documented its BCM processes in the: Emergency Control Organisation Corporate Management Practice Statement² (Emergency Control Organisation CMPS); and Business Continuity Corporate Management Practice Statements³ (Business Continuity CMPS) and Risk and Issues Management Corporate Management Practice Statement⁴ (Risk and Issues Management CMPS). These documents describe practices and procedures that business and service lines (BSL) should use in relation to the BCM framework.

11. There is however scope for the Tax Office to better integrate the administration of the component elements of its BCM framework into a single program of work and to enhance the functioning of its emergency management within the framework

12. The Tax Office's approach to BCM has been developed by drawing on the ANAO *Better Practice Guide—Business Continuity Management*⁵ and by seeking to enhance its BCM capacity through the ongoing consideration and adoption of improved practices. The BCM framework is supported by a wide-ranging set of policies, practices and procedures.

13. The BCM framework implemented by the Tax Office has evolved over a number of years and reflects the benefits of having key operational processes and people distributed across a number of locations throughout Australia. In most cases work flows affected by an outage or disruption occurring in one of the 70 office locations occupied by the Tax Office can be redirected and dealt with by staff located elsewhere while the cause of the disruption is being addressed.

14. The BCM framework demonstrates a mature application of key elements of sound BCM practices including:

- management support for BCM activities through the appointment of dedicated BCM executives and staff to develop, maintain and test the BCM plan;
- identifying key business processes and critical IT applications;

² Tax Office, Corporate Management Practice Statement, *Emergency Control Organisation*, 2003/21.

³ Tax Office, Corporate Management Practice Statement, *Business Continuity*, 2003/20.

⁴ Tax Office, Corporate Management Practice Statement, *Risk and Issues Management*, 2003/02.

⁵ ANAO *Better Practice Guide—Business Continuity Management*, January 2000, Canberra, is currently being updated for release in 2009.

- incorporating risk management and business analysis activities into the BCM strategy;
- the tailored design of business continuity treatments to address specific Tax Office challenges resulting from its decentralised operations;
- creating a detailed business continuity planning (BCP) database; and,
- the ongoing testing, evaluation, updating and reporting of the BCM plans and the overall framework.

15. The Tax Office has appropriate mechanisms to test and evaluate its administration of business continuity enabling it to continuously reassess the effectiveness of its policies and procedures. This assisted the Tax Office to demonstrate that the challenges arising from the actual crisis events, as well as the testing exercises, that occurred during the course of the audit were met effectively through the implementation of the current BCM plans. Where appropriate, lessons learnt from responding to these specific disruptions were used to reassess the ongoing effectiveness of the Tax Office BCM plans, practices and procedures.

16. The ANAO has made six recommendations aimed at improving the Tax Office's BCM planning and procedures.

Key findings by chapter

Background and Context (Chapter 1)

17. The Tax Office has allocated significant resources to achieve its outcome of effectively managing and shaping Australia's self assessment taxation systems. A key contribution to the achievement of this outcome is the work that the Tax Office has undertaken to build taxpayer confidence in the system. A significant or long term interruption to 'business as usual' within the Tax Office has the potential to disrupt or undermine revenue collections or affect its ability to respond to taxpayer enquiries on a timely basis. BCM is critical if the Tax Office is to meet Government expectations that revenue collection will continue to be managed despite disruptions to 'business as usual' which will inevitably occur.

18. A comprehensive approach to developing a business continuity strategy requires consideration of risk management and business analysis processes in identifying the potential sources of, and impacts from, disruptions to 'business as usual'. The Tax Office has identified key risk assessment

information and business processes to form part of the data used to produce its business impact analysis. This in turn has also assisted the Tax Office in building its BCP database.

19. The Tax Office has a BCM strategy which is articulated in its CMPS. This strategy is communicated through a framework consisting of emergency management, crisis management, disaster recovery and business resumption.

20. The Tax Office has distributed its key operational processes and people across a number of locations throughout Australia. This matrix structure adopted by the Tax Office gives it a high degree of business resilience that has allowed it to effectively withstand business disruptions or outages. Most documented disruptions in the 12 months to August 2008 arose from the total or partial loss of the use of buildings occupied by the Tax Office, rather than other disruptions, for example loss of IT systems capacity.

21. The Tax Office has an overarching framework that it uses to implement BCM. However this framework does not address the program management aspects of implementing BCM across an organisation as large and geographically dispersed as the Tax Office. The British BCM standard proposes that BCM is best run as an integrated program of work at a whole of organisation level.⁶ At present the Tax Office separately completes a number of related BCM projects without having an integrated program management structure that clearly articulates how the individual project components of BCM are organised, directed and implemented in a coordinated way. An integrated program structure would allow for stronger coordination of the management of the individual BCM projects and activities within the Tax Office; and their success could be better monitored and reported to inform Tax Office management of the status of overall BCM preparedness.

Business Continuity: Better Practices and Benchmarks (Chapter 2)

22. A number of Australian and international standards and publications are available to assist organisations in setting up their BCM frameworks, which can also be used to benchmark their implementation strategies. Currently the Tax Office uses the ANAO *Better Practice Guide—Business Continuity Management*⁷ as its principal source of reference in guiding its approach to BCM. However the Tax Office recognises that BCM is a dynamic field and so

⁶ British Standard BS25999-1:2006 *Business Continuity Management*, Part 1: Code of Practice.

⁷ ANAO, *Better Practice Guide—Business Continuity Management*, January 2000, Canberra.

also reviews overseas standards to identify evolving elements of better practice that may be appropriate for its circumstances and enhance its BCM approach.

23. The Tax Office has implemented a BCM framework incorporating key elements of sound BCM practices which have been articulated in a series of CMPS and other documents.

24. The Tax Office Business Continuity CMPS provides policy and procedural instruction to staff in relation to the operation of BCM within the Tax Office.

25. The development and maintenance of these policies and procedures at an operational level is reflected in detail in the Tax Office's BCP database which was produced by applying the process methodology outlined within the ANAO *Better Practice Guide—Business Continuity Management*.⁸

26. The Tax Office has recognised that emergency management, crisis management, disaster recovery and business resumption should be wholly integrated, in accordance with business continuity standards, and has based its training and awareness packages around this concept.

Business Continuity Management Framework (Chapter 3)

27. The Tax Office's BCM framework, which has evolved over a number of years, in conjunction with its decentralised management operations, and its alternate BCM management structure which is activated in the event of a crisis situation, gives the agency a high degree of resilience.

28. The Tax Office business continuity framework consists of four elements that deal with continuity issues at different times and with different yet integrated strategies. The framework is supported by the various CMPS. These documents guide Tax Office staff in the management of a business continuity event by stating who and in what circumstances a crisis or disaster may be declared. The business continuity policies then authorise designated Tax Office staff, such as the BCM Director and the Disaster Recovery Manager, to resolve the business disruption and return to normal services.

29. In dealing with a crisis or disaster, the Tax Office has three designated teams responsible for business continuity, emergency control and disaster recovery respectively, that are staffed from business service lines. The National BCM Director coordinates across all three of these designated teams to manage

⁸ ANAO, *Better Practice Guide—Business Continuity Management*, January 2000, Canberra.

the transition from one phase of a crisis to another. Information from a crisis or disaster is ultimately captured in the BCP database and this information is subsequently used to improve business continuity planning.

30. The National BCM Director within the Tax Office plays a crucial role in coordinating some, but not all, aspects of the implementation of the business continuity framework. At present responsibility for the emergency management component of BCM rests with individual staff located within each Tax Office occupied building. These staff are part of the Emergency Control Organisation (ECO) within the Tax Office and are guided specifically by the Emergency Control Organisation CMPS and the separately constituted Emergency Planning Committee (EPC) for each major Tax Office site.

31. The EPCs independently produce practices and procedures documentation and arrange for testing of the procedures. The ANAO sees benefits in using a systems based approach to managing and recording emergencies. Ideally the ECO could use the BCP database which would also more fully integrate emergency management into the business continuity framework. By more closely aligning emergency management to crisis management, staff safety could be better integrated into the response to business continuity disruptions.

32. Certificates of Assurance are provided to the Commissioner annually on business continuity, to verify BCM practices and procedures. There would be value in the Tax Office also extending the coverage of these Certificates to the ECO in order to further assist in the integration of staff safety within the business continuity framework.

33. BCM better practice suggests that most chief executive officers are unlikely to have the time to properly dedicate themselves to BCM during a crisis if they are to continue to manage their organisations. The Tax Office could therefore consider the appointment of a person other than the Commissioner as the national crisis manager. This would allow the Commissioner to ensure appropriate liaison with Government, other senior public sector agency managers, media and other stakeholders as required during the course of a BCM event.

Implementing the Business Continuity Management Framework (Chapter 4)

34. The Tax Office business continuity framework is based on accredited standards and benchmarks. In addition to these standards and benchmarks,

the Tax Office has built a business continuity tool in the form of a BCP database. The creation and ongoing use of this database is a significant achievement in defining and operationalising business process resumption plans. The information on the BCP database provides a level of structure and integration around continuity issues that is not achievable through the use of standard templates and worksheets.

35. At present the updating of the BCP database is coordinated and undertaken largely by the National BCM Director. In light of potential 'key-man' risks and the need for succession planning there may be advantages in extending the maintenance of the BCP database to other staff within the Tax Office BCM workspace to increase their BCM knowledge and skills.

36. During the audit the ANAO witnessed a number of business continuity events. The Tax Office managed these events in an appropriate and effective manner that either avoided business disruption or quickly resumed business as normal. In each case Tax Office staff, especially those with BCM responsibilities, demonstrated that lessons were learnt from the event and the BCP was, where appropriate, updated.

37. The ANAO observed that there was a reluctance in both exercises and in real time events, where appropriate, for Tax Office staff to formally declare a crisis and subsequently to declare a cessation of the crisis. If staff were provided with clear and succinct guidance on crisis declaration and cessation, it would provide a basis for the crisis management structure to be implemented thereby specifically identifying who is in control of the situation and hence responsible for decision making. This is in itself more likely to result in a more timely return to business as usual.

38. BCM better practice suggests that a schedule of exercising and testing needs to be agreed upon and implemented across an agency if it wants to assure the currency of its BCM practices and procedures. The Tax Office tests its disaster recovery procedures on a regular basis in order to maintain the currency of its recovery procedures as changes are implemented across its information communication and technology (ICT) platforms. Desk top and scenario crisis exercises have been less frequent, however the Tax Office is aware of this and has advised it is addressing this as part of the move to a site based business continuity leadership model.

39. The majority of business continuity events, as recorded on the BCP database, related to facilities, specifically buildings. In the past few years, a range of natural disasters as well as power failures and flooding due to burst

water pipes has rendered all or part of at least one Tax Office building unusable each year. However with some 70 office locations across Australia the Tax Office has been able to transfer the operation of critical processes to other buildings or locations. This has created a multi-dimensional capacity to perform critical functions despite the loss of a site.

40. Tax Office senior managers and those staff with direct BCM responsibilities who were interviewed during the audit demonstrated a good knowledge of BCM practices and procedures. However, overall staff awareness and specific knowledge gaps could be further improved by implementing a computer based awareness raising campaign to ensure the knowledge is available easily and can be readily accessed by new staff in all locations.

41. In relation to disaster recovery the Tax Office has adopted a standard that ensures that its most important data is protected to a very high degree and is recoverable in any current realistic scenario. The Tax Office, through testing and in conjunction with its outsourced ICT provider, has developed a technical solution for its mid-range mainframe and data warehouse, which based on the information and documentation provided, meets the maximum acceptable outage for these services as set by their internal clients within the Tax Office.

Summary of agency response

42. The Tax Office welcomes this review and considers the report is supportive of our overall direction in improving the continuity of business in the ATO.

43. As noted in the body of this report the ATO is managing its business continuity responsibilities by taking a systematic approach and forging and maintaining key relationships across the organisation. A number of sections of corporate documents relating to business continuity in the ATO have been reproduced in the report, and their content and relevance is noted in a positive way, in paragraph [3.32 in the Audit Report], it is stated *“BCM process detailed within the Tax Office Business Continuity CMPS represents sound BCM practice.”*.

44. A number of the recommendations are quite specific to one area requiring some minor changes to procedures or documentation. In all cases these will be implemented as soon as practical and completed well before 30 June 2009.

45. A few of the recommendations refer to more integration of services within the ATO, and in particular Recommendation No. 1 recommends that *the ATO views business continuity management as an ongoing, integrated business 'program' to be implemented across the Tax Office.*

46. The ATO will explore a range of options to achieve this goal, and have engaged Booz and Company to work with us on this task to ensure we have a clear strategy for improvement. Particular focus will be given to the critical issues of integration of activities and regular reviews of our disaster recovery capabilities.

47. The ATO notes the constructive way in which this audit was conducted and looks forward to implementing the recommendations of the report.

Recommendations

Recommendation No. 1

Para 1.22

The ANAO recommends that the Tax Office, in order to improve the administration of business continuity management, view business continuity management as an ongoing, integrated business 'program' to be implemented across the Tax Office.

Tax Office Response: *Agreed: to be reviewed as part of the Booz consultancy.*

Recommendation No. 2

Para 3.19

The ANAO recommends that, in order to enhance the functioning of the Tax Office Emergency Control Organisation:

- a) in all emergencies, the Tax Office's Emergency Control Organisation, rather than the business continuity area, should remain responsible for the safety of people until an emergency situation has been resolved;
- b) verification of Emergency Control Organisation arrangements, as stated in the Corporate Management Practice Statement, should be included in the annual Compliance Certification process;
- c) all plans and procedures for emergencies, including tests and exercises as well as incidents and actual emergencies, be recorded on the business continuity planning database; and
- d) where possible and practicable, facilities management staff be actively encouraged and supported in accepting pivotal roles within the Emergency Control Organisation.

Tax Office Response: *Agreed*

**Recommendation
No. 3**

Para 3.29

The ANAO recommends that, in order to clarify the nature of business disruptions, the Tax Office provides clear guidance to staff on crisis declaration and cessation.

Tax Office Response: *Agreed*

**Recommendation
No. 4**

Para 3.39

The ANAO recommends that in accordance with better practice, the Commissioner (or person acting in that role) is not automatically assigned the crisis management leadership role.

Tax Office Response: *Agreed*

**Recommendation
No. 5**

Para 4.18

The ANAO recommends that in order to further improve the integration of disaster recovery with business continuity, the Tax Office monitor and report the current maximum acceptable outage levels to assist in identifying appropriate levels of IT resources that need to be allocated for disaster recovery.

Tax Office Response: *Agreed: to be reviewed as part of the Booz consultancy.*

**Recommendation
No. 6**

Para 4.52

The ANAO recommends that in order to improve business continuity capability and awareness:

- a) Business continuity management exercises are conducted at least annually for each major Tax Office site, and the results from such exercises be recorded in the business continuity planning database;
- b) the Tax Office examine the distribution of staff to business continuity management roles with a view to allocating specific resources to manage and maintain the business continuity plan database; and
- c) the Tax Office introduce short computer based training modules, appropriate to each staff level, reflecting the business continuity response that the Tax Office expects from those staff.

Tax Office Response: *Agreed*

Audit Findings and Conclusions

1. Background and Context

This chapter provides a description of business continuity management and an overview of the Tax Office's approach to implementing its business continuity strategy. It also provides information on the conduct of the audit.

Introduction to business continuity management

1.1 Government agencies deliver a wide range of programs and services which are critical to the economic and social well being of our society. Irrespective of the size or geographic location of agencies, single or multiple events may cause a significant disruption or outage to their 'business as usual' operations and compromise their ability to function which could have significant consequences for citizens, business and government.

1.2 Business continuity management (BCM) received international prominence in response to the potential Year 2000 (Y2K) computer problem. Y2K necessitated development of business continuity plans (BCP) by entities across the world to ensure they could continue to function despite disruptions caused by information and communication systems when the date changed at midnight on 31 December 1999. Fortunately the year 2000 arrived safely and most BCM scenarios did not have to be implemented.

1.3 Y2K, while attracting world-wide attention, is just one in a continuing series of events that demonstrates the need for organisations to continually identify and implement better practice BCM. For example, a UK based study ⁹ has estimated that 44 per cent of businesses affected by a fire fail to reopen, and notes that the 1993 World Trade Centre bombing resulted in 150 out of 350 affected businesses being closed. The events of September 11 2001 also established a challenge for BCM when private and public sector organisations faced total building destruction and yet were still expected to continue business activities.

1.4 BCM is an integral part of the organisational risk management framework within agencies which guides them in responding to unplanned disruptions or outages, variously described as an emergency, crisis and/or disaster, when normal management practices and procedures may be unable to cope. The primary objective of BCM is to respond effectively to disruptions

⁹ Business Continuity Planning – A safety net for businesses – Wanja Eric Naef – October 2003. <<http://www.iwar.org.uk/infocon/business-continuity-planning.htm>> [accessed 12 December 2008]

to ensure the uninterrupted availability of all key resources required to support essential (or critical) business activities and to return agencies to 'business as usual' within a predefined acceptable time limit (the maximum acceptable outage—MAO).

1.5 BCM should be individually tailored to the requirements of an agency by establishing a framework that allows normal business operations to recommence once an emergency, crisis or disaster has been effectively managed. A BCM framework is characterised by factors including:

- resilience being built within the organisation to provide an effective base to achieve objectives in the event of a disruption;
- planning and testing for disruption being embedded within the organisation to ensure continuation of program service delivery to agreed service levels; and
- a proven capacity to manage disruption while protecting reputation.¹⁰

The importance of business continuity management to the Tax Office

1.6 The Australian Taxation Office (Tax Office) is the main administrator of Australia's tax and superannuation systems. As at 30 June 2008 the Tax Office employed 23 303 ongoing and non-ongoing employees and occupied office space in some 70 buildings across Australia. During the year to 30 June 2008, the Tax Office processed more than 32.5 million income tax and Business Activity Statement lodgements, and responded to more than 12 million taxpayer enquiries, in collecting taxation and excise revenues of \$278.0 billion on behalf of the Government.¹¹

1.7 The Tax Office also plays a crucial role within the Australian economy by distributing transfers and payments of \$9.3 billion¹², and collecting \$44.4 billion¹³ in GST payments for state and territory governments.

1.8 The Tax Office is allocated significant resources of some \$2.8 billion to achieve its outcome of effectively managing and shaping Australia's self assessment taxation systems. A key contribution to the achievement of this

¹⁰ British Standard BS 25999-1:2006 *Business Continuity Management*, Part 1: Code of Practice, p. 6.

¹¹ Australian Taxation Office, *Commissioner of Taxation Annual Report 2007–08*, pp. 221.

¹² Australian Taxation Office, *Commissioner of Taxation Annual Report 2007–08*, pp. iv.

¹³ Australian Taxation Office, *Commissioner of Taxation Annual Report 2007–08*, p. 273.

outcome is the work that the Tax Office has undertaken to build taxpayer confidence in the system. A significant or long term interruption to business as usual within the Tax Office has the potential to disrupt or undermine revenue collections or affect its ability to respond to taxpayer enquiries on a timely basis. BCM is critical if the Tax Office is to meet Government expectations that revenue collection will continue to be managed despite disruptions to business as usual which will inevitably occur.

1.9 The benefits to the Tax Office of a comprehensive, clearly articulated and properly tested BCM framework include:

- the ability to proactively identify beforehand, possible events that may result in a disruption to business as usual;
- having proven practices and procedures that will minimise the impact of business disruptions;
- the ability to assess and risk manage uninsurable business processes; and
- enhancing the corporate governance structure, and through this, the organisation's reputation.

Business continuity management, risk management and business impact analysis

1.10 BCM is closely related to risk management.¹⁴ The risk management process is an integral input if an agency is to ensure its BCM framework works effectively. To maximise BCM effectiveness, agencies should first undertake a thorough business analysis so that key business processes are identified on an end-to-end basis. Upon completion of this mapping exercise to understand the key business processes, a risk assessment process should identify risks to each business process and then a Business Impact Analysis (BIA) will identify those business processes which are critical to an agency's continued operation.

1.11 The risk management process determines the known risks to the business, the likelihood of these risks, and the consequences should they arise. Flowing from this determination will be mitigation strategies aimed at eliminating the risk or reducing the impact should the risk occur.

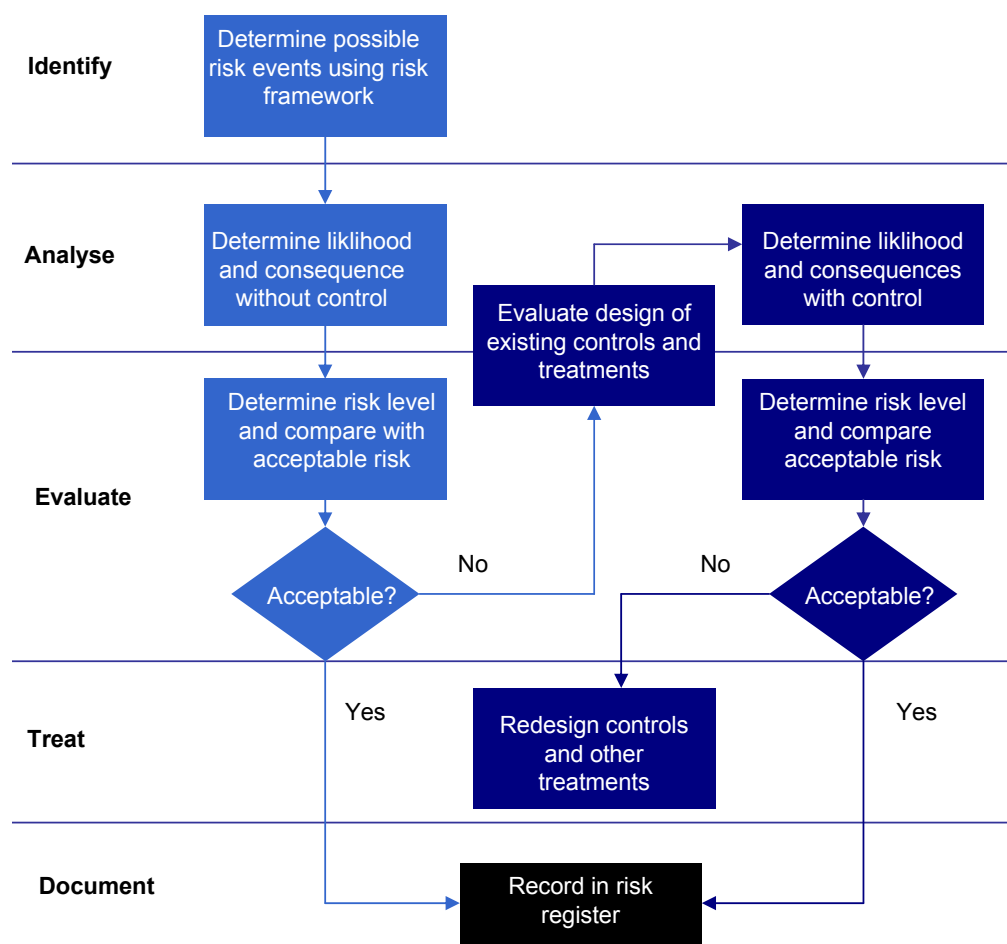
1.12 Some risks may be deemed to be acceptable to the organisation due to low consequence, a small likelihood of occurrence or because it would cost too

¹⁴ ANAO, *Better Practice Guide—Business Continuity Management*, January 2000, Canberra.

much to mitigate the risk. It is these untreated as well as unknown risks that business continuity management seeks to address.

1.13 The diagram at Figure 1.1 below is from the ANAO *Better Practice Guide—Business Continuity Management* and illustrates the risk management assessment process.

Figure 1.1
Risk management



Once risks have been identified, they are analysed in terms of their likelihood and consequences. The diagram illustrates a two-step approach which analyses risk before and after consideration of controls

Source: ANAO *Better Practice Guide—Business Continuity Management*, January 2000, Canberra p. 17.

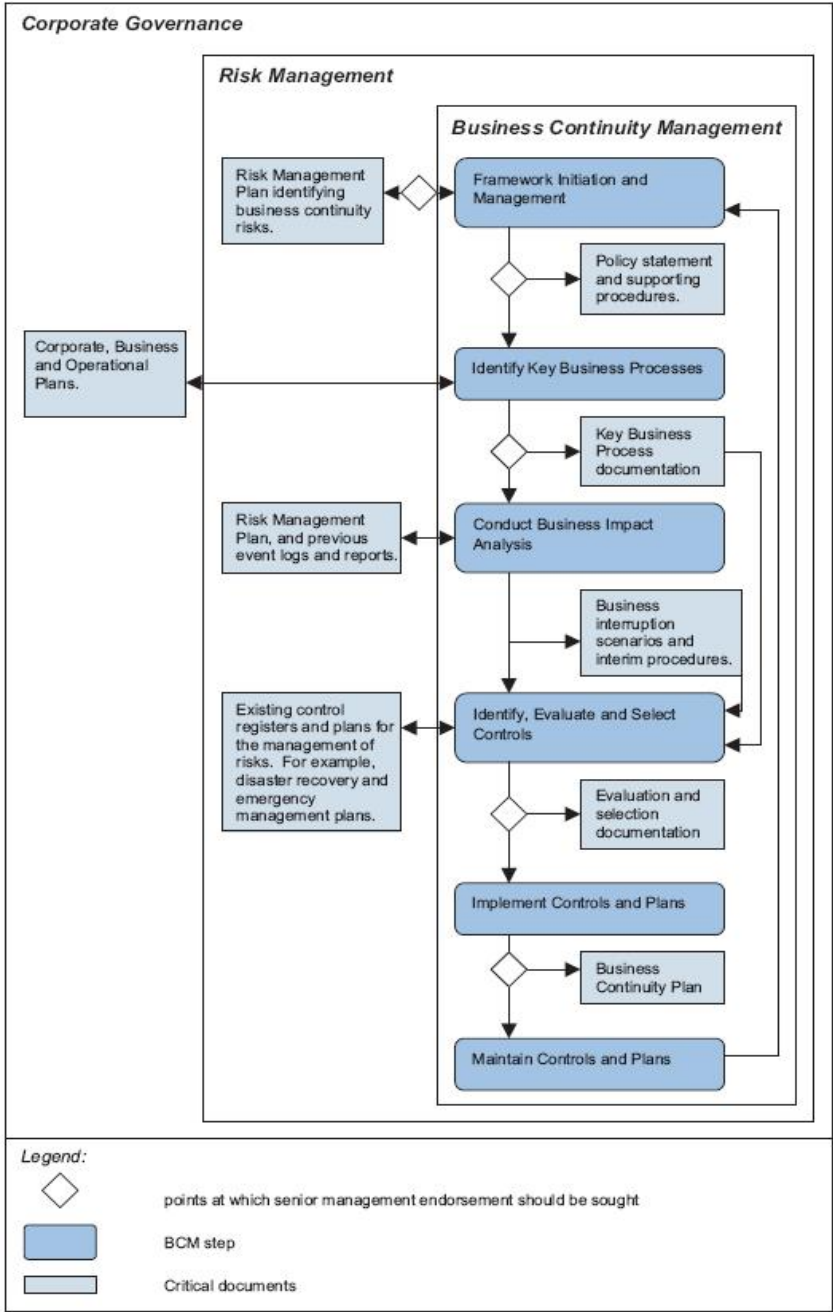
1.14 The risk management process will aim to identify all known risks to the organisation. These risks may affect any of the processes performed by the

organisation. Business continuity on the other hand deals only with the critical business processes of the organisation; those processes which, if they were to cease, would affect the functioning of the organisation. Consequently BCM strategies are developed around a crisis occurring rather than around specific events.

1.15 The diagram at Figure 1.2 (on page 30) illustrates the relationship between risk management and BCM.¹⁵

¹⁵ Note: The update to the ANAO, *Better Practice Guide—Business Continuity Management* may further refine the BCM process steps depicted in this diagram.

Figure 1.2
Business continuity management relationships



Source: ANAO Audit Report No. 53 2002–03 *Business Continuity Management - Follow-on Audit*, p. 27.

Business continuity strategy

1.16 Agencies have to ensure that, despite disruptions or outages to their business environment, they retain a capability to continue business operations at least at a minimum predefined level. The approach that an agency takes to ensuring business continuity should be clearly and concisely articulated in a business continuity strategy.

1.17 The Tax Office has a well developed BCM framework which is articulated in their Corporate Management Practice Statements (CMPS)¹⁶, and which is based around four key elements of business continuity management, represented in Figure 1.3, consisting of:

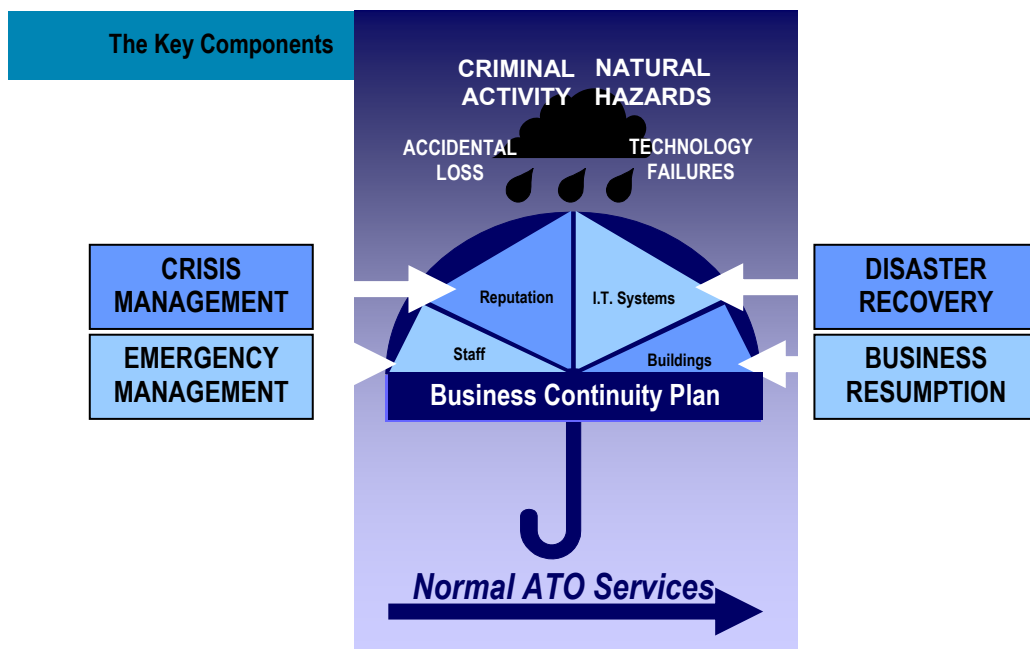
- emergency management ;
- crisis management;
- disaster recovery; and
- business resumption.

1.18 The Tax Office's BCM strategy has also been influenced by the size of its workforce and the necessity to decentralise its key operations across a number of locations throughout Australia. This matrix structure adopted by the Tax Office gives it a high degree of business resilience that has allowed it to effectively withstand business disruptions or outages. Most documented disruptions or outages in the 12 months to August 2008 arose from the total or partial loss of the use of buildings occupied by the Tax Office, rather than other disruptions, for example loss of IT systems capacity.

¹⁶ Tax Office, Corporate Management Practice Statement: *Business Continuity*, 2003/20 (Business Continuity CMPS); Tax Office, Corporate Management Practice Statement: *Emergency Control Organisation*, 2003/21 (Emergency Control Organisation CMPS); and, Tax Office, Corporate Management Practice Statement: *Risk and Issues Management*, 2003/02 (Risk and Issues Management CMPS).

Figure 1.3

Key components of business continuity management in the Tax Office



Source: Adapted from ATO Business Continuity Presentation 2008

Business continuity ‘program’ approach

1.19 The Tax Office has an overarching framework that it uses to implement BCM. However this framework does not address the program management aspects of implementing BCM across an organisation as large and geographically dispersed as the Tax Office. The British BCM standard¹⁷ proposes that BCM is an ongoing task and may best be managed as an integrated, ‘program’ of work at a whole of organisation level. At present the Tax Office separately completes a number of related BCM projects without having an integrated ‘program’ management structure that clearly articulates how the individual project components of BCM are organised, directed and implemented in a coordinated way.

1.20 The ANAO considers that, in line with such overseas BCM standards, the Tax Office could bring more efficient and effective management to its BCM by adopting a ‘program’ based better practice management framework. An integrated program structure would allow for stronger coordination of the

¹⁷ British Standard BS25999-1:2006, *Business Continuity Management*, Part 1: Code of Practice.

management of the individual BCM projects and activities within the Tax Office; and their success could be better monitored and reported to inform Tax Office management of the status of overall BCM preparedness. This could include mandatory reporting of all testing and exercises conducted as well as BCM incidents.

1.21 A program management framework would be beneficial as the Tax Office currently has to undertake a number of projects on a cyclical basis to ensure that its BCM is current and accurate. These projects include:

- identifying critical business process;
- verifying the reliability of enterprise risk analysis;
- conducting regular BIA;
- developing BCPs; and
- conducting testing and exercises.

Recommendation No.1

1.22 The ANAO recommends that the Tax Office, in order to improve the administration of business continuity management, view business continuity management as an ongoing, integrated business ‘program’ to be implemented across the Tax Office.

1.23 Tax Office Response: *Agreed: to be reviewed as part of Booz consultancy.*

1.24 Approaches to developing a program management framework that could guide the Tax Office include the United Kingdom’s Office of Government Commerce (OGC) publication,¹⁸ and the Department of Prime Minister and Cabinet (PMC) and ANAO *Better Practice Guide—Implementation of Programme and Policy Initiatives*¹⁹. The OGC’s framework proposes that a number of related projects be managed in a manner that gives improved control, especially of risk management factors, to senior management.

1.25 Tools such as OGC’s *Managing Successful Programmes*, and the PMC and ANAO *Better Practice Guide—Implementation of Programme and Policy Initiatives* are useful for improving the management of programs within organisations and therefore improving the overall corporate governance structure.

¹⁸ United Kingdom Government Office of Government Commerce, *Managing Successful Programmes*. 2007, London.

¹⁹ Department of Prime Minister and Cabinet and ANAO *Better Practice Guide—Implementation of Programme and Policy Initiatives*, October 2006, Canberra.

1.26 The Tax Office has advised that it intends to incorporate its BCM planning into the corporate planning cycle as soon as possible. The ANAO supports this initiative as it will lead to BCM being seen by Tax Office staff, including senior management, as an essential part of business planning, and not just as an adjunctive process that is activated only when an incident occurs.

Audit objective and scope

Audit objective

1.27 The objective of the audit was to assess the adequacy and effectiveness of the BCM practices and procedures within the Tax Office in preparing for, or responding to, disruptions to business as usual operations.

1.28 Particular emphasis was given to examining whether the Tax Office:

- has in place an appropriate framework for the administration of business continuity;
- adheres to BCM better practice principles for its plans, practices and procedures; and
- has appropriate mechanisms to test, evaluate, report and improve on its administration of business continuity.

Audit scope

1.29 The scope of the audit excluded an examination of the continuity planning for business processes between the Tax Office and external agencies such as the Reserve Bank of Australia and Centrelink.

1.30 Similarly the audit did not test the technical veracity of ICT disaster recovery plans as a component part of the Tax Office's BCM strategy due to their complex technical nature. Previous work undertaken by the Tax Office's Internal Audit Branch and the ANAO, as part of the review of IT controls, during its annual Financial Statement audit, has however shown this aspect to be reliable.

Audit methodology

1.31 The audit included interviews with Tax Office staff responsible for BCM and other areas impacting on implementation of the BCM framework including building facilities managers and Emergency Control Organisation (ECO) staff. The ANAO reviewed Tax Office files, databases and planning

documents. The ANAO also conducted meetings with other business continuity management topic specialists.

1.32 During the course of the audit the ANAO was able to observe actual crisis situations as well as a number of simulation tests and exercises.

1.33 The audit was undertaken in conformance with ANAO auditing standards and cost \$472 500.

2. Business Continuity: Better Practices and Benchmarks

This chapter discusses better practice benchmarks for business continuity management and assesses the Tax Office's implementation of its business continuity framework against key better practice benchmarks.

Overview

2.1 The principles and processes for developing and implementing BCM are well established. A number of Australian and international standards and publications are available to assist organisations in setting up their BCM frameworks and which can also be used to benchmark their implementation strategies. 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.²⁰ As previously mentioned the ANAO has also developed the *ANAO Better Practice Guide—Business Continuity Management*.²¹

2.2 Whilst there is no specific Australian standard for BCM²², there are a number of relevant standards and guides for BCM practitioners including:

- *Risk management* AS/NZS 4360:2004, providing a generic framework for establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk; and
- *Emergency control organization and procedures for buildings, structures and workplaces* AS 3745-2002 ,which deals with ensuring the safety of people. It covers authority and responsibility during an emergency, providing guidance on developing procedures for any organisation.

2.3 Standards Australia has also published the following handbooks on business continuity management practices:

- HB 221-2004-*Business Continuity Management Handbook*;
- HB 292-2006-*A practitioner's guide to BCM*; and

²⁰ For example, the joint publication by Business Continuity Institute and DRI International, *Professional Practices for Business Continuity Planners*, 1997.

²¹ *ANAO Better Practice Guide—Business Continuity Management*, January 2000, Canberra.

²² At the time of the audit both Australian and International Standards on BCM were being developed.

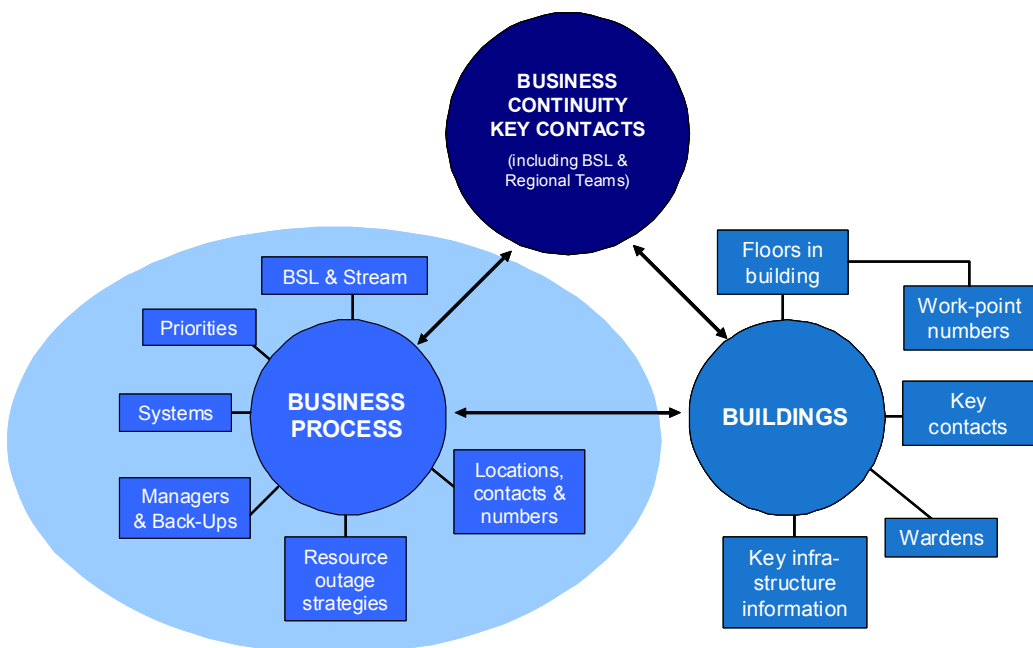
- HB 293–2006—*Executive guide to BCM*.

2.4 In the absence of an Australian Standard on BCM, the Tax Office has drawn upon better practice aspects contained in the British Standard on BCM, British Standard 25999 (BS 25999), to assist in the development of its business continuity framework.

2.5 Business continuity within the Tax Office covers emergency management, crisis management, disaster recovery and business resumption. Standards and guides are available which focus on these elements individually, while also incorporating linkages across various disciplines such as risk, harm and threat analysis as well as business continuity. The elements that are covered by business continuity within the Tax Office do not operate in isolation and it is unlikely that any business disruption or outage would stay within such predefined parameters. The diagram at Figure 2.1 below illustrates key links between business processes, business continuity contacts and buildings the Tax Office has used to construct a sound business continuity framework.

Figure 2.1

Tax Office key business continuity linkages



Source: Adapted from Tax Office, Business continuity presentation, 2008.

2.6 The Tax Office has also based its training and awareness packages around the integration of emergency management, crisis management, disaster recovery and business resumption.

2.7 In addition to the ANAO *Better Practice Guide—Business Continuity Management*, the ANAO has produced a number of audit reports which provide guidance to agencies in developing better practice BCM frameworks, including:

- ANAO Audit Report No.53 2002–03, *Business Continuity Management—Follow-up Audit*; and
- ANAO Audit Report No.9 2003–04, *Business Continuity Management and Emergency Management in Centrelink*.

2.8 These publications do not deal with BCM in isolation. The ANAO *Better Practice Guide—Business Continuity Management* and ANAO Audit Report No.53 2002–03, *Business Continuity Management—Follow-up Audit* stress the importance of risk management being undertaken comprehensively across an organisation and encourages agencies to assess and manage risk. The ANAO considers this linkage should be continually reinforced as BCM efforts will fail if based upon incorrect or outdated risk assessments.

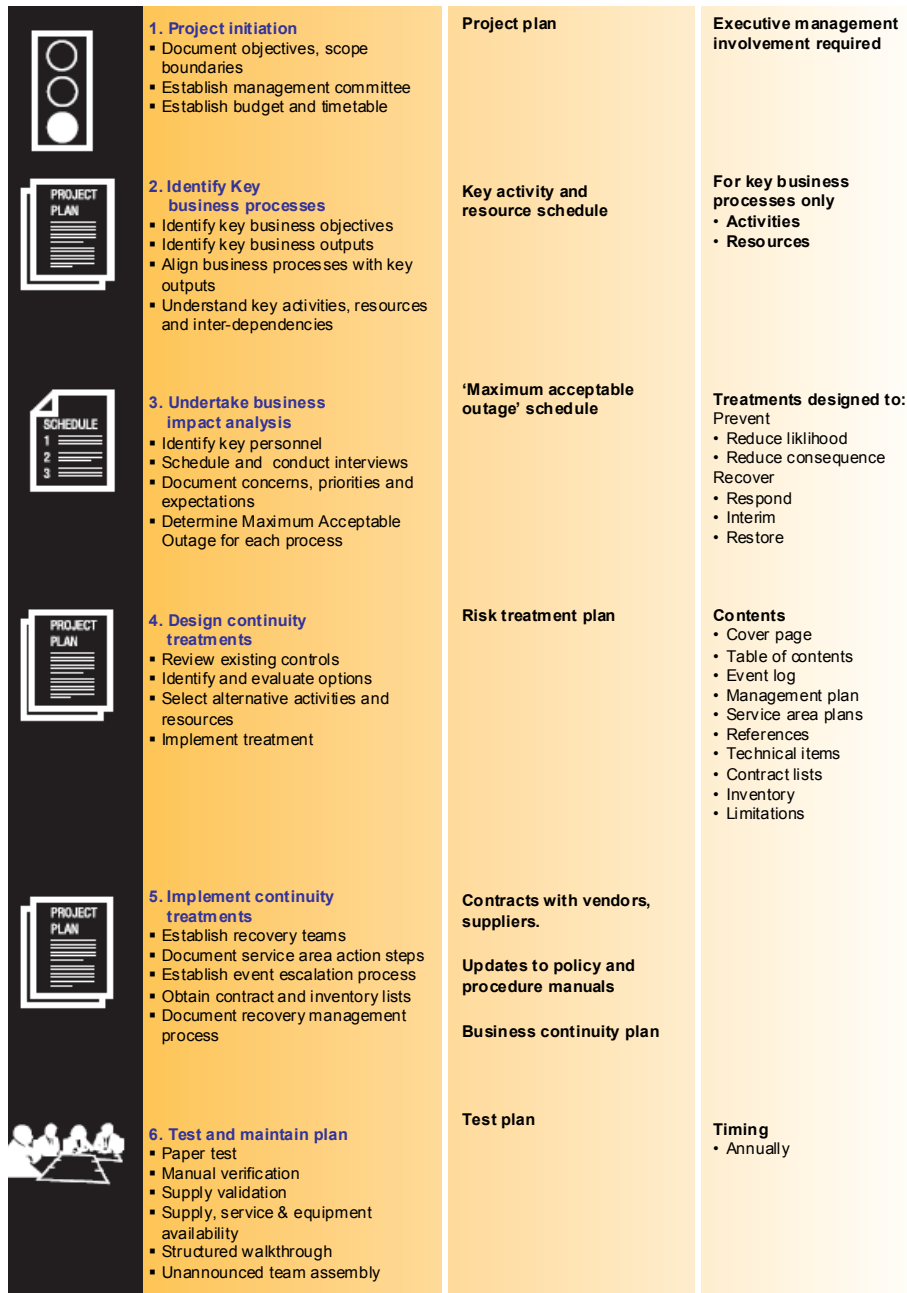
2.9 As evidenced by the various Tax Office CMPS and other documents, the Tax Office uses the ANAO *Better Practice Guide—Business Continuity Management* as a benchmark for its current BCM practices and procedures. This is demonstrated in the design and application of the Tax Office BCP database that uses the process illustrated in Figure 2.2 from ANAO *Better Practice Guide—Business Continuity Management*.

2.10 The audit of Centrelink referred to in Paragraph 2.7 highlighted the need for an organisation to effectively integrate and manage its risk management practices so they align with and complement work being undertaken within BCM. The ANAO considers that the Tax Office has applied sound BCM practices which were identified in that audit.

2.11 The Tax Office has a number of Practice Statements in relation to BCM, ECO and risk management. These policy documents are an important part of the Tax Office BCM framework and are analysed in more detail in Chapter 3—*Business Continuity Management Framework*. These statements provide policy advice as well as providing practical links to BCM, ECO and risk analysis tools and as such represent sound BCM documentation practices.

Figure 2.2

Framework for business continuity management depicted in the ANAO *Better Practice Guide—Business Continuity Management*



Source: ANAO *Better Practice Guide—Business Continuity Management*.

Note: The ANAO is in the process of updating this Better Practice Guide.

2.12 Reviewing the Tax Office's risk assessment practices and procedures as part of its BCM framework is outside the scope of this audit. However the approach taken by the Tax Office to BCM indicates that appropriate risk assessment practices have been followed across its business and service lines (BSL).

2.13 The ANAO noted that whilst the Tax Office had copies of a number of the BCM standards and other publications referred to earlier in this chapter, these were not readily accessible to staff with BCM responsibilities or staff more generally. The ANAO suggests that Tax Office consider including links within its ATONet, the Tax Office intranet, to standards, benchmarks and better practice documents in relation to BCM.

3. Business Continuity Management Framework

This chapter analyses and evaluates the Tax Office BCM framework and its associated practices and procedures.

Business continuity management in the Tax Office

3.1 The Tax Office's BCM framework, which has evolved over a number of years, in conjunction with its decentralised management operations, and its alternate BCM management structure which is activated in the event of a crisis situation, gives the agency a high degree of resilience.

3.2 The BCM framework is integrated into its business as usual operations and consists of four key elements that deal with continuity issues at different times and with different yet integrated strategies:

- emergency management (within its ECO) plans the Tax Office defines an emergency as 'a sudden state of danger, conflict, etc requiring immediate action'. It is expected that if action is taken immediately then the issue should be resolved quickly);²³
- crisis management (the initial response to a crisis);
- disaster recovery (the response to an information technology crisis); and
- business resumption planning (the response to business outage).

3.3 The BCM framework is supported by the various Tax Office CMPS. These documents guide Tax Office staff in the management of a business continuity event by stating who and in what circumstances a crisis or disaster may be declared. The business continuity framework then authorises designated Tax Officer staff, such as the National BCM Director and the Disaster Recovery Manager, to resolve the business disruption and return to normal services.

3.4 The Tax Office has developed individual CMPS that separate emergency management from crisis and disaster management. Emergency management is undertaken by wardens and communications officers, as part of the ECO, in consultation with government emergency services. If a crisis or

²³ Tax Office, Corporate Management Practice Statement, *Business Continuity*, 2003/20, p. 2.

disaster occurs simultaneously with an emergency situation remedial action will be managed by the business continuity team. It is possible that both groups could be managing an event with the ECO separating people from the original threat (or the threat from people) and business continuity team dealing with the longer term impacts of an outage.²⁴

3.5 Business continuity within the Tax Office ensures continuity of service by ‘taking necessary steps to identify the impact of potential losses; and developing viable mitigation strategies and recovery plans.’²⁵ This is achieved in the Tax Office through refining and developing BCP as well as testing plans and training staff.²⁶ Within the Tax Office, BCM focuses on keeping BSLs operating or returning them to operational status as quickly as possible after an outage.

3.6 When an emergency, crisis or disaster is declared the business continuity team and/or disaster recovery team has the responsibility to rectify the outage, including supporting BSLs in their recovery plans. The designated BCM director and Disaster Recovery manager have the delegated power to resolve the outage and return normal services.²⁷ The diagram at Figure 3.1 illustrates how the Tax Office views each phase separately, yet how each is considered interdependent of the other phases.

3.7 In order to assess Tax Office BCM practices and procedures it is necessary to consider the relevant CMPS. The key CMPS in relation to this audit are:

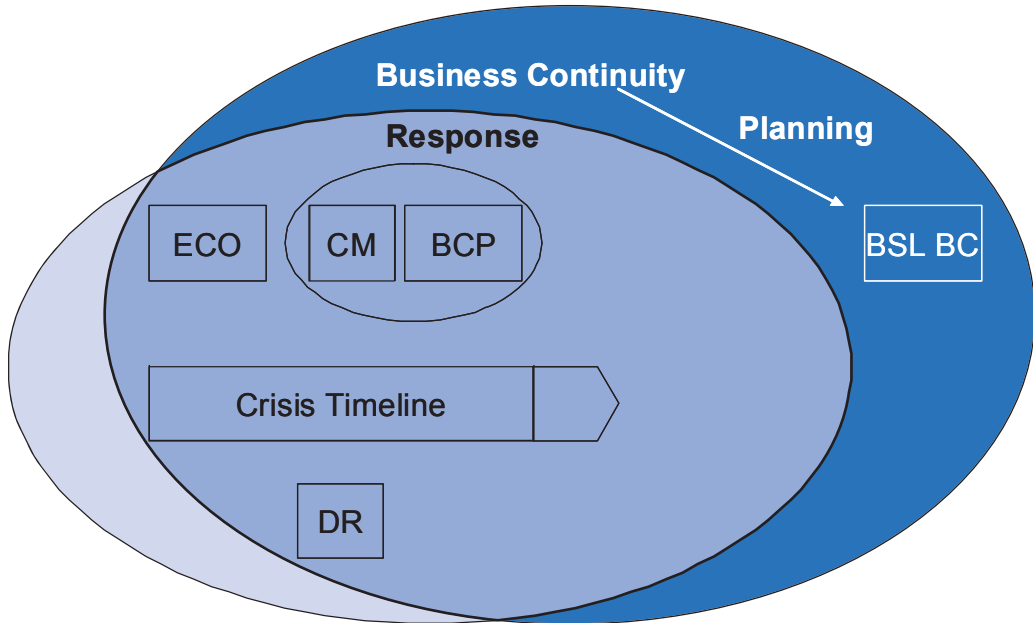
- Emergency Control Organisation CMPS;
- Risk and Issues Management CMPS; and
- Business Continuity CMPS.

²⁴ Tax Office, Corporate Management Practice Statement, *Business Continuity*, 2003/20, p. 4.

²⁵ *ibid.*, p. 1.

²⁶ *ibid.*

²⁷ *ibid.*, p. 2

Figure 3.1**Operation of the business continuity process**

Source: Adapted from Tax Office, Corporate Management Practice Statement, *Business Continuity Management* 2003/20, p. 3.

Corporate Management Practice Statement on emergency control organisation

3.8 ECO exists within the Tax Office to provide a framework to manage emergency situations in each Tax Office site and to work with BCM.²⁸ In managing an emergency within the Tax Office the ECO and the business continuity network work together as necessary, recognising which is managing the response to the emergency.²⁹ The Tax Office is guided by the Australian Standard AS3745-2002 in its approach to emergency management.³⁰ The Australian Standard defines an emergency as 'any event that arises internally

²⁸ Tax Office, Corporate Management Practice Statement, *Emergency Control Organisation*, 2003/21, p. 1.

²⁹ *ibid.*, p. 2.

³⁰ Standards Australia AS3745-2002 *Australian Standard emergency control organization procedures for buildings, structures and workplaces*.

or from external sources, which may adversely affect persons or the community generally.’³¹

3.9 The Emergency Control Organisation CMPS, while providing a link to BCM, could potentially lead to a situation in which staff with ECO duties are placed in the difficult position of assessing how immediate a threat is to a Tax Office site or to staff. An analysis of the BCP database shows instances where the ECO at a Tax Office site did not take action in relation to a threat to the site but deferred decisions to the National BCM Director. The safety of staff could be improved if such decisions were made locally so that they were more timely, and environmental factors can be more comprehensively assessed.

3.10 The Emergency Control Organisation CMPS requires that each Tax Office site sets up and maintains:

- emergency plans and procedures;
- an emergency planning committee (EPC); and
- an ECO.³²

Emergency Plans and Procedures

3.11 The Emergency Control Organisation CMPS mandates that:

The Tax Office will establish and maintain, for each building it occupies, appropriate plans to manage the response to all types of emergency situations which may affect the safety of people in a building or the community generally, and which require immediate response by the occupants.³³

3.12 At the time of the audit the Tax Office did not have in place emergency plans and procedures for each Tax Office site. This is due to range of factors such as transiting to a revised site structure from the previous regional BCM structure, through to moving of the national office into three new buildings. The ANAO acknowledges that the establishment and maintenance of emergency plans and procedures is a labour intensive process, especially in an environment where large numbers of staff are moving from one location to another. However, the importance of these plans is paramount to the safety of Tax Office staff and in ensuring that the Tax Office is well placed to manage business continuity issues.

³¹ Standards Australia AS3745-2002 *Australian Standard emergency control organization procedures for buildings, structures and workplaces*, p.6.

³² Tax Office, Corporate Management Practice Statement, *Emergency Control Organisation*, 2003/21, p. 1.

³³ *ibid.*

Emergency planning committee

3.13 The Emergency Control Organisation CMPS mandates the responsibilities of the EPC and its membership.³⁴ Because the EPCs produce practices and procedures documentation and arrange for testing of the procedures independently from the BCM framework the ANAO found that there were inconsistencies in the manner in which EPCs recorded tests, exercises and emergency incidents when compared to the BCM approach.

3.14 The ANAO sees considerable merit in using a systems based approach to managing and recording emergencies and considers the Tax Office EPCs could be better integrated into the business continuity framework if they use the BCP database to record plans and procedures for all incidents including tests, exercises and emergencies. This would provide a consolidated set of data that ECO, BCM and BSL could all use in determining Tax Office risk profiles and appropriate strategies for managing those risks. By more closely aligning emergency management to crisis management, staff safety could be better integrated into business disruption situations.

3.15 Similarly, Certificates of Assurance are provided to the Commissioner annually on business continuity, to verify BCM practices and procedures. There could also be value in the Tax Office extending the coverage of these Certificates to the ECO in order to further assist in the integration of staff safety within the business continuity framework.

3.16 The Emergency Control Organisation CMPS stipulates who should be on the EPC. While the Emergency Control Organisation CMPS nominates BSL representatives there may be merit in the Tax Office, where practicable, stipulating that nominated BSL representatives should be the BCM line representatives. This would build a level of knowledge, and promote consistency of reactions, for emergencies and business continuity issues.

Emergency control organisation

3.17 The varying size and situation of accommodation sites that the Tax Office occupies throughout Australia requires that each site has its own individual emergency plans, and therefore the ECO varies across the Tax Office. During the course of the audit a number of Tax Office sites were visited and Tax Office staff that perform ECO duties were interviewed. The ANAO found that the most knowledgeable staff in relation to ECO were from the

³⁴ Tax Office, Corporate Management Practice Statement, *Emergency Control Organisation*, 2003/21, p.2.

facilities management areas which reflected the nature of their work where these staff have an intimate knowledge of buildings, building contractors, emergency services and building owners.

3.18 The ANAO noted the Tax Office had decided for some sites, including the national office, that the facilities staff would not assume pivotal roles within ECO. The rationale for this decision was the need for facilities staff to provide advice to senior management on what was occurring at the emergency site. While there is some merit in this approach there are also advantages in having the staff that are most knowledgeable about a site involved in the management of an emergency. Facilities personnel are experienced in dealing with all aspects of the site and as such are more likely to be able to work seamlessly with building maintenance and emergency services. Further, as members of the ECO they will be able to inform senior management, as soon as possible, of the status of the emergency situation.

Recommendation No.2

3.19 The ANAO recommends that, in order to enhance the functioning of the Tax Office Emergency Control Organisation that:

- a) in all emergencies, the Tax Office's Emergency Control Organisation, rather than the business continuity area, should remain responsible for the safety of people until an emergency situation has been resolved;
- b) verification of Emergency Control Organisation arrangements, as stated in the Corporate Management Practice Statement, should be included in the annual Compliance Certification process;
- c) all plans and procedures for emergencies, including tests and exercises as well as incidents and actual emergencies be recorded on the business continuity planning database; and
- d) where possible and practicable, facilities management staff be actively encouraged and supported in accepting pivotal roles within the Emergency Control Organisation.

3.20 Tax Office Response: *Agreed.*

Corporate Management Practice Statement on risk and issues management

3.21 It is essential for any organisation to thoroughly understand and manage its risk environment if BCM practices and procedures are to be seen as

valid, and capable of restoring business after an outage. By undertaking risk management in accordance with the Australian Standard *Risk Management* AS/NZS 4360:2004, an organisation can better identify and manage risks to its operations.³⁵ Using this framework, risks can be managed in accordance with their priority and it is possible that some may even be effectively eliminated. However most risks will remain and a risk management plan will determine the resources needed to manage and mitigate these risks.

3.22 A review of the documentation supporting the Tax Office's approach to risk and issues management shows it to be consistent with better practice risk management as articulated in the ANAO Better Practice Guides and the Australian Standard *Risk management* AS/NZS 4360:2004. Within the Tax Office the guiding policy document is the Risk and Issues Management CMPS. The statement clearly articulates the Tax Office risk and issues management framework and links these concepts to the Tax Office compliance policy.³⁶ The document articulates how the Tax Office will identify, analyse, prioritise, treat and monitor risks and issues.³⁷ Specifically the Risk and Issues Management CMPS addresses:

- managing risk policy;
- corporate requirements;
- Tax Office risk management process; and
- roles and responsibility for accepting risk.³⁸

3.23 Testing of the Tax Office's implementation of the risk and issues management framework was outside of the scope of the audit.

Corporate Management Practice Statement on business continuity

3.24 The Tax Office Business Continuity CMPS, is consistent with the ANAO *Better Practice Guide—Business Continuity Management* in all key respects. The Business Continuity CMPS requires that the BCM framework establish and maintain:

- a business continuity network;

³⁵ Standards Australia AS4360-2004 *Australian Standard Risk Management*.

³⁶ Tax Office, Corporate Management Practice Statement, *Risk and Issues Management*, 2003/0 p.2.

³⁷ Tax Office, Corporate Management Practice Statement *Risk and Issues Management*, 2003/02.

³⁸ *ibid.*, p. 5.

- BCPs; and
- a regime to test the network plans.

3.25 The Business Continuity CMPS sets out the process where the management of an area affected by an outage is transferred from normal line management to the leader of the business continuity team. The roles and responsibilities of BSL, as well as specific decision makers are also articulated in the Business Continuity CMPS.³⁹

3.26 The Tax Office's use of BCM terminology is largely consistent with the ANAO *Better Practice Guide—Business Continuity Management* and standards such as BS 25999-1:2006. However the ANAO noted that in relation to IT issues surrounding disaster recovery a range of additional terms, such as 'incident' and 'problem', based upon the Information Technology Information Library (ITIL) are now being used freely within the BCM environment. The ANAO considers there may be benefit in the Tax Office revisiting its lexicon in relation to BCM and updating the precise definition and use of these terms.

Crisis situations within the Tax Office

3.27 A crisis situation requires an organisation to instigate an alternate management structure to deal with the situation and return the organisation to business as usual. Standards from the United Kingdom⁴⁰ and the United States⁴¹ document the alternate management structure. Specifically the United States standard NFPA 1600 states that 'the incident management system shall describe specific organizational roles, titles, and responsibilities for each incident management function.'⁴²

3.28 The Tax Office adheres to these standards in principle, through the establishment of business continuity teams. The Tax Office also has a good working definition of a crisis and has documented this in the Business Continuity CMPS,⁴³ however further improvement is possible by clearly articulating when a crisis begins and ends. The ANAO observed during the national office flooding in 2008 and the Northbridge 2008 simulation exercise

³⁹ Tax Office, Corporate Management Practice Statement: *Business Continuity*, 2003/20, p. 1.

⁴⁰ British Standard BS 25999-1:2006 *Business Continuity Management – Part 1: Code of Practice*, p. 26.

⁴¹ National Fire Protection Authority, *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2007 Edition*, Chapter 5.9.2.

⁴² *ibid.*, p. 10.

⁴³ Tax Office, Corporate Management Practice Statement, *Business Continuity*, 2003/20, p. 4.

that a crisis was not formally called but the crisis management structure was established and put into operation. This could have potentially created a conflict or confusion with there being no clear delineation of responsibilities between the business continuity team and business as usual line management. A crisis should be declared once it is determined that a business disruption will exceed the MAO.

Recommendation No.3

3.29 The ANAO recommends that, in order to clarify the nature of business disruptions, the Tax Office provides clear guidance to staff on crisis declaration and cessation.

3.30 Tax Office Response: *Agreed.*

Crisis situation case study - Flooding in national office

In March 2008 flooding, resulting in a major business disruption, occurred at the Tax Office's National Office affecting two of the three buildings in the Canberra Central Business District. The flooding was caused by a faulty seal in a fire hydrant and affected several floors, including the computer room.

A number of Tax Officers reacted quickly and, in conjunction with emergency services, determined that the building was safe. There was some initial confusion as to whether the incident should have been managed by site leadership or the National BCM Director. It was decided that the National BCM Director would manage the incident. The National BCM Director, who is based in Brisbane, was present in Canberra and coordinated the Tax Office response.

A number of crisis meetings were called and priority processes were allocated work space within the remaining national office sites (including redundant former national office accommodation). Most staff were sent home and told to call the 1800 emergency help line telephone number to be informed of updates.

It was quickly determined that the major issue was not accommodation as the Tax Office still had access to its old national office building and other premises. The Tax Office estimated that within 24 hours general IT requirements could be met for most staff. A priority issue related to ICT and the inability of the Tax Office to immediately replicate a development environment for some of its strategic IT programs.

The ANAO observed a 'crisis' was never formally declared nor were recovery time objectives for priority IT projects clearly articulated. Business continuity planning better practice would have seen the business resumption strategies for critical processes developed and able to be actioned in this type of crisis. The ANAO considers that given the circumstances the Tax Office managed the incident to a satisfactory conclusion.

3.31 Information from a crisis or disaster which affects the Tax Office such as that outlined in the case study above, is ultimately captured in the BCP database. This information is subsequently used to improve BCP, which is consistent with better practice.

3.32 The Business Continuity CMPS is cross referenced to the Emergency Control Organisation CMPS, and a clear differentiation between the two functions is articulated. Linking the ECO and BCM structures within the Tax

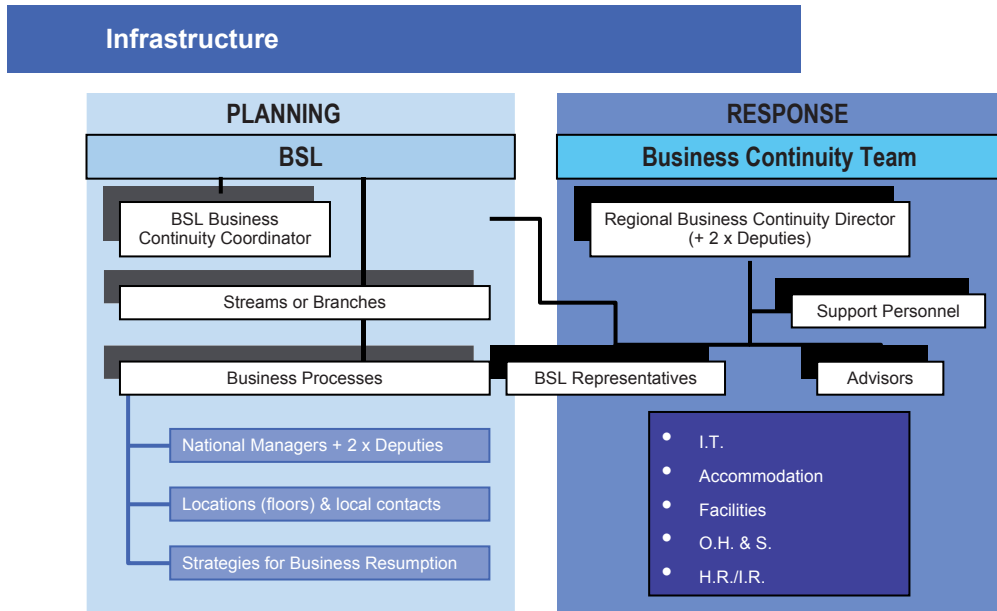
Office is indicative of better practice. More generally the ANAO considers that the documented BCM process detailed within the Tax Office Business Continuity CMPS represents sound BCM practice.

Roles and responsibilities

3.33 In dealing with a crisis or disaster the Tax Office has three designated teams responsible for business continuity, emergency control and disaster recovery respectively, that are staffed from BSLs. The National BCM Director coordinates across all three of these designated teams to ensure the seamless transition from one phase of a crisis to another.

3.34 However the National BCM Director coordinates most, but not all, aspects of the implementation of the business continuity framework. At present responsibility for the emergency management component of BCM rests with individual staff located within each Tax Office occupied building. These staff are part of the ECO within the Tax Office and are guided specifically by the Emergency Control Organisation CMPS constituted EPL for each major Tax Office site.

3.35 The Tax Office has divided business continuity into planning and response capabilities. BCM roles and responsibilities are clearly stated in the Business Continuity CMPS. The National Business Continuity Director advised the ANAO that where possible the same staff are involved in both the planning and response capabilities. The ANAO considers that the Tax Office approach to defining roles and responsibilities within the planning and response capabilities meets sound BCM practice benchmarks. Figure 3.3 details the component parts of the planning and response capabilities of the business continuity structure within the Tax Office.

Figure 3.2**Business continuity infrastructure within the Tax Office**

Source: Adaption of Tax Office Presentation 2008

3.36 Crisis management through to business resumption is clearly stated in the Business Continuity CMPS.⁴⁴ The Tax Office has a clear standard outlining by whom, and under what circumstances, a crisis can be called.⁴⁵

3.37 The ANAO noted that within the BCP database the Commissioner was allocated responsibilities as the national crisis manager. BCM better practice suggests that in most organisations the crisis manager should not be the Chief Executive Officer (CEO), but should report to the CEO. The rationale for this is that crisis managers need a high degree of competency in specific business continuity skills mastered through training and exercising which is often outside the direct experience of the CEO and that despite the depth and breadth of any crisis the CEO should continue to manage the organisation. This includes ensuring appropriate liaison with Government, other senior public sector agency managers, media and other stakeholders as required during the course of a BCM event.

⁴⁴ Tax Office, Corporate Management Practice Statement, *Business Continuity*, 2003/20, p. 7.

⁴⁵ *ibid.*, p. 8.

3.38 The CEO could however reserve the right to replace the crisis manager if necessary should a situation continue to deteriorate or not improve within pre-agreed timeframes.

Recommendation No.4

3.39 The ANAO recommends that in accordance with better practice, the Commissioner (or person acting in that role) is not automatically assigned the crisis management leadership role.

3.40 **Tax Office Response:** *Agreed.*

4. Implementing the Business Continuity Management Framework

This chapter reviews the Tax Office's planning and implementation of its BCM framework. It also reviews the approach taken by the Tax Office to test its BCP.

The Tax Office's approach to planning for business continuity management.

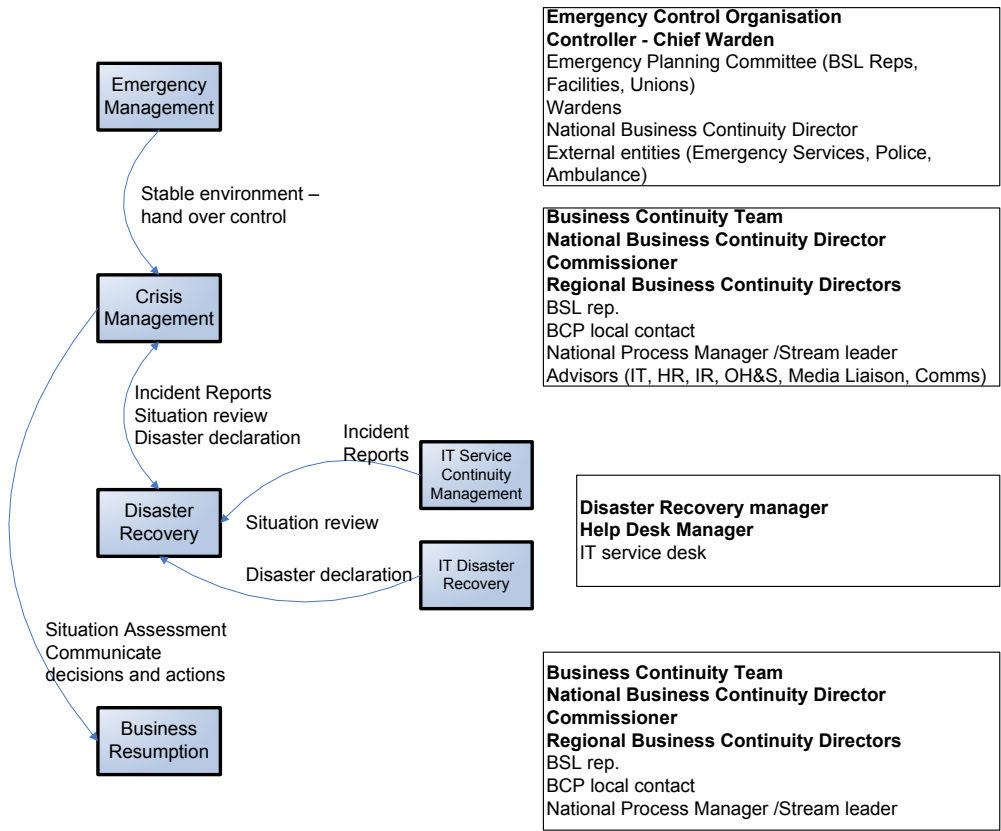
4.1 The Tax Office has built a business continuity framework based on accredited standards and benchmarks. It has adapted the underlying structure of better practice guides and standards to suite the Tax Office environment. In addition to these standards and benchmarks the Tax Office has constructed a database that is the central repository of information relating to BCM. The Tax Office has chosen to do this rather than creating a compilation of word processed documents based on templates such as provided in Standards Australia Handbook HB 221:2004 to hold all pertinent information relating to BCM.

4.2 The Tax Office BCP database, discussed in greater detail below, provides a level of structure and integration around information management that is not able to be achieved through the use of word processed documents. The information on the Tax Office BCP database primarily deals with BCP and resumption activities, but also holds emergency management and disaster recovery information.

4.3 Figure 4.1 provides a snapshot of the interactions, interdependencies and responsibilities that exist between the four key elements that the Tax Office has identified as being central to their business continuity strategic framework. These elements broadly fall into line with those publicised in standards and guides relating to business continuity.

Figure 4.1

Tax Office business continuity management framework elements



Source: ANAO analysis of Tax Office data.

Linking risk management and business continuity management

4.4 A comprehensive approach to developing a business continuity strategy also requires consideration of risk management and business analysis processes in identifying the potential sources of, and impacts from, disruptions to business as usual.

4.5 The link between business continuity and risk management can be summed up as follows:

An unanticipated or worst case event, regardless of its magnitude, has the potential to cause major disruption to an organisation....BCM provides the capability for an organisation to adequately plan for and manage these

business disruptions, as an important mitigation outcome of the risk management process.⁴⁶

4.6 The Tax Office has identified key risk assessment information and business processes to form part of the data used to produce its business impact analysis. This in turn has also assisted the Tax Office in building its BCP database.

4.7 The ANAO noted that business impact analysis undertaken by BSL did not make reference to risk assessments undertaken by the BSL as part of their normal risk management process. The corollary of this is that the lessons learnt from business continuity incidents, or testing exercises, are not systematically reported back for use in the risk assessment process. The method observed by the ANAO for updating risk related information is through informal liaison between the National BCM Director and the Chief Knowledge Officer.

4.8 Better practices and benchmarks in BCM identify risks and impacts through a process of categorisation to establish consistent criteria for developing mitigation strategies and priorities.⁴⁷ The Tax Office complies with these standards by analysing the following categories as part of its BCP:

- loss of key people;
- loss of power;
- loss of water;
- loss of IT;
- loss of communications;
- loss of access to building; and
- total loss of building.

4.9 The Tax Office BCP addresses the above categories through identifying a number of components. These components include:

- critical processes;
- critical people;
- recovery staff;
- alternate sites; and
- required resources.

⁴⁶ Standards Australia HB221-2004 *Handbook Business Continuity Management*, p. 7.

⁴⁷ ANAO *Better Practice Guide—Business Continuity Management*, January 2000, Canberra, Chapter 2.

4.10 Whilst the risk assessment undertaken to determine the impact of an outage on a particular process follows the approved Tax Office risk management framework,⁴⁸ the ANAO noted that the business impact analysis (BIA) process for BCM is not driven by the overall Tax Office risk management framework. Therefore when BSL undertake a risk assessment process they generate impact indicators that are allocated against each of their processes. This information is then stored on the BCP database.

4.11 Ideally each BSL would document their risk analysis profile and then use this as a principal input into the BIA for each of their processes. However, this is partially mitigated by the indicators held on the BCP database being presented annually to the Chief Knowledge Office and the risk management staff to ensure they fit within the Tax Office risk management framework.

Maximum acceptable outage

4.12 Standards and better practice guides identify a business impact analysis as the step necessary to determine the MAO for a process. MAO is defined as ‘the time it will take before an outage threatens an organisation achieving its business objectives’⁴⁹. To come to a determination of this time there are two methods, the first assesses over time the impacts of an outage, the second analyses the activities and resources affected by a full loss of the process. The later standards promote a time based approach which provides a level of granularity to the impact. This can be useful where the criticality of a process may become greater than others over time. The Tax Office meets this benchmark as each process within the BCP database has a stated MAO.

IT continuity management

4.13 Within the Tax Office most processes rely on IT systems to perform the activities related to that process. The unavailability of IT systems therefore impacts on the functioning of the Tax Office, potentially leading to a business continuity situation.

4.14 To help in planning and communication strategies the IT systems used by each business function are specified in the BCP database. A report is available detailing which BSLs are affected by an outage to any given IT system. During an outage of an affected IT system users are able to be

⁴⁸ Tax Office, Corporate Management Practice Statement, *Risk and Issues Management*, 2003/02.

⁴⁹ ANAO *Better Practice Guide—Business Continuity Management*, January 2000, Canberra.

identified and updated with the status of the outage and anticipated recovery times provided where available.

4.15 The Tax Office outsources its IT functionality to EDS. The contract with EDS incorporates a disaster recovery plan. The disaster recovery plan created states:

EDS will have the mainframe system ready for the ATO to perform their system and/or application validation within 24 hours....EDS will have all specified DSE environments ready for the ATO to perform their system and/or application validation within 4 hours.⁵⁰

4.16 Testing has been conducted on several occasions by EDS to measure their ability to meet these requirements. In the latest published test of 27 May 2007 the lag times of all platforms and recovery of the mainframe were acceptable, however the recovery times for the mid range and data warehouse platforms were well above the stated objective.

4.17 The ANAO noted that IT has a representative on the business continuity team and this facilitates an IT perspective on any business continuity event. The ANAO also observed effective communication between the National BCM Director and the Disaster Recovery Manager over several months during the course of the audit.

Recommendation No.5

4.18 The ANAO recommends that in order to further improve the integration of disaster recovery with business continuity, the Tax Office monitor and report the current maximum acceptable outage levels to assist in identifying appropriate levels of IT resources that need to be allocated for disaster recovery.

4.19 Tax Office Response: *Agreed: to be reviewed as part of Booz consultancy.*

Exercises to test business continuity management arrangements

4.20 The ANAO was present at two Tax Office business continuity exercises. The first was a desktop exercise involving the Chermside office BSL representatives.

⁵⁰ Tax Office, *Disaster Recovery Plan V3.2*, 26 September 2007 p. 18.

Testing case study 1 - Desktop exercise – Chermside Tax Office

The Tax Office planned and held a desktop exercise at its Chermside (Qld Region) Office in March 2008. The exercise involved the Chermside management group, including officers with BCM responsibilities.

The objective of the exercise was to increase the profile and awareness of BCM practices and procedures amongst the management group.

The exercise involved the group being walked through a scenario that involved an explosion at a neighbouring shopping centre. Staff were challenged to address issues in relation to emergency and crisis management. Many participants were surprised that the Tax Office could be required to work closely with emergency services even though Tax Office premises or staff may not be directly threatened.

The Chermside team engaged in vigorous debate and approached the exercise in a professional manner. The exercise achieved its objective of raising the general profile of BCM and individual awareness. The general consensus was that more frequent BCM exercises would improve management responses.

4.21 The second exercise at Northbridge involved a more complex simulation scenario over a longer time period.

Testing case study 2 - Partial simulation – Northbridge Tax Office

The Tax Office planned and held a partial BCM simulation at its Northbridge (WA Region) Office in May 2008. The exercise involved all elements of BCM as well as those officers with a business continuity role within the region. Selected staff from other sites were aware of the simulation as was the Tax Office executive.

The objective of the partial simulation exercise was to test staff at the Northbridge Office on their understanding of business continuity procedures.

The exercise principally involved bringing together the Northbridge business continuity team. This team exercised a real time scenario that involved Tax Office processes being threatened by a loss of staff due to multiple causes, such as a possible pandemic and sabotage.

The Northbridge team came together quickly and notified relevant Tax Office staff locally and nationally. The team effectively managed the situation they were presented with and approached the exercise in a professional manner.

4.22 As a result of the simulation nature of the exercise, Northbridge staff were exposed to more practical experiences and the skills required in relation to BCM than their Chermside counterparts. This highlights the difference in the types of exercises with a simulation providing a significant enhancement to staff skills and knowledge as opposed to a desktop exercise. The Tax Office advised that they would attempt to conduct simulation exercises every three months at a major site.

4.23 The Tax Office's Business Continuity CMPS does not explicitly set out a testing and exercise regime. Better practice dictates exercises and testing should be planned and conducted at least annually.⁵¹

⁵¹ British Continuity Institute *Good Practice Guidelines 2008 Part 5 Exercising, Maintaining & Reviewing BCM Arrangement*, p. 7.

4.24 There is currently no formal procedure for updating BCPs after an exercise or outage. There would be considerable benefit in putting in place a process to capture the results from exercises or outages into the BCP database. This could be in the form of an output of the review meeting held post event.

4.25 The National BCM Director manages business continuity disruptions and outages across the Tax Office on a real-time basis. This leaves little time to maintain the BCP database. In light of potential 'key-man' risks and the need for succession planning there may be advantages in extending the maintenance of the BCP database to other staff within the Tax Office BCM workspace to increase their BCM knowledge and skills.

Business continuity awareness

4.26 The senior Tax Office managers, and those staff with direct BCM responsibilities who were interviewed during the course of the audit demonstrated a good knowledge of BCM practices and procedures.

4.27 However, overall staff awareness and specific knowledge gaps could be further improved by implementing a computer based awareness raising campaign to ensure the knowledge is available easily and can be readily accessed by staff, especially new starters, in all locations.

4.28 This package could be placed on the ATONet and be updated annually so that all Tax officers would be aware of their role and functions in relation to BCM.

4.29 During ANAO's observation of both the actual crisis situation and simulation exercises there was confusion as to the role of some senior managers and to the technical meaning of words such as emergency, crisis and disaster. Consequently a number of other options could be considered by the Tax Office to improve general BCM awareness for senior managers including:

- Senior Executive Service (SES) to have BCM data loaded onto their note book computers to assist them and BCM staff during a BCM event;
- a hard copy information sheet out-lining senior management BCM responsibilities be produced and issued to senior managers and be kept in a BCM folder by each executive assistant;
- SES to be more involved in BCM exercises and some exercises should concentrate on SES management issues; and

- all SES, whether visiting or resident, should report to the Tax Office site manager in the event of a crisis, so that they can offer assistance appropriate to their position within the organisation.

Facilities management and disruptions

4.30 The majority of events creating crisis situations as recorded on the Tax Office BCP database involve facilities (buildings and equipment). This includes buildings being uninhabitable or unable to provide necessary services to allow the continued operation of the business.

4.31 The ANAO noted that not all incidents related to facilities are captured within the BCP database. These incidents are generally captured within the Tax Office occupational, health and safety system. The link to business continuity is made through a decision on whether or not to include the National BCM Director. There is a good working relationship existing with the current National BCM Director and facilities staff, resulting in early contact being made. This does not however, mean that the incident will be recorded in the BCP database nor will incidents be automatically reported to the future National BCM Director.

4.32 Capturing information from an incident involving facilities is at times delayed. This causes issues with correlating similar incidents, where delays in obtaining information can be as long as a week, resulting in multiple occurrences before the problem is rectified. There is currently no mechanism to correlate similar incidents to build up a profile of potential problems.

4.33 Similarly buildings may be inhabitable but not able to supply necessary services supporting activities performed in critical business processes. This may incorporate equipment failures and service outages such as computer networks, telecommunications and security systems that most processes within the Tax Office rely on to function.

4.34 The key standards and guidelines (HB 221, BS 25999, ANAO *Better Practice Guide—Business Continuity Management*, Business Continuity Institute Good Practices Guidelines 2008) all consider facilities as a critical resource requirement. In all cases where a building outage is going to exceed the organisation's recovery time objective, alternate facilities to operate out of, are crucial to the continued operations of critical business processes. With 70 locations and a business structure that allows most functions to be location independent, the Tax Office has created a matrix for performing business processes. In addition to this 'location independence', a business process may

be performed across multiple locations. Having a process performed at different locations reduces the impact if an event was to render a single facility unavailable. An example of this multi-dimensional aspect is the Parramatta office which despite being one of the largest offices, has only 6.1 per cent of the total workforce and contains many BSL. Within Parramatta the client contact BSL has 394 staff, however there are a further 768 staff located at Melbourne, Penrith and Brisbane who are able to perform the functions of client contact adequately.

4.35 This geographic spread and matrix structure generally provides the Tax Office with suitable internal alternative accommodation for scenarios in which a single building becomes unavailable. Canberra is the only key location in which multiple buildings are located within the same precinct. This could create issues in finding alternate accommodation for the number of people who work in this location. This environmental issue in Canberra is mitigated by the type of work performed in national office which tends to be policy related and not as operationally focused as other regions.

4.36 A mitigation strategy to reduce the need for alternative accommodation is the use of notebook computers with wireless network cards. The Tax Office has embarked on a program of notebook rollouts with 3G network cards, thereby allowing staff to work from anywhere. It is anticipated that locations which have high concentrations of staff in single buildings, such as Canberra, will have a high proportion of notebooks allocated to staff, reducing accommodation requirements.

Resources relevant to business continuity

4.37 The Tax Office has a national telephone number that staff can use to determine if they are affected by a business continuity event. This number is displayed on identification proximity cards provided to all employees and contractors who have access to Tax Office buildings. The use of the 1800 number was observed by the ANAO during the flooding incident of the Tax Office Canberra Gnabra Kembrey buildings. Information provided by the 1800 number informed staff when to return to work and where to gather. The ANAO observed that the majority of staff followed these instructions, gathering at 10:00 am the following day in the foyer of the Gnabra Kembrey building for a briefing by senior Tax Office management. Such an initiative is indicative of better practice in communicating the status of business continuity events to staff.

Business continuity planning database

4.38 As noted in paragraph 4.2 the Tax Office has built a valuable business continuity tool in the form of a BCP database. The creation and ongoing use of this database is a significant achievement in defining and operationalising business process resumption plans. The information on the BCP database provides a level of structure and integration around continuity issues that is not achievable through the use of standard templates and worksheets.

4.39 The BCP database is a tool that is designed to capture information on all aspects of BCM within the Tax Office. It has been developed to allow the storage of structured and unstructured data. Structured data provides a level of consistency by limiting the choice of responses in certain fields to choices that have been developed using acceptable standards. Unstructured data through free field entry allows context to be provided around responses which may have different answers for different environments. Unstructured data also caters for differences that BSL and locations may have.

4.40 The material held in the BCP database is used in the development of BCM activities such as business impact assessments, available to all Tax Office business continuity team members. It is also able to be viewed by all Tax Office staff through the BCP ATONet. The intranet site offers a wealth of information to all Tax Office staff, covering:

- what BCP is;
- why it is important; and
- how BCP will be enacted and roles and responsibilities.

4.41 ATONet also provides links to emergency management and practice management statements which provide the policy guidance for all staff to follow.

4.42 Email notification is incorporated into the business continuity strategy. The Tax Office has access to a tool from Telstra which allows it to incorporate data directly from the BCP database. This facilitates a quick and accurate means of notifying key stakeholders about the status of an incident and arranging meetings. A consequence of having this facility is that the BCP database must be kept up to date all the time.

4.43 It was observed by the ANAO during the 2008 Canberra flooding incident and the Northbridge exercise that contact data on the BCP database was out of date. The current monthly email to all process owners from the

National BCM Director is in alignment with better practice and standards, such as the BS 25999 on continuity management. The standard states that an outcome of the BCM maintenance process should include 'documented evidence of the proactive management and governance of the organisation's business continuity programme'.⁵² The email sent each month is indicative of proactive management, and governance is covered through system auditing which records the last review of the database, with any managers not reviewing their database frequently being identified and informed of their responsibilities.

4.44 Availability of this information in the case of a crisis does not rely solely on network access. The BCP database is copied each night to a stand alone version on the network which is replicated onto notebooks. This is backed up by the readiness kits which contain key pieces of information from the database. Should access to the BCP database be required during a crisis, access to ATONet may be made through 3G wireless network cards or home based broadband access.

Readiness kit

4.45 There are kits for business continuity directors and members of the business continuity team which contain information that can be useful in a crisis situation. These kits contain key items such as mobile phone and charger, regional team lists, crisis checklists, local and national contacts, outage strategies and escalation and communications strategies.

4.46 They are compiled into orange or green folders with the different colours being allocated for directors and team members. These folders are expected to be carried by the directors and team members in a crisis situation to assist their decision making processes and to improve communication. The team list and contact list contain information which would allow contact through multiple channels – phone and email.

4.47 In the April 2008 simulation exercise undertaken by the Tax Office at the Northbridge office, it was noted that a minority of team members brought their folders to the meetings that were called before and during the exercise. However during the exercise the ANAO did not observe the folders being utilised. This was despite the exchange of phone numbers regularly occurring, with these same numbers being available within the folders. If the folders had

⁵² British Standard BS 25999-1:2006 *Business Continuity Management*, Part 1: Code of Practice, p. 37.

been better utilised, team members would have been more aware of their responsibilities.

People

4.48 BCM has evolved from specialised areas surrounding technology and disasters where infrastructure was the primary concern. The emphasis has now turned to people, as processes cannot run without input, decision making and direction of output, much of which requires human intervention. The roles of people in the Tax Office in crises can be categorised into the following:

- critical people;
- crisis management team (business continuity team);
- executive management (national process managers); and
- other staff.

4.49 These roles are separate from other business continuity roles that deal with planning and management.

4.50 Critical people can be identified as those who are required to make critical processes work. Activities performed by people who are necessary to make critical processes continue to function may include: capturing and disseminating information, communicating with external stakeholders and analysing information to make informed decisions. The identification of who is critical is ideally determined prior to any crisis situation when objective decisions are able to be made without the constrained pressures present in a crisis situation.

4.51 The Tax Office has a business continuity team in place for each significant office site location. At the time of the audit the makeup of this team was going through changes with the introduction of site leadership, as opposed to regional leadership, within each location. In future the business continuity team will be the site leadership team. Currently there are issues with site leaders becoming involved in crises but not having any mandated background in business continuity.

Recommendation No.6

4.52 The ANAO recommends that in order to improve business continuity capability and awareness:

- a) Business continuity management exercises are conducted at least annually for each major Tax Office site, and the results from such exercises be recorded in the business continuity planning database;
- b) the Tax Office examine the distribution of staff to business continuity management roles with a view to allocating specific resources to manage and maintain the business continuity plan database; and
- c) the Tax Office introduce short computer based training modules, appropriate to each staff level, reflecting the business continuity response that the Tax Office expects from those staff.

4.53 Tax Office Response: *Agreed.*

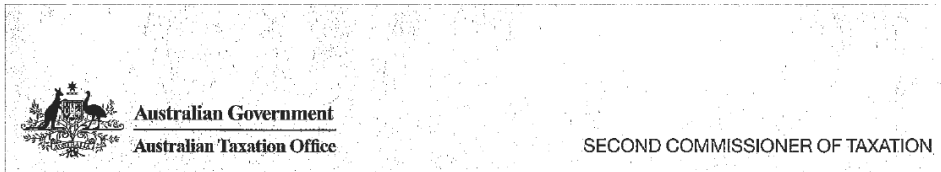


Ian McPhee
Auditor-General

Canberra ACT
22 December 2008

Appendices

Appendix 1: Agency Response



Mr David Crossley
ANAO Performance Audit Executive Director
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Mr Crossley *David*

**AUSTRALIAN NATIONAL AUDIT OFFICE PERFORMANCE AUDIT OF
AUSTRALIAN TAXATION OFFICE - ADMINISTRATION OF BUSINESS
CONTINUITY MANAGEMENT**

Thank you for your letter dated 6 November 2008 and for the opportunity to provide comments on the proposed report on the Australian Taxation Office - Administration of Business Continuity Management.

We welcome this review and consider that the report is supportive of our overall direction in improving the continuity of business in the ATO.

As noted in the body of this report the ATO is managing its business continuity responsibilities by taking a systemic approach and forging and maintaining key relationships across the organisation. We note your comment at paragraph 3.30 that "BCM process detailed within the Tax Office Business Continuity CMPS represents sound BCM practice."

The ATO accepts all six recommendations as presented in the section 19 report. We have also engaged Booz and Company to further review our Business Continuity Framework with a particular view to addressing issues around the integration of activities.

I would like to thank the Australian National Audit Office audit team for the cooperative and professional manner they have adopted in working with us on this matter. I look forward to continuing the good working relationship developed in this performance audit.

Attached is the ATO's response to the recommendations (Annexure 1) and summary of our comments to be used in the report brochure (Annexure 2).

If you require further information on this matter, please contact Brett Jeppesen, National Director Business Continuity on 07 321 35107.

Yours sincerely

Bruce Quigley
Second Commissioner
5 December 2008

Cc ANAO auditors

PO BOX 900 CIVIC SQUARE ACT 2608 AUSTRALIA
ADDRESS

+61 (0)2 6216 1111
TELEPHONE

+61 (0)2 6216 2743
FACSIMILE

Appendix 2: Glossary of terms used in relation to this Audit Report⁵³

Alternate site	A location that is available to an organisation in a crisis situation to perform critical processes disrupted by the crisis.
British Standard—Business continuity management 25999 (BS 25999)	BS 25999 BCM holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capacity for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
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.

⁵³ Given the International focus of BCM a variety of terms are used to describe the same concepts. Whilst a number of terms have become interchangeable in recent years, the terms used in this audit are those generally adopted within the Tax Office at the time of this audit.

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	An actual or virtual centre that allows effective Centre coordination and direction of a response to a crisis or incident.
Crisis management	The process used to escalate, manage, resolve and communicate issues related to a crisis.
Crisis response	The use of procedures to ensure that immediate actions are taken and issues escalated appropriately to the crisis leadership.
Critical Infrastructure	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.
Critical people	The staff belonging to an organisation who perform activities that directly relate to processes deemed to be critical processes
Critical processes	The activities performed by the organisation which are the most time sensitive to the achievement of business objectives. These are not necessarily the most important activities but by virtue of their time constraints have priority in being restored.

Disaster Recovery	Primarily relating to information technology (IT), the disaster recovery plan is the result of the recovery time objective. It details the procedures necessary to provide IT support should an incident result in the disruption to normal IT services.
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.
Exercise (testing)	Exercises are activities undertaken to properly assess the effectiveness of a business continuity or emergency management plan. These can take the form of a desktop walkthrough, a simulation and a functional exercise.
Incident (event)	An incident in business continuity terms is any activity which occurs that disrupts normal business processes, it can also be called an event.
Interim processing	Interim processing or contingency measures enable business processes to continue, prior to the restoration and resumption of primary/normal business processes.
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.

Index

A

Alternate site, 70

B

British Standard— Business continuity management, 15, 26, 32, 37, 48, 60, 63, 70

Business continuity plan, 7, 14, 15, 16, 17, 18, 25, 38, 42, 44, 45, 49, 51, 53, 55, 56, 59, 60, 62, 63, 70

Business disruption, 7, 70, 72

Business impact analysis, 7, 27, 33, 56, 70

C

Corporate Management Practice Statement, 5, 7, 13, 15, 16, 17, 19, 21, 31, 38, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 56, 58

Crisis command, 71

Crisis management, 48, 49, 51, 71

Crisis response, 71

Critical Infrastructure, 71

Critical people, 64, 71

Critical processes, 71

E

Emergency management, 41, 72

Event log, 72

Exercise, 72

I

Interim processing, 72

M

Maximum acceptable outage, 5, 7, 11, 26, 49, 56, 71, 72

R

Recovery director, 72

Resumption planning, 73

Risk event, 73

Risk management, 6, 28, 36, 47, 73

Risk treatment, 73

Series Titles

ANAO Audit Report No.1 2008–09

Employment and Management of Locally Engaged Staff

Department of Foreign Affairs and Trade

ANAO Audit Report No.2 2008–09

Tourism Australia

ANAO Audit Report No.3 2008–09

Establishment and Management of the Communications Fund

Department of Broadband, Communications and the Digital Economy

Department of Finance and Deregulation

ANAO Audit Report No.4 2008–09

The Business Partnership Agreement between the Department of Education,

Employment and Workplace Relations (DEEWR) and Centrelink

Department of Education, Employment and Workplace Relations

Centrelink

ANAO Audit Report No.5 2008–09

The Senate Order for Departmental and Agency Contracts (Calendar Year 2007

Compliance)

ANAO Audit Report No.6 2008–09

Illegal, Unreported and Unregulated Fishing in the Southern Ocean

Australian Customs Service

ANAO Audit Report No.7 2008–09

Centrelink's Tip-off System

Centrelink

ANAO Audit Report No.8 2008–09

National Marine Unit

Australian Customs Service

ANAO Report No.9 2008–09

Defence Materiel Organisation—Major Projects Report 2007–08

ANAO Audit Report No.10 2008–09

Administration of the Textile, Clothing and Footwear Post-2005 (SIP) Scheme

Department of Innovation, Industry, Science and Research

ANAO Audit Report No.11 2008–09

Disability Employment Services

Department of Families, Housing, Community Services and Indigenous Affairs

Department of Education, Employment and Workplace Relations

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

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

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

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

Current Better Practice Guides

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

Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006
Legal Services Arrangements in Australian Government Agencies	Aug 2006
Preparation of Financial Statements by Public Sector Entities	Apr 2006
Administration of Fringe Benefits Tax	Feb 2006
User-Friendly Forms	
Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006
Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
Better Practice in Annual Performance Reporting	Apr 2004
Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002

Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Commonwealth Agency Energy Management	June 1999
Security and Control for SAP R/3	Oct 1998
Controlling Performance and Outcomes	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997