

Business Continuity Management

Civil Aviation Safety Authority

Department of Finance

Department of Social Services

© Commonwealth of Australia 2014

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 0 642 81516 X (Print)

ISBN 0 642 81517 8 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit

<http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <http://www.itsanhonour.gov.au/>.

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

Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:

publications@anao.gov.au.





Canberra ACT
6 November 2014

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit across entities titled *Business Continuity Management*. The audit was conducted 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 to the Parliament.

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

Yours sincerely

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

Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

Phone: (02) 6203 7505

Fax: (02) 6203 7519

Email: publications@anao.gov.au

ANAO audit reports and information about the ANAO are available on our website:

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

Audit Team

Tracey Martin
Alison Palmer
Evan Moraitis
Edel Kairouz

Contents

Abbreviations.....	8
Glossary	10
Summary and Recommendations	13
Summary	15
Introduction	15
Audit objective, criteria and scope	18
Overall conclusion.....	19
Key findings by chapter.....	22
Summary of entities' responses.....	24
Recommendations	26
Audit Findings	27
1. Introduction	29
Business continuity management in the Australian Government	29
Audit objective, criteria and scope	35
Report structure	37
2. Business Continuity Management	38
Introduction	38
Disruption related risk	38
Business continuity management framework	39
Business continuity management responsibilities	48
Managing business continuity arrangements	50
Conclusion	51
3. Assessing and Planning for Business Continuity Needs	53
Introduction	53
Business impact analysis.....	54
Business continuity planning.....	68
Summary results for assessing and planning for business continuity management.....	72
Conclusion	73
4. Responding to Disruptions	74
Introduction	74
Activating business continuity plans	74
Post incident review	80
Conclusion	85

5. Monitoring and Review.....	87
Introduction	87
Business continuity exercising and testing	87
Monitoring overall preparedness.....	94
Conclusion	97
Appendices	99
Appendix 1: Entities' Responses	101
Appendix 2: Civil Aviation Safety Authority's Key Systems and Facilities.....	107
Appendix 3: Department of Finance's Critical Functions.....	108
Appendix 4: Department of Social Services' Critical Functions with a Major or Extreme Impact Rating	109
Index.....	114
Series Titles.....	115
Better Practice Guides	116

Tables

Table S.1: Protective Security Policy Framework—key mandatory requirements relating to business continuity management	16
Table 1.1: Protective Security Policy Framework—key mandatory requirements relating to business continuity management	31
Table 1.2: Business continuity management expectations—Protective Security Policy Framework components	32
Table 1.3: Report structure	37
Table 2.1: Example of Finance's business continuity disruption risks	39
Table 2.2: Civil Aviation Safety Authority's Business Continuity Management Framework.....	40
Table 2.3: Hierarchy of plans.....	44
Table 2.4: Entities' business continuity guidance and templates	44
Table 2.5: Purpose/objective of entity business continuity management arrangements	46
Table 2.6: Department of Social Services' Mission Critical Activities.....	47
Table 3.1: Entity approaches to business impact analysis and definition of critical functions	56
Table 3.2: Example of Finance internal and external dependencies and vital records	63
Table 3.3: Case study—Department of Social Services' response to Queensland floods—stakeholder contact.....	65
Table 3.4: Example of Department of Social Services' recovery targets for critical functions	68
Table 3.5: Finance's recovery kits	71

Table 3.6:	Department of Social Services' response and recovery strategy for making payments	72
Table 3.7:	Entity business continuity management processes	72
Table 4.1:	Activation point for business continuity management arrangements	75
Table 4.2:	Case study—Department of Social Services' response to Cyclone Oswald.....	80
Table 4.3:	Case study—Civil Aviation Safety Authority's response to the Queensland floods and Cyclone Yasi	81
Table 4.4:	Case study—Finance post incident review	82
Table 4.5:	Case study—Department of Social Services' post incident review of Queensland floods	84
Table 5.1:	Case study—Finance's Exercise Sparky	91
Table 5.2:	Case study—Department of Social Services' exercise Iron Triangle IV	92
Table 5.3:	Civil Aviation Safety Authority's performance measures.....	95

Figures

Figure 2.1:	Overview of Finance's Business Continuity Management Framework.....	42
Figure 2.2:	Business continuity management structures and key responsibilities	49
Figure 3.1:	Business function risk assessment—Civil Aviation Safety Authority's guidance	58
Figure 3.2:	Example of completed risk assessment including the Civil Aviation Safety Authority's guidance	58
Figure 5.1:	Finance's Exercise Management Process	90

Abbreviations

ANAO	Australian National Audit Office
AS/NZS 5050:2010	Australian Standard/New Zealand Standard 5050:2010 <i>Business Continuity—Managing disruption-related risk</i>
BCM	business continuity management
BCP	business continuity plan
BIA	business impact analysis
BPG	better practice guide
CASA	Civil Aviation Safety Authority
DSS	Department of Social Services
Finance	Department of Finance
HB 221–2004	Standards Australia, Handbook 221–2004, <i>Business Continuity Management Handbook</i>
HB 292–2006	Standards Australia, Handbook 292–2006, <i>A practitioner’s guide to business continuity management</i>
HB 293–2006	Standards Australia, Handbook 293–2006, <i>Executive guide to business continuity management</i>
ICT DRP	Information and Communications Technology Disaster Recovery Plan
ISO 22301:2012	International Organization for Standardization 22301:2012 <i>Societal security—Business continuity management systems—Requirements</i>
ISO 22313:2012	International Organization for Standardization 22313:2012 <i>Societal security—Business continuity management systems—Guidance</i>

ISO/IEC 27001:2013	International Organization for Standardization/International Electrotechnical Commission 27001:2013 <i>Information technology—Security techniques—Information security management systems—Requirements</i>
AS ISO 15489:2001	Australian Standard International Organization for Standardization 15489:2001 <i>Information and documentation—Records Management</i>
PSPF	Protective Security Policy Framework

Glossary

Activation	The act of declaring that an entity's business continuity arrangements need to be put into effect in order to continue the delivery of key products and services.
Business continuity	The capability of an entity to continue to deliver products or services at acceptable predefined levels following a business disruption event.
Business continuity management	The development, implementation and maintenance of policies, frameworks and programs, to assist an entity manage a business disruption, as well as build entity resilience.
Business continuity plan	Documented procedures that guide an entity to respond, recover, resume, and restore to a pre-defined level of operation following a business disruption event.
Business impact analysis	The process of analysing functions, activities, and processes—that deliver product and services—and the effect that a disruption might have upon them.
Control Team	The central point of communication, coordination and decision making during a disruption.
Critical function or activity	A function or activity to which priority must be given following an incident, in order to mitigate impacts on an entity's key products and services which support the achievement of key business objectives.
Disaster recovery planning	The operational response associated with the recovery of computer systems and associated infrastructure following a disruption to services. It may also encompass other technical facilities such as telephone and mobile services.

Enabling resources or services	The resources supporting priority functions, also known as enabling assets and services. These can include information and communication technology (ICT), property, security and human resources.
Event	Occurrence or change of particular set of circumstances.
Incident	Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
Recovery target	The period of time within which a product or service, function or activity, or resources must be resumed or recovered.

Summary and Recommendations

Summary

Introduction

1. Many services delivered by public sector entities are essential to the economic and social well-being of society—a failure to deliver these could have significant consequences for those concerned and for the nation. Other services may not be essential, but a disruption can nonetheless result in inconvenience and inefficiency, and have economic costs.
2. Government entities face a range of situations—including equipment failure, natural disaster, and criminal activity—that may lead to a significant business disruption. In response to such business disruption, entities need to have arrangements in place to support the continuation and/or resumption of essential services and ultimately return to business as usual. Often these arrangements will need to operate alongside emergency or disaster management arrangements to ensure the safety of staff and assets.
3. Business continuity management (BCM) is the development, implementation and maintenance of policies, frameworks and programs, to assist an entity manage a business disruption, as well as build entity resilience.¹ As such, BCM is an important element of good governance. BCM forms part of an entity’s overall approach to effective risk management, and can provide a capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a disruptive event.
4. To appropriately focus an entity’s business continuity arrangements, it is important to have a clear and agreed understanding of the entity’s business objectives and the critical business functions or activities which help to achieve those objectives. The business continuity arrangements should also identify the resources supporting these priority functions. These resources are known as enabling assets and services, and include information and communication technology (ICT), property and security, and human resources.

1 Resilience comes from addressing the likelihood as well as the consequence of disruptive events. Therefore it is important to have both effective risk management and business continuity management frameworks in place. Resilience allows the entity to anticipate disruptive events, constantly adapt to change, and to survive and bounce back from disruptions.

Policy requirements and better practice

5. Business continuity management in Australian Government entities is governed by the Protective Security Policy Framework (PSPF), which requires entities to use a risk management approach to cover all areas of protective security activity. The PSPF applied to all former *Financial Management and Accountability Act 1997* (FMA Act) agencies, and to those former *Commonwealth Authorities and Companies Act 1997* (CAC Act) bodies that have received a Ministerial Direction. This arrangement is currently being revised as part of the introduction of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), from 1 July 2014.²

6. For entities subject to the PSPF, the key mandatory requirements relating to BCM are GOV 11 and PHYSEC 7 (see Table S.1, below). The ANAO completed an audit in 2013–14 of the *Management of Physical Security*³ which included a focus on the implementation of PHYSEC 7 in three entities. This audit focuses on the GOV 11 requirement.

Table S.1: Protective Security Policy Framework—key mandatory requirements relating to business continuity management

Mandatory Requirement	Detail
GOV 11	Agencies must establish a business continuity management program to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a threat and risk assessment.
PHYSEC 7	Agencies must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian Government may direct its agencies to implement heightened security levels.

Source: PSPF, June 2013, pp. 18 and 34.

7. Protocols, standards and guidelines have been developed to support the mandatory requirements in the PSPF. In relation to GOV 11, this includes

2 The PGPA Act effectively replaced the FMA Act and the CAC Act from 1 July 2014. The PGPA Act introduced two broad categories of Australian Government bodies (Commonwealth entities and Commonwealth companies). Under Section 21 of the PGPA Act, non-corporate Commonwealth entities are required to comply with the policies of the Australian Government, including the PSPF. On the other hand, Australian Government policies, including the PSPF, do not apply to corporate Commonwealth entities and Commonwealth companies unless the Finance Minister issues, under sections 22 or 93 of the PGPA Act, a *Government Policy Order* that specifies a policy that is to be applied.

3 ANAO Audit Report No.49 2013–14, *Management of Physical Security*.

an expectation that an entity's BCM program should comprise the following five components:

- (a) a governance structure that establishes authorities and responsibilities for the BCM program, including for the development and approval of business continuity plans (BCPs);
- (b) an impact analysis to identify and prioritise an entity's critical services and assets, including the identification and prioritisation of information exchanges provided by, or to other entities or external parties;
- (c) plans, measures and arrangements to ensure the continued availability of critical services and assets, and of any other service or asset when warranted by a threat and risk assessment;
- (d) activities to monitor an entity's level of overall preparedness; and
- (e) the continuous review, testing and audit of BCPs.

8. In addition to these specific requirements, entities should seek to adopt a BCM approach that is relevant, appropriate and cost-effective. In this respect, clearly defining the purpose, priorities and coverage of BCM is important. The PSPF identifies several standards and guidelines that provide additional explanation for the five BCM components, and other aspects of BCM. These include Standards Australia Handbooks published in 2004 and 2006⁴ and the ANAO Better Practice Guide (BPG) 2009, *Business Continuity Management—Building Resilience in Public Sector Entities*. In addition to the standards and guidelines referred to in the PSPF, there is a range of other useful Australian and international better practice materials.⁵ Consistent with the PSPF promotion of a risk-based approach, entities are expected to tailor their BCM arrangements to their particular context and operating environment. In this regard, entities have some flexibility in relation to the structure, content and comprehensiveness of their programs.

4 Standards Australia, HB 221–2004, *Business Continuity Management Handbook*, HB 292–2006, *A practitioner's guide to business continuity management*, and HB 293–2006, *Executive guide to business continuity management*.

5 These include: ISO22301:2012 *Societal security—Business continuity management systems—Requirements*; ISO22313:2012 *Societal security—Business continuity management systems—Guidance*; ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements*; AS/NZS 5050:2010 *Business Continuity—Managing disruption-related risk*; and ISO15489:2001 *Information and documentation—Records Management*.

9. Entities subject to the PSPF are required to report annually on their compliance with the mandatory PSPF requirements to their portfolio minister.⁶ Of the 110 entities that reported on the GOV 11 mandatory requirement in 2013, 12 entities reported that they were non-compliant. The majority of the non-compliant entities were in the process of finalising reviews of their BCPs at the time of reporting.

Previous audits

10. The ANAO has conducted four audits since 2002 that have focused on BCM arrangements in entities.⁷ Each of these audits has identified areas for improvement. Specific areas for improvement include the need for enhanced oversight and testing of BCM arrangements, as well as the need to adopt a program management approach to BCM in order to facilitate continual review and adjustment. The ANAO has also considered BCP and disaster recovery planning as part of the interim phase of the audits of financial statements of major general government sector agencies. These audits have highlighted the importance of BCP and ICT disaster recovery planning to the continuing delivery of services, but have observed that a number of entities relied on unplanned disruptions to business operations to test their BCPs.⁸

Audit objective, criteria and scope

Audit objective

11. The objective of the audit was to assess the adequacy of selected Australian Government entities' practices and procedures to manage business continuity. To conclude against this objective, the ANAO adopted high-level criteria relating to the entities' establishment, implementation and review of business continuity arrangements.

6 Copies of these reports must be sent to the Attorney-General's Department and the Auditor-General.

7 These audits were: ANAO Audit Report No.53 2002–03, *Business Continuity Management Follow-on Audit*; ANAO Audit Report No.9 2003–04, *Business Continuity Management and Emergency Management in Centrelink*; ANAO Report No.16 2008–09, *The Australian Taxation Office's Administration of Business Continuity Management*; and ANAO Audit Report No.46 2008–09, *Business Continuity Management and Emergency Management in Centrelink*.

8 ANAO Audit Report No.44 2013–14, *Interim Phase of the Audits of the Financial Statements of Major General Government Sector Agencies for the year ending 30 June 2014*, pp. 69 and 70.

12. The ANAO examined BCM arrangements and practices in the:
- Civil Aviation Safety Authority (CASA)⁹;
 - Department of Finance (Finance); and
 - Department of Social Services (DSS).
13. For the selected entities¹⁰, the ANAO assessed the BCM framework and approach, including key documentation (such as BCM policy and BCPs), entity responses to actual events, BCM exercises and testing activities, and monitoring and review.

Overall conclusion

14. The risk and potential consequences of natural disasters and other business disruption events reinforces the need for Australian Government entities to have effective business continuity management (BCM) arrangements in place to provide for the continued availability of critical services and assets. Effective BCM arrangements give entity management and stakeholders greater confidence in the entity's ability to manage the impact of a disruption and return to business as usual.

15. In line with policy requirements and expectations of the Protective Security Policy Framework (PSPF), each of the entities had established relevant governance structures, assessed risks, identified critical functions, services or assets, undertaken business impact analyses, and developed business continuity plans (BCPs). Each of the entities assessed their business continuity risk at an entity-wide level, and developed a BCM program to manage their risk exposure. The program involved annual or biennial business impact analysis, development of BCPs, and testing of business continuity arrangements. Finance's approach was the most structured, providing a clear line of sight between the 17 functions it identified as critical and the actions that would be undertaken to recover in the event of a disruption, including key dependencies and resource requirements.

16. CASA, as a *Commonwealth Authorities and Companies Act 1997* body, was not required to comply with the PSPF, but had nonetheless developed its BCM approach generally in line with the PSPF. CASA has chosen to manage the

9 As a former *Commonwealth Authorities and Companies Act 1997* body, CASA was not required to comply with the PSPF.

10 Prior to September 2013, DSS was known as FaHCSIA and Finance was the Department of Finance and Deregulation. The scope of the audit included BCM arrangements in place prior to the changes.

business continuity of its most time critical activity¹¹ separate from its entity-wide BCP. While CASA's BCP anticipates having functions and systems operational in alternative locations within 24 hours, it did not identify a list of these critical functions or activities and their key dependencies. As a result, the focus of the plan was on enabling resources rather than critical functions as envisaged by the GOV 11 element of the PSPF and better practice guidance. However, CASA's BCP did provide a list of 23 ICT systems and facilities that need to be recovered within 48 hours. The absence of a list of critical functions, and the lack of integration of the arrangements for managing critical functions, introduces the risk that the delivery of key products and services will not be appropriately prioritised and addressed during a disruption. To better support the management of disruptions, CASA should identify and prioritise critical functions in its BCPs, and detail key dependencies.

17. As a larger and more diverse entity, DSS's BCM approach was to identify six Mission Critical Activities and 281 critical functions (requiring recovery within seven days). Of these critical functions, 120 related to the six Mission Critical Activities and the remainder were considered to be enabling services. Responses were to be managed across 33 BCPs, each varying in comprehensiveness. The volume of documentation is potentially problematic from a recovery perspective. To assist in making decisions regarding potential recovery action, DSS should prioritise and rationalise its critical functions at an entity-wide level. This would involve determining entity priorities for services and assets, particularly in relation to resourcing and the continuation, recovery and/or stand down of functions.

18. Since January 2010, the audited entities have each experienced a number of business disruptions, ranging in impact from the minor and inconvenient—partial evacuations and all day outages of critical systems—to the significant—week-long office closures due to weather events including cyclones and floods. In most cases the entities' emergency or disaster response arrangements were initiated quickly to provide protection for staff and property, however, in this period Finance was the only entity that had initiated its BCM arrangements in response to disruptions to provide protection for affected critical functions.

11 CASA's BCP specified that the provision of the Temporary Restricted Airspace approval process was the only critical activity requiring non-stop operation.

19. CASA and DSS managed several significant disruptions in 2011, including the Queensland floods and Cyclone Yasi, without activating business continuity arrangements. CASA has advised that some critical operational processes were diverted to other locations.¹² Beyond this, CASA adopted an emergency response intended to protect staff and property. Similarly, DSS responded with an emergency management approach—business continuity arrangements were not activated. Regardless, neither the emergency management nor business continuity arrangements extended to consideration of community services (delivered by the department’s funded service providers), consequently senior management within the Queensland Office sought to manage continuity issues in relation to these services as the event unfolded. A subsequent review recommended a number of operating changes. While DSS’s Queensland State Office had revised its BCM arrangements for the continuation of services delivered by funded service providers, these arrangements were not sufficiently proactive and have not been applied at an entity-wide level.

20. To understand and improve the operation of business continuity arrangements, it is important to review the response to disruptions. Finance systematically documented incidents and their impact, providing reasons why the BCPs were, or were not, initiated during an incident, and had undertaken post incident reviews. In contrast, CASA’s and DSS’s approaches to documenting events, their impact, BCM considerations and post incident review were not systematic, limiting the opportunity for continuous improvement.

21. Between 2009 and 2013 CASA and DSS had undertaken testing of some aspects of their BCM approach. This generally included testing critical ICT systems, DSS also usually conducted an annual test of its entity-wide BCP¹³, while CASA participated in a joint exercise with NSW police and emergency services. Relative to the other entities examined, Finance had a more comprehensive testing and exercising regime in place, and conducted entity-wide annual tests for some critical functions. This included post-exercise reviews, with assigned actions, to incorporate improvements or revisions into the BCPs.

12 This approach was consistent with CASA’s BCP which intends to have all critical functions and systems with a target recovery time of 24 hours operational in alternate locations within this timeframe.

13 DSS’s testing in 2013 was delayed until mid-2014 due to significant Administrative Arrangement Order changes which were announced in September 2013.

22. The PSPF provides entities with flexibility to establish a BCM approach which is appropriate to their business requirements. To be practical and useful during a disruption, the approach needs to establish priorities, be easy to follow and should be tested. Finance’s arrangements were more mature and reflected incremental improvements made by the department over a number of years. However, while CASA’s¹⁴ and DSS’s BCM approaches align with the PSPF expectation to have a BCM program, both entities should take a more structured and systematic approach to planning for, testing and responding to business disruptions. This provides for continuous improvement to business continuity planning. The ANAO has made three recommendations in this regard.

Key findings by chapter

Business Continuity Management (Chapter 2)

23. A key element of effective ongoing management of business continuity is developing and implementing an appropriate governance framework. Such a framework includes establishing overall policy, key responsibilities, annual planning arrangements, and performance review and monitoring arrangements. All audited entities had developed a governance framework as part of their BCM approach and had reviewed these in 2013. Each entity also issued policy and guidance, determined the objective and scope of their BCM approach, and assigned key roles and responsibilities. Generally, entities’ arrangements focused on continuing or recovering critical functions within maximum acceptable outage timeframes—mostly within one to seven days of a disruption.

24. CASA and Finance had developed overall BCM framework documents to promote a more coherent understanding of their approach, while DSS had not yet developed a similar overall representation of its BCM arrangements. Finance’s policy and guidance also provided targeted guidance for different stages of the BCM approach (and for different levels within the entity) with practical tools such as templates. CASA’s and DSS’s guidance was not as well-structured, and better links could have been established between their respective policy and guidance materials.

14 Noting that CASA was not required to comply with the PSPF.

Assessing and Planning for Business Continuity Needs (Chapter 3)

25. Effective planning of BCM includes: identification of critical business functions; undertaking a business impact analysis; and developing strategies and plans to manage the continuation and recovery of critical functions during a business disruption. While entities generally begin with the identification of all business processes, it is necessary to refine these into a prioritised list of critical processes, and assign target recovery times. In this respect, CASA would benefit from specifically addressing critical functions in its BCPs, and DSS from rationalising and prioritising its critical functions—the list of 281 critical functions is too extensive to usefully focus on the continuation or restoration of business priorities.

26. To restore business, entities must be able to readily identify and have on hand—or recover—the technology, telecommunications and vital records necessary to support these critical business functions. It is also important to understand external and internal dependencies and prepare adequate arrangements, including with third party providers, to make sure the entity can deliver key products and services within target recovery times. Neither DSS's nor CASA's business impact analyses and BCPs contained sufficient details of key dependencies for their critical functions. For DSS this is an important risk to manage given the department's use of third parties to deliver community services across Australia. There would also be merit in DSS adjusting its current approach towards more proactive and action-oriented plans that better facilitate business continuity preparedness.

Responding to Disruptions (Chapter 4)

27. When responding to a disruption an entity should record important decisions and actions, including the Control Team's considerations regarding activating BCM arrangements. After the entity has returned to normal operations it is sound practice to review its response to the disruption. This contributes to continuous improvement, potentially placing an entity in a better position to respond to similar future events. By analysing successes and failures, lessons to be learned can be drawn out, and actions can be taken to safeguard against failures and to replicate and repeat successes.

28. CASA and DSS should do more to systematically record key events, decisions and actions, including capturing details of the impact of events on the entity and any decisions to activate BCM arrangements. This information would also support post incident review to inform improvements to the

processes. Finance has systemically documented incidents and the reasons why BCPs were, or were not, activated during a disruption. Finance also used a post incident report to assess its response to the disruption and where necessary, made improvements to its plans.

Monitoring and Review (Chapter 5)

29. To practice, assess the effectiveness, and improve performance of business continuity arrangements, the PSPF expects entities to test and continuously review their BCPs. Finance had the most structured exercising regime, including guidance, an annual program of events, cross-entity testing of systems and post exercise reviews. While DSS and CASA both tested their critical ICT systems, both entities should develop and undertake a broader program of testing for their entity-wide and local level BCM arrangements.

30. The PSPF also emphasises the importance of entities undertaking a range of activities to monitor their overall level of preparedness. None of the entities sufficiently monitored their overall preparedness to manage and resolve business disruptions. To better meet the expectations of the PSPF, the audited entities would benefit from regularly monitoring their overall level of preparedness and reporting on the extent to which key performance targets are met.

Summary of entities' responses

31. The audited entities' summary responses to the audit report are provided below. Appendix 1 contains the entities' full response to the audit report.

Civil Aviation Safety Authority

32. While CASA is not required to comply with the Protective Security Policy Framework (PSPF), CASA fully acknowledges the importance of business continuity and in addition to the GOV 11 requirement CASA has adopted a BCM approach that is tailored to CASA's business objectives and operating environment, risk based and relevant.

33. Overall, CASA accepts the ANAO findings and the continuous improvement which can be generated through the implementation of the recommendations contained in the report. CASA has already undertaken steps to address the recommendations and thanks the ANAO for their professional conduct during the fieldwork and their ongoing consultation with CASA's management team throughout the process.

Department of Finance

34. The Department of Finance acknowledges the findings of this report and supports the recommendations. The Department found the audit process to be a valuable exercise and appreciates the positive feedback provided by the ANAO on the Department's performance in relation to its business continuity management practices.

Department of Social Services

35. The Department of Social Services (DSS) welcomes the ANAO audit report on Business Continuity Management and supports the recommendations made by the ANAO.

36. DSS is committed to managing business interruptions that have the potential to affect its critical services and assets as well as the wider Australian community. DSS continues to refine its framework to ensure a well-developed, structured and robust business continuity program leading to improved organisational resilience.

Recommendations

The recommendations are likely to be relevant to other Australian Government entities. Therefore, all Australian Government entities are encouraged to assess the benefits of implementing these recommendations in light of their own circumstances, including the extent to which each recommendation, or part thereof, is addressed by practices already in place.

Recommendation No.1
Paragraph 3.36

To better support the recovery of critical functions, the ANAO recommends that CASA and DSS more systematically identify and prioritise critical functions, and document the relevant external and internal dependencies in their business continuity plans.

Response from relevant entities: *Agreed.*

Recommendation No.2
Paragraph 4.26

To improve business continuity arrangements the ANAO recommends that CASA and DSS take a more systematic approach to analysing decisions and actions taken, and reviewing the effectiveness of business continuity management arrangements after the disruption.

Response from relevant entities: *Agreed.*

Recommendation No.3
Paragraph 5.16

To provide assurance that business continuity plans are current and would operate as intended during a disruption, the ANAO recommends that CASA and DSS develop and undertake more comprehensive and regular testing of their business continuity arrangements.

Response from relevant entities: *Agreed.*

Audit Findings

1. Introduction

Business continuity management in the Australian Government

1.1 Government entities face a range of situations that may lead to significant business disruption. Providing continuity of critical public services and assets in the face of a disruptive event is essential to the economic and social well-being of Australian society—a failure of a public sector entity to deliver these could have significant consequences for those concerned and for the nation. Other services may not be essential, but a disruption can nonetheless result in inconvenience and inefficiency, and have economic costs.

1.2 When a disruption occurs, often an entity will initially activate emergency response or disaster management arrangements to ensure the safety of staff and assets. However, entities also need to have arrangements in place for the continuation and/or resumption of essential services and ultimately return to business as usual. Business continuity management (BCM) is the development, implementation and maintenance of policies, frameworks and programs, to assist an entity manage a business disruption, as well as build entity resilience.¹⁵ As such, BCM is an important element of good governance and forms part of an entity’s overall approach to effective risk management.¹⁶

1.3 To appropriately focus an entity’s business continuity arrangements, it is important to have a clear and agreed understanding of the entity’s business objectives and the critical business functions or activities which help to achieve those objectives. The business continuity arrangements should also identify the resources supporting these priority functions. These enabling resources are also known as enabling assets and services, and include information and communication technology (ICT), property and security, and human resources.

15 Resilience comes from tackling the likelihood as well as the consequence of disruptive events. Therefore it is important to have both effective risk management and business continuity management frameworks in place. Resilience allows the entity to anticipate disruptive events, constantly adapt to change, and survive and bounce back from disruptions.

16 BCM should also operate alongside other corporate governance arrangements, including disaster recovery planning and incident management.

Policy requirements and better practice

1.4 Business continuity management in Australian Government entities is governed by the Protective Security Policy Framework (PSPF) which requires entities to use a risk management approach to cover all areas of protective security activity.¹⁷ The PSPF was introduced in July 2010 and applies to all former *Financial Management and Accountability Act 1997* (FMA Act) agencies, and to those former *Commonwealth Authorities and Companies Act 1997* (CAC Act) bodies that have received a Ministerial Direction. This arrangement is currently being revised as part of the introduction of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).¹⁸

1.5 For entities subject to the PSPF, the key mandatory requirements for BCM are GOV 11 (which requires agencies to establish a BCM Program to provide for continued availability of critical services and assets¹⁹) and PHYSEC 7 (which requires plans for heightened security levels in case of increased threats). Table 1.1, below, outlines these requirements. The focus of this audit is the GOV 11 requirement. The ANAO completed an audit in 2013–14 of the *Management of Physical Security*²⁰ which included a focus on the implementation of PHYSEC 7 in three entities.

17 The PSPF established a mandatory requirement, GOV 6, for entities to adopt a risk management approach. This approach should include: determining the likelihood and impact of threats to people, information and assets occurring; assessing the adequacy of existing safeguards for each threat; and implementing any supplementary protective security measures for unacceptable threats. PSPF, June 2013, p. 12. Attorney-General's Department, *Securing Government Business—Protective Security Guidance for Executives*, May 2012, Version 1.2, p. 3.

18 The PGPA Act effectively replaced the FMA Act and the CAC Act from 1 July 2014. The PGPA Act removed the distinction between FMA agencies and CAC bodies, and introduced two broad categories of Australian Government bodies (Commonwealth entities and Commonwealth companies). Under Section 21 of the PGPA Act, non-corporate Commonwealth entities are required to comply with the policies of the Australian Government, including the PSPF. On the other hand, Australian Government policies, including the PSPF, do not apply to corporate Commonwealth entities and Commonwealth companies unless the Finance Minister issues, under sections 22 or 93 of the PGPA Act, a *Government Policy Order* that specifies a policy that is to be applied.

19 As outlined above risk identification and planning is a mandatory requirement of the PSPF (GOV 6) and is integral to meeting the GOV 11 requirement.

20 ANAO Audit Report No.49 2013–14, *Management of Physical Security*.

Table 1.1: Protective Security Policy Framework—key mandatory requirements relating to business continuity management

Mandatory Requirement	Detail
GOV 11	Agencies must establish a business continuity management program to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a threat and risk assessment.
PHYSEC 7	Agencies must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian Government may direct its agencies to implement heightened security levels.

Source: PSPF, June 2013, pp. 18 and 34.

1.6 BCM is also an integral component of the PSPF's information security management (such as INFOSEC 4²¹)—where the overarching policy requirements are confidentiality, integrity and availability of information and associated assets. Specifically, system availability requirements need to be considered, and appropriate measures must be applied including the development of business continuity and disaster recovery plans.²²

Expectations underlying the GOV 11 requirement

1.7 The PSPF mandatory requirements are supported by detailed protocols, standards and guidelines. GOV 11 includes an expectation that an entity's BCM program should be comprised of five components: a governance structure; an impact analysis; plans, measures and arrangements; preparedness monitoring activities; and continuous review and testing. A detailed description of these components is provided in Table 1.2.

21 INFOSEC 4 is another mandatory requirement of the PSPF stating that entities must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the Australian Government Information Security Manual.

22 2014 Australian Government Information Security Manual (Controls document) pp. 40-41, which include mandatory requirements.

Table 1.2: Business continuity management expectations—Protective Security Policy Framework components

Component	Description
Governance structure	Establishes authorities and responsibilities for the BCM program, and for the development and approval of Business Continuity Plans (BCP).
Impact analysis	Identifies and prioritises an agency’s critical services and assets, including the identification and prioritisation of information exchanges provided by, or to other agencies or external parties.
Plans, measures and arrangements	Plans, measures and arrangements are to ensure the continued availability of critical services and assets, and of any other service or asset when warranted by a threat and risk assessment.
Preparedness monitoring activities	Activities undertaken to monitor an agency’s level of overall preparedness.
Continuous review and testing	Process of continuous review, testing and audit of BCPs.

Source: PSPF, June 2013, p. 18.

1.8 The PSPF identifies several standards and guidelines that provide additional explanation of each of the five BCM components, and other aspects of BCM, including Standards Australia handbooks published in 2004 and 2006²³ and the Australian National Audit Office (ANAO) Better Practice Guide (BPG), 2009, *Business Continuity Management—Building resilience in Public Sector Entities*. In addition to the standards and guidelines referred to in the PSPF, there is a range of other Australian and international better practice material.²⁴

1.9 Consistent with the PSPF promotion of a risk-based approach, entities should tailor their business continuity arrangements to their particular context and operating environment. In this regard, entities have flexibility in relation to the structure, content and comprehensiveness of their programs (depending on each entity’s requirements), and the standards and guidelines they adopt.

23 Standards Australia, HB 221–2004, *Business Continuity Management Handbook*, HB 292–2006, *A practitioner’s guide to business continuity management*, and HB 293–2006, *Executive guide to business continuity management*.

24 These include: ISO22301:2012 *Societal security—Business continuity management systems—Requirements*; ISO22313:2012 *Societal security—Business continuity management systems—Guidance*; ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements*; AS/NZS 5050:2010 *Business Continuity—Managing disruption-related risk*; and ISO15489:2001 *Information and documentation—Records Management*.

1.10 In addition, the National Archives of Australia has developed minimum requirements for basic information and records management.²⁵ *Check-up 2.0* established a minimum requirement for information and records management of having business continuity and disaster management plans that: identify vital records; cover records in all formats; and are regularly reviewed and updated. *Check-up Digital* also requires business continuity and disaster recovery plans for all digital information.

Developments in International Standards

1.11 The 2009 ANAO BPG and Australian Standards handbooks are referenced in the PSPF as further guidance. Over time, some elements of this guidance have been superseded, or are no longer relevant.²⁶ For example, Standards Australia's HB 292–2006 *A Practitioners Guide to Business Continuity Management* notes that there is no internationally defined or accepted standard for business continuity.²⁷ This changed in 2012, when the following international BCM standards were released:

- ISO 22301:2012 *Societal security—Business continuity management systems—Requirements*; and
- ISO 22313:2012 *Societal security—Business continuity management systems—Guidance*.²⁸

1.12 These standards provide references to more recent guidance material, including the latest risk management standard and they adopt international BCM terminology, methods, concepts and practices. These international standards have not been adopted by the PSPF (or Standards Australia).

25 National Archives of Australia (NAA), *Check-up 2.0*, 22 August 2012, Section 6: Business Continuity Management. In July 2014, NAA released *Check-up Digital*. *Check-up Digital* is an online tool to assess agencies' digital information management maturity and capabilities. The minimum requirements for BCM remain the same, although the requirement to identify vital records is not explicitly stated in *Check-up Digital*. *Check-up Digital* includes an additional requirement for entities to successfully test or simulate its business continuity and disaster recovery plans on a regular basis. Available at <<http://www.naa.gov.au/records-management/check-up/index.aspx>>; [accessed 1 August 2014].

26 For example, the Standards Australia handbooks and the 2009 ANAO Better Practice Guide make reference to the Australian/New Zealand Standard AS/NZS 4360:2004—*Risk Management*. AS/NZS 4360: 2004 was replaced in November 2009 by AS/NZS ISO 31000: 2009 *Risk management—Principles and guidelines*.

27 Standards Australia, HB 292–2006, *A Practitioners Guide to Business Continuity Management*, p. 11.

28 In 2010, Standards Australia released an updated BCM standard: AS/NZS 5050:2010 *Business continuity—Managing disruption-related risk*. In addition, other International Standards that have implications for BCM have been released including: ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements*.

Australian Government reporting on business continuity management arrangements

1.13 Entities subject to the PSPF must report annually on their compliance with the PSPF to their portfolio minister.²⁹ Of the 110 entities that reported on the GOV 11 mandatory requirement in 2013, 12 entities reported that they were non-compliant. The majority of the non-compliant entities were in the process of finalising reviews of their business continuity plans (BCPs) at the time of reporting.

1.14 Comcover also conducts an annual Benchmarking Survey of its Fund Members' Risk Management. The survey includes consideration of Business Continuity and Disaster Recovery. In 2013, 143 Fund Member entities responded to the survey. Comcover noted that one of the most significant changes since the survey was first undertaken in 2010 was in relation to improvements in the maturity of business continuity and disaster recovery. Responses indicated that many entities were building enhanced BCPs which were critical to respond to adverse events impacting agency operations. Survey results also indicated entities were investing in establishing and regularly testing BCPs, including defining roles and responsibilities for critical business processes.

Previous audits

1.15 The ANAO has conducted four audits since 2002 that have focused on BCM arrangements in entities.³⁰ Each of these audits has identified areas for improvement. Specific areas for improvement include the need for enhanced oversight and testing of BCM arrangements, as well as the need to adopt a program management approach to BCM to facilitate continual review and adjustment to remain relevant to changing operating and external environments. ANAO has also considered BCP and disaster recovery planning as part of the interim phase of the audits of financial statements of major general government

29 This mandatory requirement is established by GOV 7 in the PSPF. Copies of this report must be sent to the Attorney-General's Department (AGD) and the Auditor-General. Entities must also advise non-compliance with relevant mandatory requirements to the Defence Signals Directorate, the Australian Security Intelligence Organisation, and/or heads of any entities whose people, information or assets may be affected by non-compliance.

30 These audits were: ANAO Audit Report No.53 2002–03, *Business Continuity Management Follow-on Audit*; ANAO Audit Report No.9 2003–04, *Business Continuity Management and Emergency Management in Centrelink*; ANAO Report No.16 2008–09, *The Australian Taxation Office's Administration of Business Continuity Management*; and ANAO Audit Report No.46 2008–09, *Business Continuity Management and Emergency Management in Centrelink*.

sector agencies. These audits have highlighted the importance of BCP and ICT disaster recovery planning to the continuing delivery of services, but have observed that a number of entities relied on unplanned disruptions to business operations to test their BCPs.³¹

Audit objective, criteria and scope

1.16 The objective of the audit was to assess the adequacy of selected Australian Government entities' practices and procedures to manage business continuity.

1.17 To conclude against this objective the ANAO adopted the following high-level criteria:

- entities established a sound BCM framework that supports effective ongoing management of business continuity, and which is integrated with other corporate governance arrangements;
- entities effectively implemented the BCM framework, including documenting key analysis, plans, controls and testing of arrangements; and
- entities established effective monitoring and review arrangements, which supports continuous improvement in BCM arrangements.

1.18 The scope of the audit included the examination of BCM arrangements in three entities. The entities were selected to provide a range of the BCM challenges across Australian Government entities. These entities were the:

- Civil Aviation Safety Authority (CASA);
- Department of Finance (Finance). Formerly the Department of Finance and Deregulation; and
- Department of Social Services (DSS). Formerly the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA).

1.19 The ANAO assessed these entities against key requirements of the PSPF. CASA, as a former CAC Act body³², was not required to comply with the PSPF, nonetheless it had developed BCM arrangements. During the course of

31 ANAO Audit Report No.44 2013–14, *Interim Phase of the Audits of the Financial Statements of Major General Government Sector Agencies for the year ending 30 June 2014*, pp. 69 and 70.

32 CASA had not received a ministerial direction to comply with the PSPF.

the audit, machinery of government changes affected DSS and Finance. These changes had a significant impact on the coverage and relevance of DSS's BCM arrangements.³³

1.20 The three entities differed considerably in terms of the type of services they provided to the Australian public, their operations, structure, geographic locations, and size. Each entity had functions that would not be noticeably affected by a week-long disruption to operations, for example, a delay in CASA's industry delegate training would result in individuals needing to wait longer than normal to receive training and be appointed as industry delegates. This is also the case for many functions performed by DSS³⁴ and Finance.³⁵ However, each of the entities also had functions where even a brief disruption may have serious repercussions for the delivery of key activities and services to the Australian public. These critical activities include ongoing management of Australian airspace, controlling and monitoring the movement of funds through the Official Public Account, the delivery of payments to more than eight million Australians, and the delivery of essential community services to the vulnerable including daily services for disability and mental health programs which are delivered by funded service providers.

1.21 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of \$572 543.

33 In September 2013 FaHCSIA was abolished and DSS was established. Major changes to matters dealt with by the department included losing Indigenous programs and policy, and gaining working age payments, services to help people with disabilities obtain employment, and policies and programs for the aged. The Administrative Arrangement Order of September 2013 also affected the matters dealt with by the Department of Finance (formerly the Department of Finance and Deregulation), but these changes did not impact on any of the identified critical functions.

34 For example, in relation to the Department's property and procurement activities, non-critical functions include: procurement reporting obligations, and managing staff housing.

35 For example, Finance's production of the annual appropriation Bills for Parliament and adjustments to appropriation Acts as required by the Machinery of Government changes was considered important but a disruption to the function can be managed for up to two weeks.

Report structure

1.22 The structure for the report is outlined in Table 1.3.

Table 1.3: Report structure

Chapter	Chapter Overview
Chapter 2—Business Continuity Management	This chapter examines the policy and guidance framework, and management arrangements for business continuity in the entities.
Chapter 3—Assessing and Planning for Business Continuity Needs	This chapter examines the entities' approaches to business impact analysis and business continuity planning, as well as the extent to which the entities applied these processes to identify critical functions and plan for the continuation or recovery of these functions in the event of a disruption.
Chapter 4—Responding to Disruptions	This chapter examines the activation of business continuity plans, and the reporting and review of the entities' responses to business disruptions.
Chapter 5—Monitoring and Review	This chapter discusses the extent to which entities monitor their level of overall preparedness by testing and reviewing their business continuity arrangements.

2. Business Continuity Management

This chapter examines the policy and guidance framework, and management arrangements for business continuity in the entities.

Introduction

2.1 Under the Protective Security Policy Framework (PSPF), all relevant Australian Government entities are expected to develop a business continuity management (BCM) governance structure as part of their BCM approach. At a basic level, a governance framework will establish the scope, objectives, and roles and responsibilities for BCM arrangements. The framework should also establish policy and guidance which outlines key management processes to be undertaken as part of the business continuity arrangements, including expectations in relation to business impact analysis, development and approval of business continuity plans (BCPs), testing arrangements, and monitoring and review. In addition, the BCM framework should be linked with other governance frameworks in the entity including the risk management framework. Once a BCM governance framework is established, the entity then needs to put in place a work program to support the maintenance, review and continuous improvement of business continuity arrangements. The extent of the program of work will be informed by an assessment of disruption related risk.

Disruption related risk

2.2 An entity's risk assessment of business activities and IT services provides useful information to assist in analysing an entity's business continuity needs and subsequent approach. An entity-wide risk assessment process was undertaken in each of the audited entities and identified business continuity related risk exposures affecting the delivery of services or ICT arrangements. Both Finance and DSS assessed their business continuity related risk as a matter that needed to be monitored at an entity-wide level. This assessment heightened the importance of BCM arrangements in these entities. In comparison, CASA had assessed its business continuity related risk as a matter that could be monitored at a business group level. This risk rating was derived from an assessment that CASA's existing business continuity arrangements were sufficient to manage BCM risk from an entity-wide perspective. These assessments influenced the nature, scale and scope of the entity's annual work program for BCM and BCM arrangements.

2.3 Another valuable source of information for analysing an entity's business continuity needs is an assessment of the risk of disruption scenarios to which the entity may be vulnerable. CASA and DSS did not assess the risk of disruption scenarios. Training material delivered by Finance in mid-2013 indicated that Finance was considering treatment of disruption related risk. The approach outlined in the training material sought to proactively manage disruption related risk by establishing mitigation strategies for times when key resources—such as buildings, equipment, technology and staff—were not available. Finance considered that this approach supported a business continuity response, regardless of the scenario.³⁶ An example of the type of business continuity risk considered using Finance's approach at a branch level is provided at Table 2.1. Each risk would then be supported by a consideration of the: causes; consequences; risk rating; mitigation strategy (which would be documented in the relevant branch recovery kit³⁷); residual risk rating; and responsible officer.

Table 2.1: Example of Finance's business continuity disruption risks

Business continuity risks at a branch level:

- our key buildings are unavailable;
- the equipment we rely on is not available;
- our phones or ICT are unavailable;
- our key staff are unavailable;
- our recovery kit fails on the day;
- recovery kit is unavailable on the day; and
- other risks.

Source: Adapted from Finance's training material.

Business continuity management framework

2.4 Each of the entities had developed policy and guidance, governance structures, and processes that formed part of their BCM framework. The frameworks were based on a variety of better practice material, although DSS was the only entity to identify the GOV 11 requirement from the PSPF in its

36 An alternative approach would be to consider the cause—such as a flood, cyclone or power failure—of disruption related risk, however, such an approach focuses the entity's response on a particular type of event rather than the impact of the event on the entity's business.

37 Finance's recovery kits guide the response of business continuity Control and Response Teams. These kits are discussed further in Chapter 3 and 4 of this report.

framework documentation. Each of the frameworks identified that BCM was cyclical and ongoing in nature, with DSS and Finance having established an annual review process and CASA a biennial review process, unless the circumstances required an earlier review.³⁸ Approaches taken by the three entities are summarised below.

Civil Aviation Safety Authority

2.5 To promote a more coherent understanding of its BCM approach, CASA had developed an overarching framework³⁹ document which included: BCM planning processes; required documentation; and a summary of key elements considered essential for an effective BCM program.⁴⁰ CASA’s expectations for each of these components are provided in Table 2.2.

2.6 CASA’s framework stated that a communication policy should be developed covering all critical aspects of communication and related activities, including dealing with the media. CASA’s framework also emphasised the importance of maintaining current standard operating procedures for business units to assist personnel who are unfamiliar with a task during an incident.

Table 2.2: Civil Aviation Safety Authority’s Business Continuity Management Framework

Component	Description
Planning process	<p>The planning process defines the role of the executive, business units and enabling services (which includes information technology, property and security, people, and media and communications) in identifying key products and services, maximum tolerable periods of disruption, critical activities, risk assessment, and strategies and plans to manage business continuity risks.</p> <p>The planning phase also considers related plans, including the: emergency management plan; communication plan; pandemic plan; risk management plan; security plan; ICT disaster recovery plan; and standard operating procedures.</p>

38 An earlier review would be required in situations such as the introduction of a new system or a change in business operations.

39 Guidance in CASA’s framework was based on a variety of better practice documentation including: *Business Continuity Institute Good Practice Guidelines 2010—Global Edition*; British Standards Institute BS 25999–1:2006 *Business Continuity Management—Code of Practice*; British Standards Institute BS 25999–2:2007 *Business Continuity Management—Specification*; the 2009 ANAO Better Practice Guide; and AS/NZS ISO 31000:2009 *Risk Management—Principles and Guidelines*.

40 CASA, *CASA Business Continuity Management Framework*, Version 1.1, July 2013, p. 5.

Component	Description
Documentation	Policy statement. Business impact analysis, risk assessments and agreed strategies. Business continuity plans (and possibly an emergency management plan). Registers of reviews, exercises, incident summaries and audits, as well as an exercise program or schedule. Review and maintenance program. Training and awareness raising.
Key elements	Business continuity plans including team briefs, and contact, action and stakeholder lists. Command team, including team composition and an incident recorder. Timings for each activity which support overall achievement of maximum tolerable periods of disruption. Standard operating procedures. Exercising program, and incident and business continuity preparedness.

Source: *CASA Business Continuity Management Framework*, Version 1.1, July 2013.

Department of Finance

2.7 Finance's BCM framework⁴¹ incorporated three distinct areas of focus: Finance's role within Continuity of Government Planning; departmental-wide BCM; and group level BCM for different areas in the department. A key expectation noted in the framework was that the departmental and group BCM would operate in unison. Finance's framework overview document provided a pictorial presentation of the framework and explained the focus and components of BCM arrangements (see Figure 2.1 below for a high level summary of the Finance framework).

41 Finance's framework identified that it was developed to be consistent with AS/NZS 5050:2010 *Business continuity—Managing disruption-related risk*, and the 2009 ANAO Better Practice Guide.

Figure 2.1: Overview of Finance’s Business Continuity Management Framework

Secretary			
Emergency Management Framework	Business Continuity Management Framework:		External Continuity Planning^(B)
	1. Continuity of Government Planning. ^(A)		
	2. Departmental Business Continuity Management: <ul style="list-style-type: none"> • Central Control Team (CCT); and • Enabling Services Advisors (Human Resources, Information and Communication Technology Disaster Recovery, and Accommodation and Facilities). 		
	3. Group Business Continuity Management.		

Source: Summary of Finance’s Business Continuity Management Framework Diagram, 2013.

- Note:
- (A) The Continuity of Government (CoG) Plan provides for the continuity of the executive functions of the Australian Government during a national security emergency. The CoG plan is the responsibility of the Department of Prime Minister and Cabinet with the coordination and implementation responsibilities falling to the Attorney-General’s Department.
 - (B) Where external continuity planning includes: service providers, co-tenants, other relevant agencies and portfolio agencies.

Department of Social Services

2.8 DSS’s Business Continuity Management Policy stated that the department’s:

Risk Management and BCM frameworks, which include the over-arching Business Continuity Plan, form the basis for continued provision of key services in the event of an emergency, national disaster or incident that causes significant disruption to [DSS’s] business ...⁴²

2.9 While the policy⁴³ identified that there was a departmental BCM framework, the elements of this framework were not captured in a single BCM document or diagram. DSS advised the ANAO that it intended to develop such a document to assist in the better understanding of BCM arrangements across the department.

42 DSS, *DSS Business Continuity Management Policy*, June 2013, Overview and Policy, p. 1.

43 DSS’s policy acknowledged the PSPF GOV 11 mandatory requirement. It also had regard for a range of better practice material including: the ANAO Better Practice Guide 2009; AS/NZS ISO/IEC 27001:2006 *Information technology—Security techniques—Information security management systems—Requirements*; AS/NZS 5050:2010 *Business continuity—Managing disruption-related risk*; Standards Australia handbooks, HB 292:2006 *A Practitioners Guide to Business Continuity Management* and HB 221:2004 *Standards Australia/Standards New Zealand Business Continuity Management Handbook*; and other Australian Government obligations including the Continuity of Government Plan and Bilateral Arrangements with the Department of Human Services.

Policy and guidance

2.10 To support their approaches to BCM, each of the entities had developed policies, including guidance and templates, and had reviewed these policies in 2013. The policies generally outlined the business continuity objectives, approach, key processes and outputs (such as business impact analysis, the development of BCPs, and testing and exercises), related frameworks and governance arrangements including roles and responsibilities.

2.11 The PSPF expects an entity's BCM governance arrangements will provide a structure for the development and approval of BCPs. In this respect entities need to consider whether there should be a single plan, or a hierarchy of BCPs. A hierarchy of plans might include an: entity-wide plan; group, branch and/or regional plans that reflect the structure of the entity; and functional level plans for each critical business function or process. Larger entities are more likely to need a range of different plans with an entity-wide plan to coordinate business continuity sub-plans for operational matters.

2.12 While each of the entities had established a hierarchy of plans to guide their response to a disruption, see Table 2.3, CASA's BCP arrangements could be more comprehensive (as its framework does not specify the need for critical function BCPs or the need for business continuity arrangements to address the continued availability of critical services and assets, beyond establishing recovery times for critical ICT assets and the non-stop management of temporary restricted airspace). However, to assist potentially inexperienced personnel in unfamiliar roles, CASA's BCM approach relied on business areas developing and maintaining standard operating procedures that would be called upon as supporting plans in a business recovery situation.⁴⁴ CASA's approach also relied on disaster recovery arrangements to be in place for critical systems.

44 In addition, one business area within CASA developed a BCP which was not approved as part of the entity-wide approach. CASA advised that, while not approved as part of the CASA wide approach, this document supports the CASA business continuity arrangements and acknowledges its subordinate role to the CASA wide BCM arrangements.

Table 2.3: Hierarchy of plans

	CASA	Finance	DSS
Entity-wide, including enabling resources	✓ ^(A)	✓	✓
Group, branch and/or regional plans	✓ ^(B)	✓	✓
Critical function	na	✓	✓

Legend: ✓ have an approved plan at this level
na not applicable

Source: ANAO analysis.

Note: (A) CASA's National Headquarters BCP is focused on a location, but it also includes arrangements for enabling resources including ICT, people management, communications and media, and property and security.
(B) CASA's BCM policy indicated regions would develop plans, but not divisions, groups or branches.

2.13 Each of the entities had also developed several templates to support the development of key BCM documents including business impact analyses and BCPs. BCM policy and guidance by entity is summarised in Table 2.4.

Table 2.4: Entities' business continuity guidance and templates

CASA	Finance	DSS
Business Continuity Management Framework.	Overview Business Continuity Management.	Business Continuity Management Policy.
Business Continuity Management Policy.	Roles and Responsibilities.	Business Impact Analysis Guide.
Business Continuity Plan Quick Reference Guide.	Group Business Continuity Management Planning.	Overarching Business Continuity Plan.
Business Impact Analysis of Critical Functions Template.	Maintenance of the Business Continuity Management Framework.	Business Impact Analysis Template.
Business Continuity Plan Template.	Activation and Response.	Business Continuity Plan Template.
	Communication During a Business Interruption Event.	
	Business Continuity Pandemic Arrangements.	
	Analysis of Functions, Resources and Vital Records Template.	
	Business Impact Analysis Template.	
	Business Continuity Plan Template.	
	BCM Strategy Template.	
	Recovery Kit Templates ^(A) .	

Source: Entity documentation, 2012 and 2013.

Note: (A) Finance had a range of templates supporting the development of documentation at the branch, division and group level. In relation to recovery kits supporting templates included: an index; pre-activation checklist; activation checklist; contact list; critical function listing; critical IT application listing; event log; meeting agenda guide; personnel report to HR; and critical infrastructure listing.

2.14 Finance's guidance was well-structured and targeted to different stages of the BCM approach (and for different levels within the entity⁴⁵) with practical tools such as templates that were linked to stages of the BCM approach.⁴⁶ CASA's and DSS's guidance was not as well-structured, and better links could have been established between their respective policy and guidance materials. For example, CASA's framework and policy documents did not make reference to existing templates to support business impact analysis and development of BCPs, instead the framework provided an overview of the content of a BCP and a link to completed BCPs. Similarly, DSS's policy listed the department's overarching BCP as a related document but did not refer to other relevant material such as the Business Impact Analysis Guide or existing templates.

Business continuity management coverage

2.15 A key step in establishing BCM arrangements is determining the scope of the BCM program and related BCPs. This includes determining factors such as: strategic and operational objectives; expected deliverables and outcomes; time requirements, demands and constraints; resourcing capabilities and limitations; geographical coverage; and which parts of the entity would be included.

Business continuity management objectives

2.16 Each of the entities had identified that the purpose, aim or objective of their business continuity arrangements was to continue to deliver key services within maximum acceptable outage periods, mostly within one to seven days of a disruption. Each entity supported these objectives by developing a program of work for business continuity (the program of work established by entities is discussed at paragraphs 2.26 to 2.28). An overview of each entity's primary BCM objective is provided in Table 2.5.

45 For example, the guidance addressed departmental business continuity at an entity-wide, group and branch level.

46 For example, Finance's Group BCM planning guidance provides an overview of a four step BCM planning process that needs to be completed by groups and branches within the department as part of annual business planning. For each step the guidance provides a link to a template that should be completed by the business area to support the planning process. The guidance clearly indicated if approval of the outputs for key steps was needed and whether the next step should be undertaken.

Table 2.5: Purpose/objective of entity business continuity management arrangements

Entity	Objective
CASA	The BCM Framework is intended to ensure the ability of CASA to continue to maintain efficient delivery of key products and services, within agreed timeframes, in the event of a major incident.
Finance	BCM refers to Finance’s ability to achieve critical functions during a business interruption event to safeguard the reputation and interests of the department.
DSS	This [BCM] Policy aims to ensure that [DSS] is prepared to deal with interruptions to critical service delivery and that in times of significant business disruption, critical departmental services are maintained to our ministers, parliamentary secretaries, communities, clients, stakeholders and service providers.

Source: CASA BCM Policy (September 2013), Finance BCM Framework (July 2013), and DSS BCM Policy (July 2013).

Business continuity management scope

2.17 Having extensive BCM arrangements for all aspects of an entity’s operations will, in most cases, not be practical. Entities need to define the scope and focus of their arrangements in policy and guidance to best manage the entity’s needs in the context of their approach to risk. Each of the audited entities sought to have an entity-wide approach to BCM, generally focusing the scope of the business continuity strategies and plans by dealing with the most critical activities, services or systems.

Civil Aviation Safety Authority

2.18 There were no specific limitations to the scope of CASA’s BCM arrangements, although the policy noted that safety of people was the single most important stage of incident management and was closely aligned with Emergency Management Plans. CASA’s arrangements were designed only to address the first three weeks of a major disruption, beyond this period standard management decision making practices were to be adopted. In addition, the plan focused on enabling resources by providing a list of 23 critical systems and facilities including telephone, website, internet and email (see Appendix 2). The National Headquarters BCP also specified that where an incident affected the provision of the Temporary Restricted Airspace approval (a function which required non-stop operation) the relevant standby procedures were to be activated independently of any decision to invoke the BCP on a wider basis.

Department of Finance

2.19 The focus of Finance’s BCM approach was on the continuation, or timely resumption of, critical functions, which must be restored within five days of the interruption event.⁴⁷ The approach recognised that critical functions were dependent on other enabling resources such as ICT, facilities, accommodation and human resources. Finance’s 2013 framework identified 17 critical functions including: controlling and monitoring the movement of funds through the Official Public Account—Cash Management; COMCAR reservations, allocations and driving operations; and supporting the government in the preparation and ongoing management of the budget. A complete list of critical functions is provided at Appendix 3.

Department of Social Services

2.20 DSS’s Business Continuity Management Policy limited its scope to six critical departmental processes with a maximum allowable outage of seven days or less. DSS’s June 2013 BCP identified that the six Mission Critical Activities (MCAs) for DSS related to ministerial support and to making payments. The list of MCAs is provided in Table 2.6. DSS identified 281 critical functions relating to the MCAs and enabling resources.

Table 2.6: Department of Social Services’ Mission Critical Activities

The following Mission Critical Activities (MCAs) were endorsed by DSS’s Executive Management Group in April 2013, following 2012–13 business impact analysis process.

- critical Ministerial and Parliamentary Secretary support;
- enabling Centrelink to make payments on [DSS’s] behalf;⁽¹⁾
- making payments to service providers, including via hosting arrangements;
- making payments to [DSS] staff;
- making payments to suppliers, and state and territory governments; and
- enabling payments on behalf of DisabilityCare Australia.⁽²⁾

Source: DSS, April 2013.

- Notes: (1) In May 2014 this MCA was changed to enabling DHS to make payments to individuals.
- (2) With the introduction of National Disability Insurance Agency (NDIA), the sixth MCA is now captured by the third MCA payments to service providers. In May 2014, the sixth MCA was changed to working with aged care providers and state emergency agencies to maintain continuity of care, particularly during emergency events.

47 This means a business impact analysis and BCP is not developed for functions that are classified as important (which must be restored in six to 14 days) or general (which have a recovery period of greater than 14 days).

Business continuity management responsibilities

2.21 The PSPF expects that entities will establish authorities and responsibilities for the BCM program, and for the development and approval of BCPs. In better practice entities, the entities' executive would be expected to sponsor the business continuity arrangements by endorsing business continuity policy, business impact analyses and BCPs, as well as participating in exercises. A senior manager or committee would generally be given direct responsibility for the execution and support of business continuity arrangements. This senior manager or committee should be supported by a team that coordinates and implements day-to-day BCM tasks.

2.22 Each of the entities included business continuity governance structures, roles and responsibilities in their policy or framework documents, and in their continuity plans. Consistent with sound practice, each of the entities involved executive and senior management in the sponsorship and execution of business continuity arrangements. The typical management structures and key responsibilities are summarised in Figure 2.2. When responding to disruptions the Control and Response Teams⁴⁸—which are depicted in Figure 2.2—are critical to the success of the entity's business continuity arrangements.

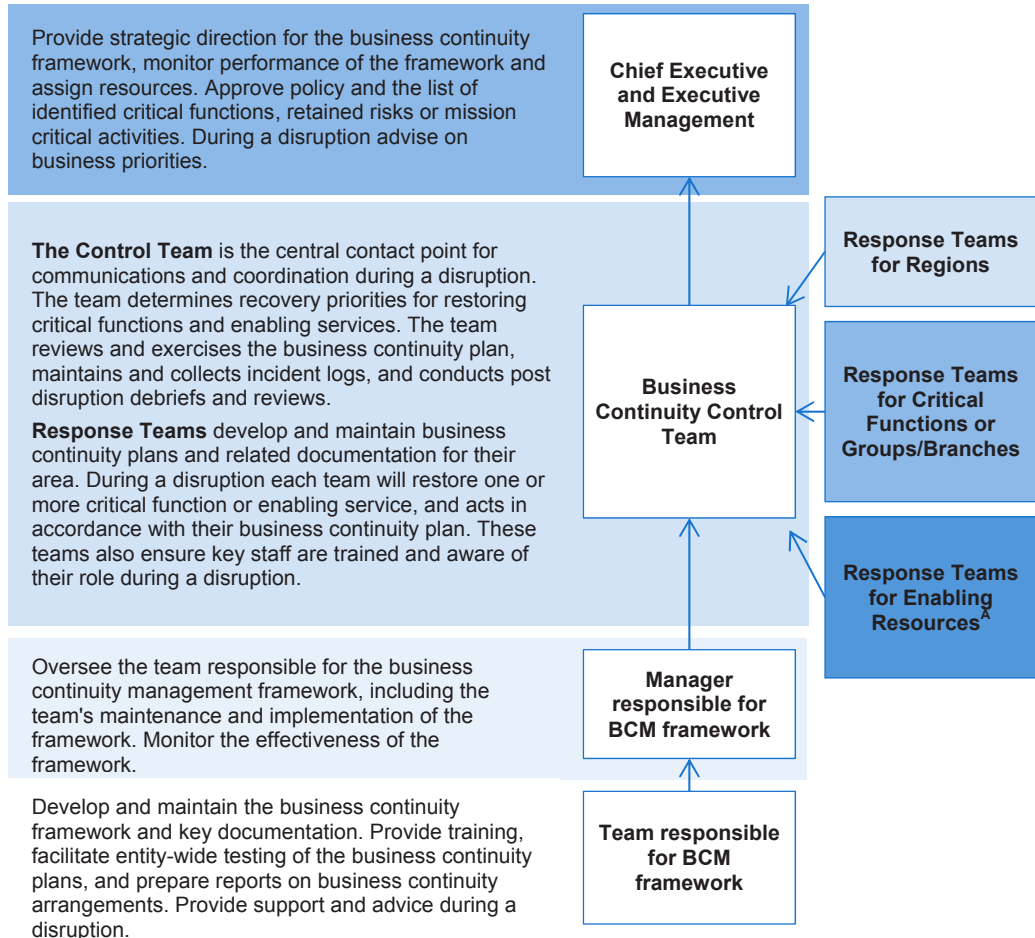
2.23 Within each entity the head of the Control Team was generally at a Deputy Chief Executive level and was supported by a number of other senior managers. These teams also had at least one manager responsible for enabling resources. In addition, a senior manager was the head of each of the Response Teams. For example, at a regional level the State Manager would be the head of the State's Response Team.

2.24 In the audited entities, various managers were responsible for developing BCPs and response plans. Generally these were managers with responsibility for critical functions, enabling resources or regional areas. CASA's BCM policy specifies that the Director is responsible for approval of the BCM policy and related documentation. CASA advised that this responsibility includes the approval of the National Headquarters BCP but does not extend to the approval of regional BCPs. Finance required approval of critical functions by the relevant Deputy Secretary and also the then Executive

48 Each entity had a different name for these teams. For example, the Control Team was known as the Command Team, the Crisis Response Team and the Central Control Team in CASA, DSS and Finance respectively.

Board prior to developing BCPs. Finance then required Deputy Secretary approval of group BCM strategies, which covered critical function BCPs. DSS’s entity-wide BCP was approved by the Chief Operating Officer and the department’s BCP template required relevant branch managers to approve branch and state office plans.

Figure 2.2: Business continuity management structures and key responsibilities



Source: ANAO, adapted from entity BCM frameworks.

Note: A. Enabling resources includes property and security, human resources, finance, and ICT.

Links to other entity frameworks

2.25 To provide a more coherent approach, each of the entities had established links between BCM arrangements and other frameworks including: enterprise risk management; security; ICT disaster recovery; emergency management; pandemic; and communication. CASA's business continuity framework also emphasised the link between BCM and standard operating procedures. Of particular note, Finance's framework linked BCM to the annual business planning process to assist with annual review, and integrated its ICT disaster recovery planning into its broader BCM framework.

Managing business continuity arrangements

2.26 After an entity has established a business continuity framework and developed BCPs, these arrangements need to be managed on an ongoing basis. Better practice suggests that ongoing management involves systematically reviewing and updating arrangements on an annual basis through integrating business continuity activities into annual business planning and periodically updating BCP contact lists. To support the PSPF expectation that entities periodically test their BCPs, entities should develop an exercise schedule to assess business continuity arrangements for critical functions and resources. Entities should also have a structured and regular system of performance monitoring.

2.27 In each entity, the business continuity framework and policy documents supported ongoing management by establishing an annual or biennial requirement to conduct a business impact analysis, develop BCPs, and test business continuity arrangements. In addition to these internal policy requirements, each entity developed an annual program of work to support the ongoing management of business continuity arrangements. The entities' work programs varied—with Finance having the most extensive program of work—generally the planned activities included maintaining and enhancing business continuity arrangements, conducting business continuity exercises, and having BCPs in place.⁴⁹ Finance had integrated its identification of critical functions, business impact analysis process and development of BCPs with its business

49 In late 2012, DSS also developed a strategic plan for the improvement of BCM which involved: revising and updating business impact analyses and the Mission Critical Activities; updating existing and/or developing new business continuity sub-plans as required; developing an over-arching BCP to address how the Department as a whole responds to a crisis, and reviewing the current format of business continuity sub-plans to maximise their usefulness during a crisis.

planning process. Finance also supplemented its annual work program with a 12 month calendar of business continuity events.

2.28 While each entity planned to undertake an annual or biennial program of work, only Finance completed business impact analyses, developed BCPs and tested arrangements in 2012–13.⁵⁰ Business impact analysis and business continuity planning are discussed further in Chapter 3 and business continuity testing is discussed in Chapter 5.

Conclusion

2.29 Each of the entities had BCM arrangements in place which were informed by a risk assessment approach. The entities had updated their BCM governance arrangements in 2013. In general, the entities' governance arrangements established the objective and scope of their BCM approach, and assigned key roles and responsibilities for BCM. Each of the entities established a range of plans to support entity-wide and operational continuity. The arrangements aimed to continue or recover critical functions within maximum acceptable outage periods and generally focused on functions that needed to be recovered within a week of a disruption.

2.30 Finance's policy and guidance provided targeted guidance for staff relating to different stages of the BCM approach including identifying critical functions, developing continuity plans, activating plans, and maintaining BCM arrangements. The guidance for key stages in developing BCM arrangements was supported by practical tools such as templates. CASA's and DSS's guidance was not as well-structured, and better links could be established between their respective policy and guidance materials. There would also be merit in CASA and DSS integrating their BCM arrangements more fully within their business planning processes to support timely periodic review.

2.31 In general, management structures provided for entity executive and senior management sponsorship of BCM. At an entity-wide level, arrangements were in place for a Control Team (comprised of senior managers) to act as a central point of contact for communications and coordination during an incident. Another important element of the entities' BCM arrangements was response teams. Each of the entities had identified teams responsible for establishing and activating a BCP for an enabling

50 For example, CASA has not conducted an entity-wide business impact analysis since 2010–11.

resource, regional office or critical function. Finance established responsibilities for approval of group BCM strategies which include BCPs and DSS established responsibility for approval of branch and regional BCPs, in contrast, CASA had not sufficiently specified responsibility for approval of regional BCPs.

2.32 Each of the entities developed a BCM program which involved, to varying degrees, annual or biennial business impact analysis, development of BCPs, and testing of business continuity arrangements. The programs were also influenced by the nature, scale and scope of the entities' business functions and the risk of disruption.

3. Assessing and Planning for Business Continuity Needs

This chapter examines the entities' approaches to business impact analysis and business continuity planning, as well as the extent to which the entities applied these processes to identify critical functions and plan for the continuation or recovery of these functions in the event of a disruption.

Introduction

3.1 Under the Protective Security Policy Framework (PSPF) entities⁵¹ are expected to:

- undertake an impact analysis to identify and prioritise the entity's critical services and assets, including identifying and prioritising information exchanges provided by, or to other entities or external parties; and
- develop plans, measures and arrangements to ensure the continued availability of critical services and assets, and of any other service or asset when warranted by a threat and risk assessment.

3.2 Once an entity has established its BCM framework, the next step is to prioritise its objectives, and identify and document the critical business services and assets (critical functions) that support these objectives. The identification of critical functions often occurs as part of a business impact analysis (BIA), which generally is used to determine how urgent each critical function is, based on an assessment of the impact of a disruption over time. This analysis allows the development of a list of time-critical functions with details of their target recovery time⁵² and resource dependencies.⁵³ Using a threat and risk assessment, the entity can then identify other services and assets, and supporting functions, that need to be continuously delivered. From this list the entity is expected to develop business continuity plans (BCPs) to address the impact of a disruption on each critical function.

51 CASA, as a *Commonwealth Authorities and Companies Act 1997* body, was not required to comply with the PSPF.

52 Across the entities different terminology was used to determine target recovery time including maximum tolerable period of disruption, maximum acceptable outage, maximum allowable outage and cry and die points.

53 Resource dependencies include a range of internal and external processes, personnel, technology, vital records and stakeholders that are essential to delivering a critical function.

3.3 To assess the preparation of entity business continuity arrangements, the ANAO examined each entity's approach to identifying critical functions, conducting BIAs including identifying critical functions, and the subsequent development of BCPs.

Business impact analysis

3.4 Business impact analysis assesses the tangible and intangible impacts of a business process being disrupted or downgraded for different time periods. It begins with identifying and understanding the critical business processes that support the entity's business objectives. It is important for entities to identify the activities and resources that support critical business processes, as well as internal and external dependencies. Then the entity can analyse the consequences of a business disruption. Finally prioritisation of the key processes enables the organisation to apply its limited resources in the most effective manner.

3.5 In line with policy expectations of the PSPF and each entity's program of work⁵⁴ (see paragraphs 2.27 and 2.28), the entities had identified critical functions, services or assets, and undertaken BIA processes. The ANAO has examined business impact analyses conducted by entities in 2012–13. In Finance and DSS the BIA involved most business areas, however, in CASA the BIA was limited to four of its six regions⁵⁵, and also did not involve National Headquarters.⁵⁶

3.6 ANAO analysed a sample of the current BIAs from each entity to consider the processes used to identify critical functions, as well as the resourcing, dependencies and target recovery time for critical functions. The results identified against the key areas of entity approaches to BIA in relation

54 Finance and DSS planned to undertake an annual program of work including a BIA, while CASA planned to undertake a biennial program of work. On this basis, each entity was due to undertake a BIA in 2012–13.

55 The four regions involved in the BIA were: North Queensland Region (which includes Townsville and Cairns offices); Central Region (which includes Adelaide and Darwin offices); Southern Region (which includes Melbourne Office); and Western Region (which includes Perth Office). The two regions not included were Eastern Region (which includes Brisbane and Tamworth offices) and Sydney Region. CASA also has four satellite offices in northern Australia.

56 In April 2014 CASA advised that the focus of the regional BIAs was to assess the ability of regional offices to deliver their functions (including regulatory services, surveillance and risk assessment and mitigation) without the support of CASA systems. CASA further advised that these regional BIAs were not undertaken specifically to confirm or verify CASA's critical business systems but to assess those which are critical to its front line service delivery staff and whether the measures the offices had in place to mitigate any major outage were appropriate.

to identifying critical functions, identifying and mapping resources and other dependencies, and target recovery times are outlined below.

Entity approaches to business impact analysis and identifying critical functions

3.7 Each of the entities had established processes for identifying and prioritising critical business functions. An overview of the approaches to BIAs and the definitions of a critical function are provided in Table 3.1. For each entity, the approach was generally supported by an established process and a template to assist business areas capture key information generated by the process, in a consistent manner. At a minimum the BIA processes were designed to identify: all functions and then critical business functions and provide a brief description of these functions; the ICT and non-ICT resources necessary to deliver the function; internal and external dependencies or stakeholders; and any workarounds or controls in place. There were a number of differences in the approaches adopted by the entities, which are discussed below in relation to each entity.

Table 3.1: Entity approaches to business impact analysis and definition of critical functions

Business impact analysis process	Critical functions definition and other conditions
CASA	
<p>The business impact analysis is to contain a list of the key functions and systems and their maximum tolerable period of disruption.</p> <p>The business impact analysis template was developed to document the listing of primary business functions (as specified in business and risk management plans) for a division, branch or region, and then to undertake a risk assessment to determine whether these functions were critical based on an overall risk level rating.</p>	<p>The business functions with an overall risk level rating of high or extreme are to be included in detailed business continuity planning as critical functions.</p>
Finance	
<p>Finance has a two stage process. First each branch is to identify all business functions. Critical functions are identified based on their maximum allowable outage period, and a business impact analysis should be completed for each critical function. These processes are supported by the following templates:</p> <ul style="list-style-type: none"> a) analysis of functions, resources and vital records; and b) business impact analysis. <p>Any critical functions identified through this process are approved by the relevant deputy secretary for inclusion in the group BCM strategy. Then a consolidated list of critical functions is endorsed by the then Executive Board.</p>	<p>Critical functions are those which have a maximum allowable outage of between zero and five days.⁽¹⁾</p>
DSS	
<p>Each business area is to undertake a business impact analysis. The analysis involves identifying business processes, and their maximum allowable outage and the impact or consequence of a disruption. Risk analysis is to be applied to determine a final rating.</p>	<p>Critical processes are those with a final risk rating of high or extreme.</p>

Source: Adapted from entity 2012 and 2013 policy and guidance.

Notes: (1) Finance identified two time critical points for its critical functions: the 'cry point' is when workarounds must commence; and the 'die point' is when workarounds can no longer be sustained.

Civil Aviation Safety Authority

3.8 The four regional BIAs conducted by CASA in 2013 did not include functions undertaken by the CASA National Headquarters or the Brisbane Office which were responsible for most of the entity's business functions.⁵⁷ The absence of an assessment of the functions undertaken by National Headquarters and Brisbane Office was inconsistent with CASA's policy expectations, which required a BIA at least every two years.⁵⁸

3.9 CASA's 2013 approach determined whether a function was critical based on a risk assessment of the function, having regard to its business objectives. Business objectives were listed in the division's or region's business and risk management plan, and CASA advised that it intended these objectives would be assigned to business functions performed by the division or region. CASA also advised that its risk management team facilitated the workshops in each of the four regions to ensure consistency in the understanding and application of the process. However, CASA's documentation provided limited guidance to business areas on the process for identifying and assessing risk (see Figure 3.1).⁵⁹ In practice, the BIAs undertaken by CASA's regional offices focused on business functions only, rather than also referencing the relevant business objectives, as can be seen in Figure 3.2.

-
- 57 In 2010–11 most business areas in CASA completed a BIA. This BIA process formed part of a review of CASA's BCM arrangements and the development of BCPs for National Headquarters, Brisbane Office and Cairns Office. National Headquarters' responsibilities include airspace and aerodrome regulation, standards, industry permissions and enabling resources. CASA advised that the Operations division is located across six regions and nine regional offices across Australia and is responsible for the majority of CASA's industry surveillance and entry control functions. Senior managers for this function are located in the Brisbane and Sydney offices. Senior managers for industry permissions and safety education and promotion are also located in Brisbane Office.
- 58 CASA advised a review of the Headquarters BIA was scheduled to commence in September 2013 on completion of the regional offices review, however this was deferred due to announcement of the ANAO audit in August 2013.
- 59 CASA's BIA process identifies nine risk areas including: commercial and legal risks; economic/financial risks; technology risks; operational risks (note: this may be divided into more specific sub headings); political risks; management activities/control risks; human resource risks; occupational health and safety/environmental; and natural events.

Figure 3.1: Business function risk assessment—Civil Aviation Safety Authority’s guidance

<p>2. RISK ASSESSMENT: Note: At least one Business Objective must be entered for each Business Function;</p> <p>2.1 List a maximum of five (5) different Business Objectives for each Business Function;</p> <p>2.2 For each Business Objective identified, allocate it to one (1) of the nine (9) risk areas, i.e. Commercial & Legal;</p> <p>2.2.1 Select the appropriate Consequence rating;</p> <p>2.2.2 Select the appropriate Probability/Likelihood rating;</p> <p>2.2.3 Add the Consequence and Probability/Likelihood score together to give the Overall Risk Level score.</p>					
Business Function	Business Objective(s)	Risk Area	Consequence Rating	Likelihood Rating	Overall Risk Level

Source: CASA, BIA of Critical Business Functions—Template, 2013, extract, p. 5.

Figure 3.2: Example of completed risk assessment including the Civil Aviation Safety Authority’s guidance

<p>2. RISK ASSESSMENT: Note: List each Business Function undertaken by the office;</p> <p>2.1 For each Business Function identified, allocate it to one (1) of the nine (9) risk areas, e.g. Operational, Technology, etc (see Annex A);</p> <p>2.2.1 Select the appropriate Consequence rating assuming the business objective will not be met;</p> <p>2.2.2 Select the appropriate Likelihood rating that the business function will not be deliverable in the event of a major incident taking into account any existing mitigation factors such as available workarounds, redirection of tasks to other offices, etc;</p> <p>2.2.3 Add the Consequence and Likelihood score together to give the Overall Risk Level score.</p>				
Business Function	Risk Area	Consequence Rating	Likelihood Rating	Overall Risk Level
Enforcement	Legal risk	Moderate	Possible	5
Regulatory Services	Political and legal	Moderate	Likely	6
Surveillance	Operational	Major	Likely	7

Source: Extract from a regional business impact analysis completed in 2013.

Notes: A risk level rating of six or more for a business function means that the function is critical.

3.10 CASA's most recent BIA processes, undertaken in 2013, have not resulted in a complete up-to-date assessment of critical functions within the entity, nor has it identified the relative priorities of these functions.⁶⁰ While its BIAs identified critical functions, CASA focused on confirming a list of critical systems and facilities developed as part of its 2011 BIA processes, rather than critical functions. This led to CASA's 2011 and 2013 BCPs only including critical ICT systems and facilities.⁶¹ The absence of an up-to-date and complete entity-wide list of critical functions introduces the risk that the delivery of key products and services will not be appropriately prioritised and addressed during a disruption.

3.11 CASA required a BIA to be undertaken at least every two years.⁶² As previously mentioned in paragraph 3.5, CASA's review has been partial and did not include two of its regions or the National Headquarters. CASA advised that it chose to focus on four regions because there were sufficient similarities between the regions. Nonetheless, the approach to this review meant that many business functions were not considered.

Department of Finance

3.12 Consistent with sound practice, Finance identified critical functions prior to conducting BIAs through identifying all business functions for an area and then determining the maximum acceptable outage ('die point') for each function. This assessment resulted in the ready classification of critical, important and general functions.⁶³ Finance required BIAs and critical business functions to be reviewed at least annually (on an entity-wide basis consistent with the scope and approach of their BCM arrangements). To ensure that the annual review was undertaken, Finance sought to integrate the identification of critical functions and the subsequent BIA process into the entity's annual business planning process.

60 In 2009 an entity-wide BIA identified a set of 28 critical business processes and recovery priorities, however, this has not been updated as the focus of subsequent BIAs moved to critical systems.

61 In April 2014, CASA advised that the BIAs completed in 2011 identified the critical systems required to support a variety of CASA functions and also listed any critical functions (for example, approval of Temporary Restricted Airspace) which did not rely on system support.

62 CASA also intend to review key functions and systems—and their maximum tolerable period of disruption—when any new system is introduced. In April 2014, CASA advised that over the past five years there have been no new systems but rather replacements of existing systems.

63 Where critical functions have a maximum acceptable outage of up to five days, important functions have a maximum acceptable outage of six to 14 days and general functions have a maximum acceptable outage of more than 14 days.

Department of Social Services

3.13 DSS defined critical processes as those with a final risk rating of high or extreme.⁶⁴ DSS's BIA guide did not use maximum acceptable outage as a criterion for determining whether a business function was critical. Nonetheless the department identified that its business continuity planning only applied to functions with a maximum acceptable outage of up to seven days. To identify critical functions DSS's process required first that the maximum acceptable outage for each function be determined and then an impact rating and a risk assessment be completed. An examination of ten BIAs completed in 2013 indicated that business areas assigned an impact rating, but did not undertake a risk assessment and as a result a final risk rating was not assigned. Therefore the department's list of critical processes was not developed in accordance with its guidance. Rather than focusing on the high risk functions, DSS's list focused more broadly on functions that needed to be restored within seven days, and as a result about 80 per cent of the functions included had in fact been assessed by DSS as having a negligible to moderate impact on DSS's operations during a business disruption.

3.14 DSS required BIAs and critical business functions to be reviewed at least annually on an entity-wide basis consistent with the scope and approach of their BCM arrangements.

Identifying and mapping resources and other dependencies

3.15 To enable continuity or rapid recovery of critical functions during a disruption, relevant enabling resources, workarounds, and other dependencies should be identified and mapped to each critical function. In most cases there will be a range of internal and external dependencies, including processes, key personnel, technology, vital records⁶⁵, suppliers and organisations that are essential to delivering a critical function. The identification of key personnel and stakeholders would also support the PSPF expectation that relevant information exchanges will be identified and prioritised. It is also important that practical steps are taken to support an efficient response during a

64 DSS's risk management framework specifies that risks rated as 'high' or 'extreme' are generally considered unacceptable and require treatment.

65 The National Archives of Australia (NAA) has developed minimum requirements for basic information and records management in *Check-up 2.0*. *Check-up 2.0* established a minimum requirement for information and records management of having business continuity and disaster management plans that: identify vital records; cover records in all formats; and are regularly reviewed and updated. In July 2014, NAA replaced *Check-up 2.0* with *Check-up Digital*.

disruption, such as maintaining details of key contacts.⁶⁶ The extent to which key dependencies were identified for the purposes of BCM varied across the entities.

Civil Aviation Safety Authority

3.16 CASA's 2013 BIAs outlined some dependencies for the entity's identified critical functions, primarily relating to the IT applications and unspecified ICT personnel. For critical functions there was also some consideration of linkages with other areas in⁶⁷ CASA but contact details for these areas were not included in business continuity documentation. Regional BIAs examined by the ANAO identified some external dependencies, but generally none of the critical functions presented in the linkages section of CASA's regional BIAs, matched the description of critical functions identified in other sections in the BIA. As a result, it is not clear whether the dependencies related to a critical function. Overall, CASA would benefit from more clearly identifying key personnel for critical functions and the internal and external areas that affect the delivery of critical functions, or which are affected by non-delivery of CASA's critical functions.

3.17 To support incident and business continuity preparedness, CASA's framework established an expectation that a vital records analysis would be undertaken to establish the hard copy records that would be necessary in the event of an incident and how these records should be managed. As outlined in paragraph 1.10, the National Archives of Australia established a requirement for entities to have business continuity and disaster management plans that: identify vital records; cover records in all formats; and are regularly reviewed and updated. However, CASA does not identify vital records in any format for the purpose of business continuity. CASA's records are held in electronic systems, including an electronic document and records management system, and beyond fully restoring these systems CASA has no other means of readily accessing the information. An exception is that CASA's People and Performance Response Plan is required to be maintained off-site, and back-up arrangements are in place for the Command and Response Team members in National Headquarters and Brisbane offices. This plan also indicates that there

66 This information should be captured as part of the BIA process and included in BCPs.

67 CASA's BIA guidance asked regions: to identify any key linkages to or from other CASA functions; describe the linkage; does the business process use inputs from or created outputs for other processes or users; and what are the linkages that the key processes have to other internal/external processes? These questions generally focus on internal linkages.

is a vital records policy that needs to be communicated to staff when business continuity arrangements are activated. CASA's arrangements would be improved by identifying vital records for critical functions.

Department of Finance

3.18 Finance's BIA process identified key personnel, internal and external ICT resource dependencies, and accommodation and facilities requirements for critical functions. Finance also identified dependencies⁶⁸ in terms of internal and external parties, and identified vital records. An example of Finance's dependencies is outlined in Table 3.2.

68 These internal or external dependencies, involve either: the provision of a service or product by another branch or entity without which the critical function could not produce its service or product; or where the critical function is necessary to support another function performed by a branch within the entity or by a third party.

Table 3.2: Example of Finance internal and external dependencies and vital records

Appropriations and Cash Management Branch
<p>Critical function: Facilitate, maintain and monitor the movement of appropriations and other funds through the Official Public Account.</p>
<p>Key internal and external dependencies were described as areas which either the department or group relied on to support their activity or where the clients relied on the activity that the department performs. For example, in relation to external dependencies, the branch was asked to consider:</p> <ul style="list-style-type: none"> • Outside Finance, who do you rely on to undertake this function? • Is there a way to undertake this function without relying on these external parties stated above? • Outside Finance, who relies on this function? <p>The branch identified that it relied on the Reserve Bank of Australia, the Australian Office of Financial Management, and Commonwealth entities to undertake this critical function. The BIA concluded that the branch would be unable to provide this function if the Reserve Bank was not operational. Outside Finance there were many external parties identified as reliant on this critical function to be provided by the branch including government ministers, Commonwealth entities, parliamentarians, members of the public, and government employees.</p> <p>Communication with stakeholders is addressed in the business continuity plan for this critical function, where the branch was asked:</p> <ul style="list-style-type: none"> • Which clients/service providers/stakeholders do you need to communicate with? <p>For each internal area or external entity that the branch needed to communicate with, the plan listed a primary contact and an alternate contact, providing a name, office phone number and mobile phone number. Consistent with the business impact analysis, the plan included contacts for the Reserve Bank of Australia.</p>
<p>Vital records were described as records that are vital for the function to operate or have historical or legal significance. The vital records identified for this critical function included:</p> <ul style="list-style-type: none"> • Appropriations and Cash Management Module of the Central Budget Management System; • Appropriations and Cash Management Module reports showing available appropriations; • appropriation development system information files; • Reserve Bank of Australia signatories; • procedural documentation; and • annual administered and departmental appropriations. <p>For each vital record the branch recorded: whether it was electronic or paper based; where it was held; where duplicate versions were held; security levels of records; and the timeframe in which the vital record was required.</p>

Source: Adapted from Finance’s Appropriations and Cash Management Branch business continuity documentation.

Department of Social Services

3.19 Like Finance, DSS also identified enabling resources and internal and external stakeholders, but for some stakeholders the BIA documentation did not establish how these dependencies affected the critical process or were affected by the critical process. Generally DSS did not capture contact information for these external stakeholders in its business continuity documentation.⁶⁹ In addition, DSS identified vital records in the BCP—if determined to be appropriate by the business area. Some critical processes⁷⁰ did not have vital records.

3.20 During a business disruption, depending on its nature and severity, funded service providers may also need to be contacted by the relevant funding department regarding their capacity to continue to provide services. Although DSS's funded service providers deliver programs across Australia, in the sample of BIAs reviewed⁷¹, only the Queensland DSS State Office identified key stakeholder engagement (including funded service providers⁷²) as a critical function. In response to the 2011 Queensland floods and Cyclone Yasi, the State Office engaged with key stakeholders to identify lessons learned and developed a Stakeholder Contact Strategy to facilitate contact with funded service providers during a business disruption (see Table 3.3). While this is a positive step, the strategy could be made more practical, by including a list of

69 For example, the BIA analysis undertaken by DSS's Financial Accounting Branch identified the Reserve Bank of Australia as an External Stakeholder for three of its critical functions, however, while the related BCP indicated that the Reserve Bank BCP should be an attachment, this stakeholder's BCP was not attached and there were no contact details for the RBA. Similarly, ministerial staff were identified as external stakeholders for the critical function of enabling the provision of advice to ministers and the executive, but there were not contact details for these staff, instead there appeared to be a reliance on critical ICT systems to support contact.

70 For example, Ministerial, Parliamentary and Executive Support Branch was responsible for the critical function of enabling the provision of advice to ministers and the executive and through its BIA identified that it did not have any vital records.

71 A review of DSS's list of critical functions indicated there were a few other examples of stakeholder engagement being identified as a critical function at a branch or regional level. For example, stakeholder engagement was also identified in relation to program administration, program management or contract management by the Mental Health Branch, Stronger Communities Branch and the Northern Territory—Alice Springs Office. Considerations of issues and crisis management were also identified by the Victorian State Office and Tasmanian State Office in relation to making payments to service providers.

72 Key stakeholder engagement involves liaison with State Government, non-government organisations and community organisations, and funded service providers.

stakeholder contacts, and should be used more broadly in the BCPs for other areas of the department.⁷³

Table 3.3: Case study—Department of Social Services’ response to Queensland floods—stakeholder contact

Between January and February 2011 two of DSS’s Queensland regional offices were affected by floods in Brisbane and Cyclone Yasi in Cairns. The response to these incidents was managed at a local level by the regional offices.

In March 2011, DSS completed a post-flood review that identified that the Queensland State Office BCP did not provide a stakeholder management strategy, or an approach to manage service providers. Contact with funded service providers during these events raised the following issues:

- many DSS staff were involved in identifying and contacting service providers—this was initially uncoordinated and fragmented, as there was no plan to identify the affected service providers;
- service providers observed that they were burdened by the extent of contact from Commonwealth and state government entities each seeking different information;
- while service providers were clear about what was needed to best assist clients during the disruption, they were not in a position to provide the information necessary to assist DSS to determine the overall need; and
- service providers were not advised of DSS temporary office closures in advance of the closures.

DSS’s Queensland Office has since recognised the importance of pre-planning stakeholder contact well before events occur and has established a funded service contact strategy as an attachment to its BCP.

Source: ANAO analysis of post-flood review documentation from DSS.

Target recovery time

3.21 Generally, a BIA should identify recovery times for critical functions.⁷⁴ Target recovery time reflects the relative criticality of a business function from an entity-wide perspective, and should be reflected in the relevant BCPs. Determining the target recovery time requires an informed understanding of the

⁷³ The ANAO notes that in its current form the service contact strategy relies on significant work to occur once an incident commences. This work includes arranging system access, interrogation of key financial and grants management systems, as well as manual review of service contract lists to identify who is likely to have been affected. It is only then that the affected service providers are identified and contact can be initiated. While it is an improvement on previous arrangements, it remains a reactive approach. A better approach would involve developing and maintaining lists of regional service providers as part of the BCP.

⁷⁴ Across the entities different terminology was used to determine target recovery time including maximum tolerable period of disruption, maximum acceptable outage, maximum allowable outage and cry and die points.

function and its dependencies, the sustainability of workarounds, and the resourcing required to resume normal operation within a target time frame. For example, recovery of critical functions may be dependent on the recovery of ICT systems that support these functions. Therefore recovery timeframes for enabling systems and resources would be relevant to the development of BCPs.

Civil Aviation Safety Authority

3.22 As previously discussed in paragraph 3.10, CASA's 2011 and 2013 BIA processes focused on identifying a list of critical systems and facilities, rather than critical functions. This led to CASA's 2011 and 2013 BCPs only including recovery times for critical ICT systems and facilities (see Appendix 2).⁷⁵ The recovery times for critical systems and facilities identified in 2013 did not directly align to recovery targets for critical functions identified in the 2011 BIAs. Better alignment of recovery times would assist in appropriately prioritising recovery action during a disruption. For example, for the four regions that completed a BIA in 2013, CASA identified critical business functions that had maximum tolerable periods of disruption of one to two weeks. In comparison, CASA's 2011 BIA⁷⁶ process identified critical functions with maximum tolerable periods of disruption generally ranging from 48 hours to three weeks.⁷⁷ The ICT systems related to these functions generally needed to be recovered within the same timeframe as the function.⁷⁸

Department of Finance

3.23 As noted in paragraph 2.19, Finance identified 17 critical functions. The priority given to these functions was determined based on recovery targets with maximum acceptable outages of 24 hours to one week.⁷⁹ Finance's BCPs linked recovery times for critical functions to the BIAs. Finance's executive has endorsed a list of critical functions and recovery times at least annually

75 In April 2014, CASA advised that the BIAs completed in 2011 identified the critical systems required to support a variety of CASA functions and also listed any critical functions (for example, approval of Temporary Restricted Airspace) which did not rely on system support.

76 The 2011 BIAs involved groups within its National Headquarters and some regions, including Brisbane Office in Eastern Region.

77 For example the BIA process in 2011 identified that functions requiring recovery within 48 hours included Industry Permissions Division functions relating to aviation medicine, flight crew licencing, and maintenance crew licencing.

78 For example, the Aviation medicine critical function is dependent on access to a full back-up of the Medical Records System, Aviation Industry Regulatory Systems, Financial Management Information System and other databases within 48 hours.

79 Finance advised one of the functions, AusTender, did not have a die point as it does not rely on departmental enabling services for continuity of service.

since 2010. This approach has assisted the department to address a recommendation from a 2008–09 internal audit to: review and rationalise critical functions at the departmental level, including their maximum acceptable outages and the critical IT applications.

Department of Social Services

3.24 As a larger and more diverse entity, DSS identified 281 critical functions⁸⁰, many with the same recovery targets—with maximum acceptable outages ranging from zero hours to seven days. DSS’s BCPs linked recovery times for critical functions to the BIAs. DSS used a rating scale to assess its priorities where a rating of ‘1’ was considered to have an insignificant impact⁸¹, and a rating of ‘5’ was considered to have an extreme impact.⁸² Of the 281 critical functions, only 20 per cent were rated as having a major or extreme impact, and nearly 30 per cent were rated as having an insignificant or minor impact.⁸³ Of these critical functions, 120 were considered to be directly related to the six Mission Critical Activities (refer to Table 2.6 on page 47) and the remainder were considered to be enabling resources for the Mission Critical Activities. The critical functions were identified across a total of 59 branches and regional offices. Notwithstanding DSS’s size and diverse functions, the value of the entity’s business continuity arrangements was diminished as there was no clear priority for business continuation and recovery action. To address this, DSS should prioritise and rationalise its critical functions at an entity-wide level. Examples of maximum acceptable outages for seven out of DSS’s total of 281 critical functions for are provided in Table 3.4 (Appendix 4 contains a list of the 57 critical functions where DSS had assigned an impact rating of major or extreme).

80 DSS’s entity-wide BCP included two lists of critical business activities; the list sorted by Mission Critical Activities included 281 critical activities, while the list sorted by maximum allowable outage included 254 critical activities. As outlined in paragraph 3.13, DSS did not complete its BIA process for the identification of critical functions, as it did not complete a risk analysis.

81 For example, an insignificant impact might involve situations resulting in minor injury, internal dissent, or minimal impact on non-core operations.

82 For example, an extreme impact might involve situations resulting in multiple deaths, national public outrage, or critical business failure, preventing performance of core activities.

83 Eight critical functions were rated as insignificant, 72 were rated as minor, 144 were rated as moderate, 38 were rated as major, and 19 were rated as extreme.

Table 3.4: Example of Department of Social Services’ recovery targets for critical functions

Maximum allowable outage (days)	Impact	Critical function
0.25	Extreme	The preparation of payment files for payroll function.
0.25	Major	To enable costings to be created to respond to urgent need and to facilitate payments to customers by DHS.
1	Extreme	Release funds to Centrelink.
1	Extreme	Process payroll.
2	Moderate	Key stakeholder engagement (of funded service providers).
2	Moderate	Managing the Office of Women international inbox.
2	Moderate	Conducting the certificate of compliance process for the Secretary.

Source: Extract from 2013 DSS BCP Appendix 2—Critical Business Activities by Maximum Allowable Outage.

Business continuity planning

3.25 In accordance with the PSPF, entities are expected to have plans, measures and arrangements to ensure the continued availability of critical services and assets, and any other services and assets when warranted by a threat and risk assessment. For each of the critical business functions identified in the BIA process, plans are expected to reduce the effect (likelihood and consequence) of a disruption to the activities, resources or systems on which the critical processes rely. This includes identifying alternative activities such as manual workarounds and resources, and planning the restoration of normal operations. It is also important to maintain contact lists for key personnel and stakeholders.

3.26 Business continuity plans should be documented, endorsed by the entity’s executive and be kept up-to-date. If there are multiple BCPs, it is generally sound practice to have an overarching entity-wide plan to coordinate business continuity sub-plans for enabling resources, critical functions and regional offices.

3.27 The audited entities each developed BCPs that describe and direct the actions to be followed in the event of a business disruption. Although some of DSS’s response and recovery procedures involve designing a strategy rather

than specifying actions (see paragraph 3.33). Key aspects of the entities BCPs are discussed below.

Civil Aviation Safety Authority

3.28 CASA developed an overarching National Headquarters BCP, and six regional BCPs.⁸⁴ The plan states that:

Key functions and systems and their respective priorities have been determined ... The BIA, upon which this BCP is based, is reviewed and the respective BCPs updated with the introduction of any new systems, and at least biennially ... This plan is primarily designed to facilitate an orderly transition of the Command Team and other essential personnel to a secure site to facilitate the overall management of an incident and to ensure the timely continuation of critical activities, if necessary at suitable alternate sites.⁸⁵

3.29 CASA's National Headquarters BCP specified that the provision of the Temporary Restricted Airspace approval process was the only critical activity requiring non-stop operation, and it was managed independently of the entity-wide BCP. The BCP specified that most activities could be deferred for 24 to 48 hours, but restoration of enabling services should commence immediately. While CASA's BCP anticipated having functions and systems operational in alternate locations within 24 hours, it did not provide a list of these critical functions or activities and their key dependencies.

3.30 CASA's BCP also provided a list of 23 ICT systems and facilities that needed to be recovered within 48 hours.⁸⁶ However, restoring the systems on the list in isolation would not necessarily ensure the continuation of the entity's critical functions. As a result, the focus of the plan was on enabling services rather than critical functions and increased the risk that the delivery of key products and services would not be appropriately prioritised and addressed during a disruption. The BCPs would benefit from the inclusion of workarounds and other recovery strategies for critical functions, and contact details for key personnel.

84 CASA has also developed response plans for media and communications, people management and property and security.

85 CASA, *Canberra National Headquarters BCP*, July 2013, pp. 5 and 6.

86 Refer to Appendix 2.

3.31 CASA's⁸⁷ BCPs and enabling service response plans generally did not contain external stakeholder contact lists (such as relevant clients, suppliers and/or service providers) to guide an efficient response in the event of a disruption. CASA's framework established an expectation that lists of key personnel⁸⁸ (those personnel that were essential to continue day-to-day operations) and key stakeholders would be maintained. CASA's people and performance response plan contained office telephone and email addresses, and occasionally contained home or mobile telephone contact information, for people management, as well as response teams for CASA's regional offices.

Department of Finance

3.32 There was a clear line of sight between the critical functions identified in the Finance and DSS BIAs and their BCPs. Consistent with its BIAs, Finance's BCPs contained contact details of key stakeholders. Finance's documentation stated that its business continuity arrangements at a departmental level were based on the restoration of key enabling services (enabling resources) that supported business groups in continuing to undertake critical functions. Finance developed targeted recovery kits to support the Control Team and other response teams to respond to a business disruption (see Table 3.5). The Control Team's recovery kit included all group business continuity strategies⁸⁹ and related critical function BCPs. In practice this meant that a branch responsible for a critical function developed a BCP for the continuation or restoration of that function and a recovery kit. Critical function BCPs formed part of the group recovery kits and business continuity strategies. Overall, Finance's BCPs were well-structured, clearly written and, in the main, comprehensive.

87 Although, CASA BCPs often provided emergency service contact details and some other external contacts including its landlord.

88 Although CASA's framework indicated that the personal details of key personnel would be held separately to the BCP.

89 Group business continuity strategies focused on establishing and documenting the action plans to ensure the continuation and/or resumption of identified critical functions if key enabling services were lost or became unavailable.

Table 3.5: Finance’s recovery kits

Overview
<p>Recovery kits were prepared for use by Finance’s Control Team and enabling service response teams, and by groups and branches responsible for critical functions.</p> <p>Recovery kits were the operational tools or business continuity action plans, used to assist in managing an event and re-establishing critical functions in an acceptable timeframe.</p> <p>Recovery kits were required to be maintained and stored in off-site locations, in a manner that was secure and readily accessible if a business interruption event was declared. Critical data and information held in the recovery kits includes:</p> <ul style="list-style-type: none"> • contact lists; • activation checklists; • critical function information (including business impact analyses and BCPs); and • recovery procedures for enabling services.

Source: Finance, *Finance Business Continuity Management Framework*, 1. Overview, July 2013.

Department of Social Services

3.33 In 2013, DSS prepared an entity-wide BCP that included the critical functions identified in its BIA process. DSS’s entity-wide BCP also included a list of 33 BCPs for national office branches, and the states and territory offices. Analysing the link between the 281 critical business functions and a sample of DSS’s national office, and state and territory office BCPs, the ANAO observed inconsistency in the approach adopted by business areas. Specifically, half of the BCPs included all critical functions relevant to the business area, while others only addressed the critical functions with an impact rating of major or extreme (see paragraph 3.13). DSS’s BCPs generally did not contain external stakeholder contact lists (such as relevant clients and/or service providers) to guide an efficient response in the event of a disruption. DSS’s BCPs were not always action-oriented. For instance, rather than establishing procedures to put in place when a disruption occurred, DSS’s response and recovery procedures sometimes involved designing a strategy to restore a critical function. An example of this approach is outlined in relation to making payments to suppliers, and state and territory governments, see Table 3.6.

Table 3.6: Department of Social Services’ response and recovery strategy for making payments

Response and recovery strategy for making payments to suppliers, and state and territory governments
Description: Ensure payments are able to be made in line with agreements.
<p>Response:</p> <ol style="list-style-type: none"> 1. Determine the potential interruption to IMPACT. 2. Select a processing strategy. Consider: <ul style="list-style-type: none"> • In order to process a manual electronic funds transfer, the bank/branch number, bank account number, bank account name and amount are required. • If this information is not available from the SAP/ FaHCSIA Online Funding Management System (FOFMS) Team, the vendor may need to be contacted by phone to obtain the details. 3. Design a strategy for managing: <ul style="list-style-type: none"> • Emergency payments (if required). • Adjustments and corrections (once normal systems are available). 4. Implement the strategy: <ul style="list-style-type: none"> • Monthly backup reports from FOFMS provided by Program Establishment and Management Branch enable the above response.

Source: Adapted from DSS, Financial Accounting Branch BCP, 2013.

Summary results for assessing and planning for business continuity management

3.34 A summary assessment for each entity against the key steps in business continuity planning is presented in Table 3.7. Adequate BCM arrangements should address these steps.

Table 3.7: Entity business continuity management processes

Processes	CASA	Finance	DSS
Periodically conducts or reviews business impact analyses across business areas	✘	✓✓	✓✓
Identifies a list of critical functions	✘	✓✓	✓
Sets target recovery times	✓	✓✓	✓
Identifies resources needed for recovery of critical functions	✓	✓✓	✓
Identifies key dependencies	✓	✓✓	✓
Documents a practical business continuity plan for each critical function	✘	✓✓	✓

Legend: ✓✓ good ✓ requires further work ✘ insufficient.

Source: ANAO analysis.

Conclusion

3.35 Consistent with PSPF expectations, each of the entities identified critical business functions, conducted BIAs for critical functions, and developed strategies and plans to manage the continuation and recovery of critical functions or systems during a business disruption. CASA identified critical functions for some regions in 2013, however, a more comprehensive BIA involving all of CASA's divisions was not undertaken in 2013. Instead, as a product of a more comprehensive 2011 BIA process, CASA identified a list of critical systems and facilities rather than functions. Finance had developed a prioritised list of critical functions to guide recovery decisions. DSS should rationalise and prioritise its list of 281 critical functions to better support decision making in the event of a disruption; potentially this would be achieved by completing the agreed BIA process. To assist in business continuity preparedness, there would also be merit in DSS standardising its approach to BCPs by making them proactive and action-oriented.

Recommendation No.1

3.36 To better support the recovery of critical functions, the ANAO recommends that CASA and DSS more systematically identify and prioritise critical functions, and document the relevant external and internal dependencies in their business continuity plans.

3.37 This recommendation was directed to CASA and DSS. Finance also commented.

Civil Aviation Safety Authority

3.38 *CASA agrees with this recommendation.*

Department of Social Services

3.39 *Agreed.*

Department of Finance

3.40 *Supported.*

4. Responding to Disruptions

This chapter examines the activation of business continuity plans, and the reporting and review of the entities' responses to business disruptions.

Introduction

4.1 There are different types of potential disruptions that an entity may be faced with and not all of these will require activation of BCPs. However, there is a point when a decision must be made as to whether a local or entity-wide BCP should be activated. The transition from 'incident' (or 'emergency') to 'business continuity event' will usually involve an element of judgement, and may not be the same for any two incidents. A sound BCM approach will seek to provide relevant guidance to decision makers to assist them in assessing whether conditions have been reached that would require the activation of a BCP. Entities' guidance on activating the plan and considerations during an incident is outlined below. The ANAO also examined entities' use of incident records and post incident reviews, to understand and improve the operation of their business continuity arrangements.

Activating business continuity plans

4.2 The potential impact on critical functions and the expected time to resolution are common issues to be considered by responsible officers, when making a decision around activating BCPs and other BCM arrangements. In this respect, each entity specified different BCP and business continuity activation points, although common key considerations were the expected duration of the outage and the impact on critical functions and systems. Arrangements could also be activated locally or at an entity-wide level. For example, CASA's regional BCPs were to be activated by state managers, although for major incidents the Command Team would activate the National Headquarters plan. The triggers for activating BCM arrangements in each entity are outlined in Table 4.1.

Table 4.1: Activation point for business continuity management arrangements

Entity	Activation point
CASA	<p>The BCP is to be activated if it is determined that the extent of the outage will impact upon sustaining key functions or systems and the duration will exceed 24 hours. NOTE: If any region sustains a major incident the National Headquarters plan may also be invoked to facilitate executive management and support of business recovery.</p> <p>If CASA's key critical function—Temporary Restricted Airspace approval—was affected by an incident its standby procedures would be activated independent of any decisions to invoke the BCP on a wider basis.</p>
Finance	<p>The BCM framework is to be activated when an incident occurs affecting enabling services, and the expected outage would exceed the maximum acceptable outage for any of the identified critical functions.</p>
DSS	<p>The Crisis Response Team, which has responsibility for entity-wide BCM arrangements, may be activated due to one of the following situations:</p> <ul style="list-style-type: none"> • an incident or problem being managed through normal business operations reaches a point where it becomes a crisis or a significant disruption to DSS's business; or • a major emergency or significant business disruption impacts upon DSS.

Source: CASA, *Canberra National Headquarters BCP*, July 2013, pp. 6 and 17; *Finance BCM 5. Activation and Response*, March 2013, p. 2; and *DSS Business Continuity Plan*, June 2013, p. 6.

Civil Aviation Safety Authority

4.3 CASA's activation guidance briefly outlined two key considerations for activating the plans. To support activation, CASA's plan included: a list of critical systems and facilities; overall incident response (which starts with emergency management); command team plan and other enabling service response team plans; team resources; incident recording templates (such as an incident log, a business interruption assessment sheet, and communications log); and key stakeholders.

Department of Finance

4.4 Finance's guidance succinctly outlined a number of key considerations for deciding whether to activate the framework, including safety, communication and coordination, and impact on critical functions. The guidance also indicated key matters to be addressed once the framework was activated. Tailored recovery kits were developed for Central Control Team, enabling services, and division and branch managers who had responsibility for one or more critical functions (see paragraph 3.32). The purpose of the recovery kit was to structure the BCM information, to make it more easily accessible during an incident. The recovery kit was split into two sections, one

addressing an emergency incident—which is not yet a business interruption event—and one addressing the business continuity event.⁹⁰

Department of Social Services

4.5 The activation of the DSS’s plan was the responsibility of the relevant group, state and branch managers, but DSS’s guidance did not concisely outline activation considerations. DSS’s plan identified that there were three phases that would be applicable to the management of any crisis:

- evaluation and planning phase—emergency management;
- plan implementation and coordination phase—continuity/recovery management; and
- situation recovery and closedown phase—recovery management.

Control team arrangements following activation

4.6 In response to an actual or potential disruption, CASA and Finance required their response teams to make an assessment of the situation and advise the Command or Control Team of threats to critical functions and enabling resources. Response teams were responsible for activating regional or critical function plans. At an entity-wide level, the Command and Control teams would then formulate strategies and allocate resources to continuing or restoring critical functions or systems.⁹¹ These steps were supported by the checklists established in business continuity planning documentation. Rather than implementing existing business continuity documentation in anticipation of or following an incident, at an entity-wide level DSS’s Crisis Response Team Recovery Director would assemble the Crisis Response Team to brief them on the initial analysis of the crisis and establish all impact/s prior to the development of an Action Plan. The analysis process would attempt to identify:

- the full impacts of the crisis on DSS's critical business processes, and identify events that may cause an escalation of the crisis;

90 The recovery kit includes: emergency incident documentation (such as staff listing, personnel report, notification to Comcare—incident forms, and pre-activation checklist); business continuity management response (including Business Continuity Strategy, and the BCM activation checklist); contact lists; information relating to critical functions including the BCP and the BIA; and an event log.

91 In Finance’s case, senior management would also be advising on their priorities, while business groups would be advising of support requirements and be implementing business continuity strategies.

- any critical business service maximum acceptable outage triggers reached and implement those BCPs; and
- whether additional personnel are required to meet with the Crisis Response Team for the development, communication and implementation of a more specific Action Plan for an unforeseen event.

4.7 This approach to entity-wide management of a business disruption was similar to the approach adopted in a number of DSS's critical function BCPs, which were not proactive and action-oriented. That is, at a branch level, response and recovery strategies sometimes involved designing a strategy to restore a critical function, rather than implementing pre-determined procedures (see paragraph 3.33 and Table 3.6). Similarly, DSS also developed approaches that were reactive rather than proactive, for example, rather than maintaining contact lists, they developed a strategy for developing a contact list once an incident occurred (see paragraph 3.20 and Table 3.3). Such an approach limits the department's preparedness for a business disruption.

4.8 Each of the entities' plans or guidance indicated that the decision to stand-down Command, Control or Recovery Teams and move to business as usual should be a clearly documented decision. There is an opportunity for entities to consider whether the documentation (for notifying staff of the conclusion of an incident and return to business as usual) could be strengthened, as in practice it did not discuss resumption of normal operations. Advice to staff generally noted when they could return to work. Further, to support continuous improvement each of the entities' stand-down processes included debriefing those involved, and for Finance and DSS, and to a lesser extent CASA, also involved lessons learnt, documentation review, process capture and preparation of a post incident review for the Command, Control or Recovery Team.

Incident records

4.9 Incident records are an important element of assessing the effectiveness of BCM arrangements and each of the entities' BCM arrangements highlighted the importance of maintaining an incident record during the incident. Such a record should include a concise and factual recording of incident-related events, decisions and actions taken.

4.10 To facilitate the incident recording process, each entity had an incident recording template (or set of templates) that could be used to support incident recording. The incident recording template can assist with meeting insurance

requirements, and in monitoring requests for services or support, and tracking tasks and resources. In practice, when an incident record was not used, regular email communication often provided a partial record of the incident. CASA's BCM arrangements required an officer to be designated to perform the role of incident recorder, although this was not a requirement identified by Finance or DSS.

Incidents

4.11 Since January 2010, the number and frequency of disruptions encountered by each entity has varied considerably, resulting in three disruptions affecting CASA, at least seven disruptions affecting Finance and more than nine disruptions affecting DSS. These disruptions ranged in impact from the inconvenience of a partial evacuation⁹², to all day outages of critical systems and week-long office closures due to extreme weather events. To reflect the differences in the number and nature of disruptions, the ANAO selected a sample⁹³ of 16 disruptions to review the extent to which continuity plans were enacted in response to the selected business disruptions, the templates that guide documentation of the disruption events, and reporting of the response to the events. For a sample of 16 incidents⁹⁴, ANAO examined incident reports and other incident documentation, such as entity event logs.

Civil Aviation Safety Authority

4.12 For the three incidents examined by the ANAO, CASA did not document the activation of BCPs in incident reporting or whether the Command Team was involved. CASA maintained a detailed event log for one of the incidents, and for another incident maintained less detailed records of events through regular email communication with the BCM team in National Headquarters. The third incident was logged and managed through an IT service request system. Based on the incident records examined, there is scope for CASA to improve its incident recording.

92 Some of these disruptions, due to their nature and impact, did not need to progress beyond an emergency response such as an evacuation. However, it is important that when faced with a disruption that there is a clear understanding of when and how business continuity should be considered in a situation that starts as an emergency response.

93 The ANAO selected incidents that affected the entities' operations in the Australian Capital Territory, Queensland and Victoria.

94 The sample includes incidents that occurred between 2010 and 2013, this included three incidents affecting CASA, six incidents affecting Finance and seven incidents affecting DSS.

Department of Finance

4.13 For the six incidents affecting Finance, there was systematic documentation of each incident⁹⁵ and reasons why the BCP was, or was not activated during the incident. For example, BCPs were activated twice for incidents that threatened to disrupt critical functions. For another incident, the possibility of implementing the BCP was discussed with the Business Continuity Manager. The incident report for a fourth incident, noted that disruption occurred in the middle of the night and that services continued to be delivered with the use of workarounds until the issue was resolved.⁹⁶

Department of Social Services

4.14 Of the seven DSS incidents examined, only one incident reported the active and early involvement of the department's Crisis Response Team, and the activation of business continuity arrangements. Three of the incidents only required emergency response and in two cases detailed event logs were completed. For another incident, some email records provided limited information about the event, although they clearly established the involvement of the Crisis Response Team Secretariat, and showed that the State Office considered there were no significant BCP issues (see Cyclone Oswald Case Study in Table 4.2). DSS did not record the details of the remaining two incidents or document considerations regarding the activation of relevant BCPs for these events.

95 In an incident report and/or a post incident review document.

96 While this incident report did not explicitly mention business continuity, it addressed key continuity considerations concerning the ability to continue to deliver services. Finance advised that in this case business continuity arrangements did not need to be activated.

Table 4.2: Case study—Department of Social Services’ response to Cyclone Oswald

Cyclone Oswald affected the Queensland coast in late January 2013, causing extensive flooding. Two DSS offices, Rockhampton and Brisbane were directly affected, while the offices in Grafton and Coffs Harbour were aware of the potential threat, including staff being cut off by flooding.

The Rockhampton office was closed for two business days adjoining a weekend, and the Brisbane office was closed for one day. The State Office Manager’s decision to close their office was consistent with the advice of the DSS Extreme Weather Preparedness Plan.

The DSS business continuity arrangements were activated to the extent that a central phone number enabled staff to check arrangements, and the Brisbane office switchboard was diverted by national office.

The DSS Queensland State Office did not request national office assistance. Queensland State Office advised, prior to the office closure, that there was no threat to the premises, and there were no business continuity problems of significance. The email advice to national office also indicated that some staff would work remotely during the closure. A briefing paper, for the Crisis Response Team Recovery Director, written immediately after the event, was consistent with the email advice given by Brisbane office.

Post incident review

4.15 Actual events provide important feedback on the success and usefulness of the continuity arrangements. Post incident review, including debriefing for major disruptions, is an essential component of the BCM lifecycle.

Civil Aviation Safety Authority

4.16 CASA’s experience dealing with disruptive events was given consideration between 2010 and 2013. In particular, in 2011 Cyclone Yasi and the Queensland floods were a catalyst for a revision of CASA’s business continuity arrangements, as outlined in Table 4.3.

Table 4.3: Case study—Civil Aviation Safety Authority’s response to the Queensland floods and Cyclone Yasi

In anticipation of severe flooding, CASA evacuated staff from its Brisbane premises on Tuesday, 11 January 2011. The following day, CASA commenced a systematic shutdown of Brisbane Office IT infrastructure (landlines and computer services) and building services. On Thursday, after the Brisbane River peaked, phones computers and building services were reinstated. On Monday 17 January 2011 Brisbane Office reopened, six days after the closure.

CASA buildings and assets were not damaged during the floods. Throughout the period CASA used mobile phones and modems to communicate with local staff and Headquarters. The priority throughout this period was to safeguard CASA staff and assets.



CASA is a co-tenant of Cairns and Townsville Airports. In anticipation of Cyclone Yasi, CASA shut down Cairns and Townsville offices on 1 February and reopened on 8 February 2011. There was no damage to the Cairns Office and some water damage to the Townsville Office. For some of the CASA shutdown period, the airports in Cairns and Townsville were also closed. CASA used email to communicate with Headquarters prior to and following the incident. Consistent with CASA’s approach to the floods, the focus throughout this period was to safeguard CASA staff and assets.

4.17 At the time of the Queensland floods and Cyclone Yasi, CASA did not have regional office BCPs, so the response to these events was heavily reliant on the actions and knowledge of individual CASA staff. Although CASA maintained an event log during the floods, it did not document actions taken with respect to critical functions for the floods or the cyclone. In addition, there was no documented post incident review for either incident.

4.18 Following these incidents, CASA updated policy and guidance documents, and developed BCPs for Cairns and Brisbane, and updated the National Headquarters BCP by June 2011. These BCPs included incident

recording forms, however, these forms did not prompt consideration of the lessons learnt or the opportunity to improve BCM arrangements.⁹⁷ This limits the potential to improve continuity planning from these events. There is scope for CASA to upgrade its post incident review arrangements to document the extent to which continuity arrangements were followed during disruption events, consider lessons learnt, and assign action items to improve continuity arrangements.

Department of Finance

4.19 The post incident reports completed by Finance between 2010 and 2013 discussed the implications of the event from a business continuity perspective including aspects which worked well and where further consideration was needed. In 2013, only Finance used a post incident report template to assess its response to the business disruptions and incidents. The template prompted discussion of the impact of the disruption on business operations, actions taken to resolve the problem, and further actions needed to improve business continuity arrangements in the future. A snapshot of the post incident report for an incident which occurred at Finance in 2013 is outlined in Table 4.4.

Table 4.4: Case study—Finance post incident review

In August 2013, an overnight water leakage from a tenancy on the floor above flooded a server room. This put Finance's communications infrastructure at risk, threatening several critical projects. The business continuity plan for the service centre and switchboard was enacted. The duration of the event was a full day.

Finance's post incident report included:

- an outline of staff impact, the root cause, corrective actions, implications for IT planning, and communications;
- review and approval of the report;
- a detailed event log; and
- a summary of issues arising from the incident, including assigned actions and due dates.

Source: Finance, *Post Incident Report* 29 August 2013.

97 Similarly, CASA's IT incident reporting form did not prompt documenting the corrective actions or lessons learnt, or assign action items to improve responsiveness.

Department of Social Services

4.20 Between 2010 and 2013 DSS reviewed its response to three major disruptive events: a review of the response to an all-day power failure and IT systems outage that occurred in June 2010; and post incident reviews for the Brisbane floods and Cyclone Yasi (see Table 4.5).⁹⁸ While the DSS review did not address the extent to which business continuity arrangements were followed it identified some opportunities for improvement but did not assign responsibility for implementing change. Post incident review arrangements would have been more effective if the department had assigned action items to senior officers.

4.21 There was scope for DSS to upgrade its post incident review arrangements to document the extent to which continuity arrangements were followed during disruption events, consider lessons learnt, and assign action items to improve continuity arrangements. In July 2014, DSS provided the ANAO with a draft post incident review template that addresses many of these considerations.

98 DSS did not undertake a post incident review of Cyclone Oswald in 2013.

Table 4.5: Case study—Department of Social Services’ post incident review of Queensland floods

In 2010–11, the department was affected by a number of natural disasters, including the Queensland floods and Cyclone Yasi in Far North Queensland. The department responded at a local level during the Queensland floods and Cyclone Yasi, which affected staff and property, and required additional service delivery.



In March 2011, the department completed a post-flood review to identify better practice and areas for improving their business continuity plans and arrangements. The review made a number of recommendations, including a strategy for contacting service providers, the need to debrief and access counselling, developing basic disaster recovery plans in small Indigenous communities, and improved central coordination. The review did not assign action items. Most of these recommendations were addressed in the 2013 Queensland State Office Business Continuity Plan.

The Queensland State Office also completed a lessons learnt paper, with updated procedures, and assigned action items. These changes were to be incorporated into the Queensland Business Continuity Plan.

Conclusion

4.22 Each of the entities developed guidance for the activation of BCM arrangements or BCPs at an entity-wide and local level. Key considerations for activation of arrangements generally addressed duration of the disruption and the impact on critical functions and systems. Following activation, at an entity-wide level, CASA's and Finance's continuity arrangements were generally action-oriented, while DSS was focused initially on a more detailed assessment of the impacts of the interruption which would then lead to the development of an action plan for managing business continuity.

4.23 To facilitate incident recording each of the entities had an incident recording template. For the incidents examined between 2010 and 2013, Finance systematically recorded key events, decisions and actions, including capturing details of the impact of events on the entity and decisions to activate or not activate BCM arrangements. During this period, DSS and CASA did not consistently record key decisions and actions, although both entities used email communication to provide a partial record of their decisions and actions. They also did not generally document consideration of whether BCM arrangements should be activated.

4.24 Finance also consistently completed post incident reviews for incidents that occurred between 2010 and 2013. These reviews identified aspects of the BCM arrangements that worked well and where further consideration was needed. DSS undertook some post incident reviews which lead to improvements in some BCM arrangements, however, the reviews did not assign action items or responsibility for the lessons learnt. CASA did not routinely review its response to the business disruption events, although these events were the catalyst for developing BCPs for Brisbane and Cairns offices, and updating its Headquarters BCP.

4.25 For CASA and DSS there is scope for more systematic recording of key events, decisions and actions, including capturing details of the impact of events on the entity and any decisions to activate BCM arrangements. This information would also support improved post incident review in these entities, including: the extent to which the BCP was followed and whether other business continuity issues should have been considered; suggesting improvements to the processes; and assigning further actions as appropriate.

Recommendation No.2

4.26 To improve business continuity arrangements the ANAO recommends that CASA and DSS take a more systematic approach to analysing decisions and actions taken, and reviewing the effectiveness of business continuity management arrangements after the disruption.

4.27 This recommendation was directed to CASA and DSS. Finance also commented.

Civil Aviation Safety Authority

4.28 *CASA agrees with this recommendation.*

Department of Social Services

4.29 *Agreed.*

Department of Finance

4.30 *Supported.*

5. Monitoring and Review

This chapter discusses the extent to which entities monitor their level of overall preparedness by testing and reviewing their business continuity arrangements.

Introduction

5.1 Under the PSPF, all relevant Australian Government entities are expected to monitor their level of overall preparedness to respond to business disruption. They are also expected to review, test and audit their BCPs. Monitoring and review arrangements should be both comprehensive and balanced. In the business continuity context, this includes testing and exercising BCPs, reviewing broader business continuity arrangements and reporting on the entity's preparedness to manage and resolve business disruptions. The following sections examine the extent and nature of business continuity testing, and other measures the audited entities had in place to monitor preparedness.

Business continuity exercising and testing

5.2 Conducting exercises provides an entity with a safe environment to practice and rehearse responses to various potential incidents. Accordingly, entities should plan a variety of testing and exercises to gauge the level of overall preparedness. The number and frequency of exercises is dependent on the needs, size and complexity of the entity but ideally every member of a response team should participate in at least one exercise per year.

5.3 Exercises may range from simple discussion based activities, through to complex, high risk, high cost, full-scale simulations. Pass/fail types of exercises are typically used to test the performance of equipment and technology capabilities within a required timeframe. Exercises should focus on different elements of the entity's BCM arrangements including testing entity-wide arrangements (and the operation of the Control Team), local and business area BCPs (and the operation of Response Teams), and recovery arrangements for enabling resources such as ICT disaster recovery testing. To assess testing and exercising of entity continuity plans, the ANAO examined the planning of exercises, post-exercise review, and the extent to which the reviews of exercises were used to revise BCPs.

Civil Aviation Safety Authority

5.4 Both the 2011 and 2013 CASA BCM frameworks emphasised the importance of regular exercising of the plan; including the planning, conduct, review and update process for the exercise schedule. The framework indicated that ongoing exercises would be scheduled, and that these exercises would follow a staged approach, which would commence with a walk through of plans. CASA considered that incrementally increasing the scope of exercises would progressively build the capability of staff and the usefulness of its plans. CASA's 2013 framework required:

Whether it is a simple exercise to validate a contact list, or a major simulation, all exercises must be recorded, reviewed, debriefed, the outcomes acted upon and verified, and the results maintained in an Exercise Register.⁹⁹

5.5 Testing scenarios and desktop reviews were also identified as risk treatment strategies in CASA's 2009 and 2013 risk management plans. The plans were silent regarding the type and frequency of exercises that should be conducted. Although testing and exercising expectations were established by CASA, a schedule of testing was not established.¹⁰⁰

5.6 CASA developed one testing scenario, in October 2013, but did not use the scenario to test its BCM arrangements. The scenario focused on the Headquarters BCP and the role of the Command Team. CASA advised the ANAO that undertaking scenario testing would not be cost effective, relative to the risk exposure. While no tests of overall BCM arrangements involving the Command Team have occurred, CASA has undertaken some testing of disaster recovery and emergency management. As outlined in Chapter 3, CASA's BCP focuses on critical systems and facilities, therefore disaster recovery testing concentrates on the most important element of CASA's BCM arrangements. ICT disaster recovery testing was most recently conducted in August 2012, in accordance with the May 2012 IT Disaster Recovery Plan. The report on the testing included issues, risks and recommendations regarding the infrastructure tested. In 2014, CASA advised that it conducted regular

99 CASA *Business Continuity Management Framework*, July 2013, p. 7.

100 CASA planned to test its emergency response arrangements, for example by planning fire drills.

out-of-hours testing of the Temporary Restricted Airspace hotline system, but also relied on unplanned outages to test its systems.¹⁰¹

5.7 CASA has also benefited from joint airport emergency exercises. For example, in April 2011, a major multi-agency exercise (involving Sydney Airport, NSW Police and a variety of other entities)¹⁰² was conducted to test the response to a plane crash. Lessons learnt from the exercise were documented, and CASA's Critical Occurrence Response Plan was updated. Overall, while CASA has tested some elements of its BCM arrangements, particularly its ICT disaster recovery, there is scope for CASA to improve its testing by developing and undertaking a program of testing its BCPs and critical functions.

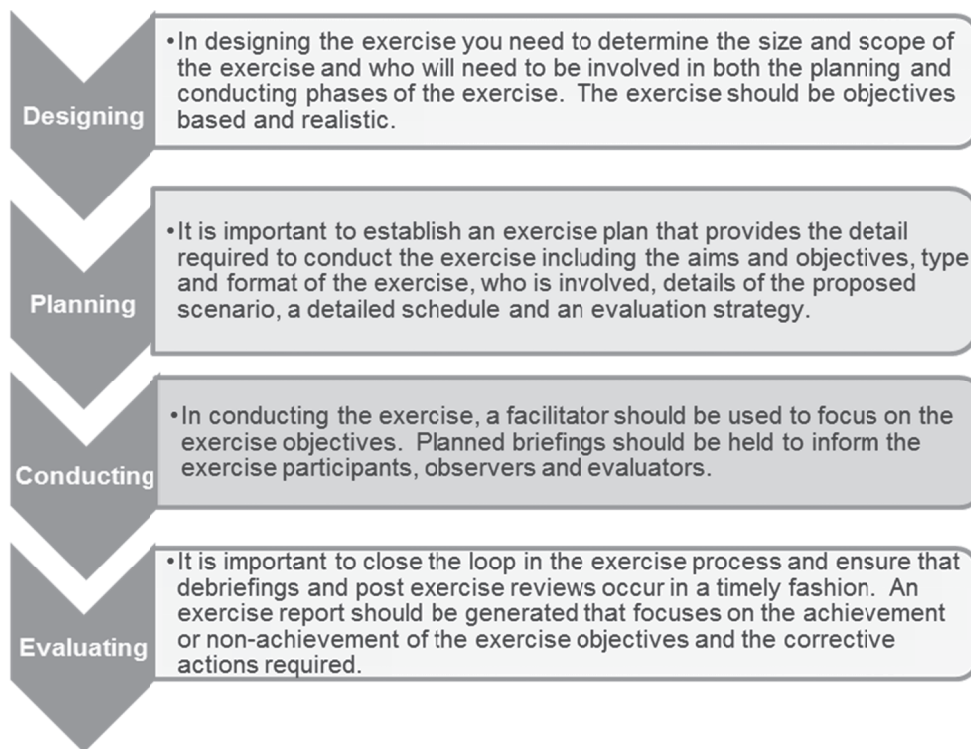
Department of Finance

5.8 Of the three entities audited, Finance had the most structured approach to testing its business continuity program, as well as the most comprehensive guidance for planning, conducting and reviewing exercises. Finance's framework established roles and responsibilities for exercises at the entity-wide level and then the critical function level. There was an expectation that the Control Team would undertake an annual exercise, while critical functions would be tested more frequently. To guide its overall approach, Finance developed an annual business continuity calendar which included a schedule for exercises, planning, and meeting with other entities that relied on Finance's critical systems. Finance's approach is set out in Figure 5.1.

101 Note that the Temporary Restricted Airspace hotline is the single most important critical function in CASA's operations. Business continuity issues for Temporary Restricted Airspace are managed separately to the entity-wide business continuity arrangements (see Table 4.1).

102 Participants in Exercise Capricorn included Sydney Airport personnel, the NSW Police Force, Fire and Rescue NSW, the Ambulance Service of New South Wales, NSW Health, the Australian Transport Safety Bureau, the Australian Federal Police, Sydney Airports Corporation Limited, Marrickville Council, Rex Regional Express Airlines and Airservices Australia.

Figure 5.1: Finance’s Exercise Management Process



Source: Finance, *Finance Business Continuity Management, 4. Maintenance of the Business Continuity Management Framework*, April 2013, p. 4.

5.9 Finance’s major business continuity exercise for 2012–13 was Exercise Sparky (see Table 5.1).

Table 5.1: Case study—Finance’s Exercise Sparky

Exercise Sparky tested Finance’s response to a power outage to its tenancies. It comprised three phases undertaken in 2012 and 2013:

- Phase One—the Central Control Team (CCT) declared a business interruption event and activated the departmental BCM arrangements;
- Phase Two—the communications strategies and decision-making processes used by the CCT and Enabling Services Advisors to effectively manage a coordinated response to the scenario; and
- Phase Three—Enabling Services Advisors separately convened members of their Recovery Team to practice their response.

This exercise:

- practiced a response to a whole-of-department interruption event;
- was planned in advance and articulated each phase’s aim, scope and objectives;
- was executed in accordance with its proposed plan;
- involved a range of BCM stakeholders within Finance and across various levels, including the Executive Board;
- documented the outcomes and action items of the phases; and
- identified follow-up of action items after the completion of the exercise.

Exercise Sparky provided the Executive Board and BCM stakeholders with insights into the level of assurance Finance’s BCM procedures provide in the event of a business interruption event. The exercise also highlighted areas for improvement to be followed up.

5.10 In addition to this overall exercise, some individual branches within Finance that were responsible for critical business functions also planned testing of their arrangements; some of these tests included other entities. For example, the Official Public Account administration team conducted business continuity testing at the Reserve Bank of Australia facilities, but the timing and results of this testing was not monitored centrally. In addition, a schedule of

testing and maintenance of Finance’s ICT disaster recovery plan was undertaken to ensure that it remained relevant.

Department of Social Services

5.11 DSS’s BCM policy and BCP set out expectations regarding testing and exercising the business continuity framework, including that a testing plan was to be developed and exercised annually. The BCM team had responsibility for exercise and testing of BCPs across the department, including for state offices. DSS required documentation to be maintained with respect to the implementation and testing of the business continuity policy. The DSS BCP was to be tested regularly to evaluate its effectiveness and capabilities.

5.12 Since 2008, DSS had generally scheduled an annual program of testing and review activities, which included a major, annual scenario test, known as ‘Iron Triangle’. Iron Triangle was designed to test selected areas of the department with a scenario based crisis and involved oversight by the Crisis Response Team. The earlier iterations of the exercise each involved recovering IT systems. The most recent exercise, which was completed in June 2012 (see Table 5.2), involved grants administration, ministerial support, and media and communications. The exercise was followed by a post exercise report, participant feedback, and recommendations. However, consistent with the discussion in relation to the DSS’s Queensland State Office stakeholder contact strategy (see paragraph 3.20), it is not clear that the revision sufficiently addresses the issues identified.

Table 5.2: Case study—Department of Social Services’ exercise Iron Triangle IV

The scenario primarily involved malware being detected on key funding and grant management systems, resulting in significant systems outages to isolate the problem and sanitise the systems.

The post exercise report identified a number of strengths in the department’s approach including responding to the media and prioritising issues and then resolving them. There were also opportunities to improve. These opportunities included: ensuring that when dealing with a disaster it was declared and communicated to the department; ensuring that the Crisis Response Team considers the wider implications of the disaster for the community as a whole; and ensuring there is a clearer understanding of the strategic issues, including consideration of Mission Critical Activities and their maximum acceptable outages in priority order, and whether BCPs are adequate in the circumstances.

In response to these issues, and the findings of an internal audit, DSS undertook a significant revision of their business continuity arrangements.

5.13 A business continuity exercise was not conducted in 2013. Developing a review program was delayed to allow for changes to the business continuity arrangements in response to an internal audit conducted in 2012. While DSS planned to undertake scenario testing of its new arrangements in November 2013, testing was further delayed by the Machinery of Government changes to the department in September 2013. After a two year gap in testing, in June 2014, DSS conducted Exercise Firefly. This exercise focused on the initial management of a business continuity event by the Crisis Response Team and Secretariat, as well as the resumption of critical processes in accordance with maximum allowable outages. A post exercise review was completed in July 2014 and identified opportunities to improve BCM arrangements including the operation of Crisis Response Team meetings, understanding roles and responsibilities, understanding the longer-term impact of the disruption and using BCPs.

5.14 As an important enabling resource, ICT systems that support critical functions should be regularly tested. DSS conducted an annual ICT disaster recovery test. Some post incident analysis was undertaken and the results of activities were reported to Executive Management Group. The test conducted in March 2013 indicated that disaster recovery processes for priority applications were in place and performed as required, but that there was scope to improve communications and planning.

5.15 The PSPF expects continuous review and testing of BCPs, which would include testing entity-wide, regional, branch and critical function BCPs. With the exception of ICT disaster recovery testing, DSS's tests and exercises were not sufficiently frequent or comprehensive to provide assurance on the business continuity arrangements. To better meet the expectations of the PSPF regarding testing its BCPs, DSS needs to ensure that it has a regular testing program in place.

Recommendation No.3

5.16 To provide assurance that business continuity plans are current and would operate as intended during a disruption, the ANAO recommends that CASA and DSS develop and undertake more comprehensive and regular testing of their business continuity arrangements.

Entity response

5.17 This recommendation was directed to CASA and DSS. Finance also commented.

Civil Aviation Safety Authority

5.18 *CASA accepts this recommendation and will develop a comprehensive program to enable testing of its business continuity arrangements and implement testing commensurate with the organisations risk appetite and cost benefit analysis practices.*

Department of Social Services

5.19 *Agreed. DSS conducted its annual testing in June 2014.*

Department of Finance

5.20 *Supported.*

Monitoring overall preparedness

5.21 All entities subject to the PSPF are required to undertake activities to monitor the entity's level of overall preparedness in the event of a business disruption event. Monitoring preparedness includes establishing key performance measures and targets to support assessments of whether business continuity arrangements are: current; provide adequate coverage; and BCP testing is planned and undertaken. Preparedness can also be informed by the results of internal audits and reviews.

5.22 CASA was the only entity to include incident and business continuity preparedness arrangements in its business continuity guidance. CASA identified six preparedness activities that should be undertaken and reviewed, including maintaining lists of key personnel, establishing succession plans for all managerial and operational key roles, maintaining up-to-date standard operating procedures for all business units, undertaking a vital records analysis to establish which hard copy records may be necessary in the event of an incident, developing a communication policy, and reviewing evacuation assembly points to ensure that they provide adequate protection for personnel (as well as undertaking evacuation exercises). While CASA's framework identified these preparedness activities, a number of the activities did not occur in practice, including a vital records analysis and maintaining complete contact lists.

5.23 Similarly, Finance and DSS had completed activities that would support preparedness, including updating BCPs and some testing of its arrangements. However, aspects of DSS’s approach could be more practical, for example, BCPs that contain procedures that were action focused rather than focused on developing further plans would better assist response teams when a disruption occurs (see paragraph 3.33). In addition, practical steps such as having up-to-date stakeholder contacts lists would further facilitate a timely response (see paragraph 4.7). These steps would ease the pressure on response teams and provide a level of assurance that priority functions are being managed.

Performance measures and targets

5.24 All three entities had made some effort to develop ways of measuring the performance of aspects of their BCM approach. CASA adopted a broader approach than Finance and DSS involving a mix of quantitative, qualitative and process measures (see Table 5.3). Although these measures were established, CASA did not collate data or report on the extent to which the performance measures were achieved. Finance and DSS developed a small number of indicators relating to the performance of certain processes. These indicators included updating framework documents and completing a training and testing program.

Table 5.3: Civil Aviation Safety Authority’s performance measures

<p>Event evaluation—quantitative measures:</p> <ul style="list-style-type: none"> • The incident is rectified within the Maximum Tolerable Period of Disruption; and • No severe insurable loss to disrupt CASA’s financial position. <p>Event evaluation—qualitative measure:</p> <ul style="list-style-type: none"> • No reputational damage as a result of an incident. <p>Preparedness process measures:</p> <ul style="list-style-type: none"> • All new projects are assessed with respect to business continuity impacts prior to initiation; and • The business impact analysis is reviewed when any new system is introduced or at least biennially.
--

Source: CASA Business Continuity Policy, September 2013.

5.25 Overall, only CASA identified activities to undertake and review to monitor preparedness, although it did not undertake all of the specified activities, and none of the entities reported on the performance of their BCM arrangements using the performance indicators that they had developed.

Audits and reviews

5.26 Regular internal audit or external reviews and evaluations of their business continuity program are further mechanisms for entities to obtain assurance over the effectiveness of their BCM arrangements.

Civil Aviation Safety Authority

5.27 Between 2009 and 2013, CASA has not audited its overall business continuity arrangements.¹⁰³ However, aspects of CASA's continuity planning have been updated approximately every two years since 2007. CASA's BCM framework, some regional BIAs, and all BCPs were most recently updated in 2013. Prior to this, the continuity framework and most business area BIAs were revised in 2011¹⁰⁴, following Cyclone Yasi.

Department of Finance

5.28 Since 2008, three internal audits of aspects of Finance's business continuity arrangements prompted significant re-focusing of Finance's BCM arrangements. These audits covered business continuity management in 2009, ICT Disaster Recovery Planning in 2010, and compliance with the PSPF in 2013. In response to the 2009 audit, critical functions were rationalised, the reporting framework for BCM was strengthened, and a schedule for updating BCPs was established, resulting in Finance developing a structured approach to continuously improving its business continuity strategies and plans.¹⁰⁵ The ICT Disaster Recovery audit focused on reviewing core recovery documentation, agreeing on recovery times with the relevant business areas, and testing the disaster recovery plan. The 2013 PSPF audit found that Finance was compliant with GOV 11.

Department of Social Services

5.29 A 2012 internal audit of DSS's business continuity arrangements prompted a cross-entity update of BCM arrangements. Recommendations from the audit related to updating BIAs, preparatory controls, governance, disaster response teams, testing, target recovery time and IT backup. In

103 CASA has undertaken some audits of IT systems which were a focus of CASA's BCM arrangements.

104 These arrangements were updated in 2013, although there have only been minor changes to the Framework and Policy. The 2011 BCM Strategy document indicated that there were a range of actions that needed to be completed for the strategy and plan to be effective.

105 This approach includes a schedule of key documents, templates and plans, BCM coordinator meetings and meetings to review arrangements with other entities.

response to this audit, DSS updated the BIAs and BCPs across the department in early 2013. By July 2013, DSS had also developed an overarching BCP.

Conclusion

5.30 In accordance with the PSPF, relevant Australian Government entities are expected to monitor their level of overall preparedness through exercising and review of their business continuity arrangements. While all entities subject to this audit undertook testing of their critical ICT systems, and CASA participated in joint exercises, only Finance had a comprehensive testing and exercising regime. This included post exercise reviews, with assigned actions, to incorporate improvements or revisions into the BCPs.

5.31 Both CASA and DSS identified the importance of regular exercising of the BCP. However, neither entity developed or had undertaken a business continuity exercising and testing program for 2012–13 or 2013–14, nor had they provided detailed guidance on how to structure, undertake and report on exercises and testing of the business continuity arrangements.

5.32 All of the entities could do more to monitor and report on their overall preparedness to manage and resolve business disruptions. In addition, DSS would benefit from developing a more proactive approach that better supports response teams during a disruption.



Ian McPhee
Auditor-General

Canberra ACT
6 November 2014

Appendices

Appendix 1: Entities' Responses



Australian Government
Civil Aviation Safety Authority

OFFICE OF THE DIRECTOR OF AVIATION SAFETY

CASA Ref: G114/1145

23 October 2014

Dr Andrew Pope
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
19 National Circuit
BARTON ACT 2601

Dear Dr Pope

Australian National Audit Office Business Continuity Management (BCM) audit

Thank you for your letter dated 22 September 2014 inviting the Civil Aviation Safety Authority (CASA) to respond to the ANAO proposed cross-agency report on Business Continuity Management. I am pleased to provide the following formal response on behalf of CASA:

Formal Response

CASA welcomes the ANAO's BCM audit report and agrees with the recommendations contained therein. CASA would like to emphasise that while it is not required to comply with the Protective Security Policy Framework (PSPF) it has actively sought to apply best practice principles from a variety of sources in developing and implementing its business continuity management (BCM) arrangements. This includes the adoption of important aspects of GOV 11 and a focus on applying a risk management approach to develop and implement a program which is tailored to CASA's business objectives and operating environment, risk based and relevant.

CASA accepts the ANAO findings and acknowledges that continuous improvement can be generated through the implementation of the recommendations contained in the report. As noted during the audit CASA deferred its planned BCM review until finalisation of this report and has now scheduled its review to commence this financial year. Included with the action plan in place for that review will be the implementation of these recommendations.

I would like to express my appreciation for the professional conduct of your team during the fieldwork and their willingness to consult with my management team throughout the process.

GPO Box 2005 Canberra ACT 2601

Telephone: (02) 6217 1001

Facsimile: (02) 6217 1555

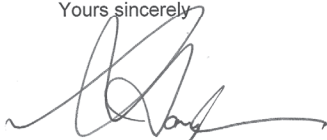
Response to recommendations:

	Recommendation	Response
1	To better support the recovery of critical functions, the ANAO recommends that CASA more systematically identify and prioritise critical functions, and document the relevant external and internal dependencies in their business continuity plans	CASA agrees with this recommendation.
2	To improve business continuity arrangements the ANAO recommends that CASA take a more systematic approach to analysing decisions and actions taken, and reviewing the effectiveness of business continuity management arrangements after the disruption.	CASA agrees with this recommendation.
3	To provide assurance business continuity plans are current and would operate as intended during a disruption, the ANAO recommends that CASA develop and undertake more comprehensive and regular testing of their business continuity arrangements	CASA accepts this recommendation and will develop a comprehensive program to enable testing of its business continuity arrangements and implement testing commensurate with the organisations risk appetite and cost benefit analysis practices.

Please find CASAs summary response at attachment A; and additional editorial commentary at attachment B.

Should you require further information on this matter, please contact Ross Barnes, Manager Governance Systems, Office of the Director of Aviation Safety on (02) 6217 1614.

Yours sincerely



Terry Farquharson
Director of Aviation Safety

Attachments:

- A. CASA summary response to the report
- B. CASA additional editorial commentary



Australian Government
Department of Finance

Jane Halton PSM
Secretary

Our Ref: SEC0010960

Dr Andrew Pope
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Pope

Thank you for your letter dated 22 September 2014, providing an opportunity for the Department of Finance to comment on the proposed Australian National Audit Office (ANAO) audit report on Business Continuity Management.

The Department of Finance notes the audit report and supports the recommendations. The Department also notes the case studies that involve the Department and agrees for the ANAO to include these in the report.

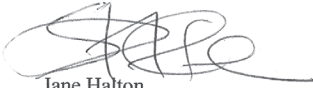
The following comments are made for inclusion in the report summary:

The Department of Finance acknowledges the findings of this report and supports the recommendations. The Department found the audit process to be a valuable exercise and appreciates the positive feedback provided by the ANAO on the Department's performance in relation to its business continuity management practices.

I appreciate the professional approach the ANAO adopted in dealing with Finance business groups during the audit process. The discussions between Finance staff and ANAO officers in the course of the audit will assist this Department further refine its approach to business continuity management.

If you have any further questions about the Department's response, please contact Mr Steve O'Loughlin, Assistant Secretary, Enterprise Management Office on (02) 6215 2757 in the first instance.

Yours sincerely

A handwritten signature in black ink, appearing to read 'J Halton', written in a cursive style.

Jane Halton
Secretary
2 October 2014



Australian Government
Department of Social Services

Finn Pratt PSM
 Secretary

Dr Andrew Pope
 Group Executive Director
 Performance Audit Services Group
 Australian National Audit Office
 GPO Box 707
 CANBERRA ACT 2601

Dear Dr Pope

Proposed audit report on Business Continuity Management.

Thank you for your letter dated 23 September 2014, providing the Department of Social Services (DSS) the opportunity to comment on the Australian National Audit Office's (ANAO) Section 19 Report for the Audit on Business Continuity Management.

DSS acknowledges the efforts of the ANAO to ensure that entities establish and manage sound Business Continuity practices.

I understand staff from the Audit Office have met with representatives from my department during an exit interview to discuss the audit's preliminary findings and proposed recommendations.

DSS agrees with the ANAO's three recommendations, and has provided details in the below attachments.

As per ANAO's request, DSS' response has been prepared in three parts:

1. Formal response and summary to the proposed report (Attachment A);
2. The Department's response to the Recommendations (Attachment B); and
3. A summary of actions from DSS' Business Continuity and Disaster Coordination transition plan (Attachment C).

Please do not hesitate to contact Helen Martin A/g Branch Manager responsible for the Department's Business Continuity Management on 02 6146 3417, if you have any queries on this matter.

Yours sincerely

Finn Pratt
 16 October 2014

PO Box 7576 Canberra Business Centre ACT 2610
 Email Finn.Pratt@dss.gov.au • Facsimile 02 6293 9692 • Telephone 02 6146 0010
 National Relay Service: TTY – 133 677, Speak and listen – 1300 555 727, Internet relay – www.relay.service.com.au
 www.dss.gov.au

Department of Social Services - Formal Response and Summary

Formal agency comments to be included in full as an appendix to the final report.

Formal Response to the Report

The Department of Social Services (DSS) welcomes the ANAO audit report on Business Continuity Management and supports the recommendations made by the ANAO.

DSS has put in place strengthened arrangements to provide a greater focus on business continuity management. This includes enhancements to the Critical Incident Response Team (CIRT) and supporting business continuity documents. Subsequent to the completion of the audit, DSS has combined the business continuity and disaster coordination functions, which further complements the coordination of its business continuity arrangements. It should be noted that a number of the issues identified have been or are being addressed.

DSS is committed to managing business interruptions that have the potential to affect its critical services and assets as well as the wider Australian community. DSS continues to refine its framework to ensure a well-developed, structured and robust business continuity program leading to improved organisational resilience.

SUMMARY of DSS' formal response

The Department of Social Services (DSS) welcomes the ANAO audit report on Business Continuity Management and supports the recommendations made by the ANAO.

DSS is committed to managing business interruptions that have the potential to affect its critical services and assets as well as the wider Australian community. DSS continues to refine its framework to ensure a well-developed, structured and robust business continuity program leading to improved organisational resilience.

Appendix 2: Civil Aviation Safety Authority’s Key Systems and Facilities

CASA’s key systems and facilities are identified through its business impact analysis process. These systems and facilities have target recovery times ranging from non-stop to 48 hours.

Item	System or Facility	Recovery time
1	TRA Hotline—Temporary Restricted Airspace	Non-stop
2	Laptop PC with CASA SOE and wi-fi capability to VPN	Non-stop
3	Landline telephones—CASA exchanges	4 hours
4	CASA website	4 hours
5	Email—OWA—Outlook Web Access	4 hours
6	Internet access	4 hours
7	Sat phones	4 hours
8	FAX capability	24 hours
9	Email—CASA network	24 hours
10	Networked PCs with CASA SOE	24 hours
11	TRIM—Total Records Information Management	24 hours
12	AIRS—Aviation Industry Regulatory Systems (managed by Accenture)	24 hours
13	MRS—Medical Records System	24 hours
14	FMIS—Financial Management Information System	24 hours
15	CCM—Complex Case Management	48 hours
16	AvMed PHID—Aviation Medicine Photo ID	48 hours
17	DAME—Designated Aviation Medical Examiner	48 hours
18	WMS—Workflow Management System	48 hours
19	eRoom	48 hours
20	LARP—Licensing, Aircraft Registrations and Publications	48 hours
21	ChangePoint—(especially DTAR and OTAR)	48 hours
22	TESS—HR Travel—The Employee Self-Service	48 hours
23	HRMS—Human Resources Management System	48 hours

Source: CASA BCP July 2013, Appendix 1.

Appendix 3: Department of Finance’s Critical Functions

Critical functions are functions that must be restored or achieved during a business interruption event. These functions generally require continuity within 5 days of the interruption.

Critical Function	Maximum allowable outage
COMCAR—Reservations and Allocations and Driving Operations.	1 day
Provision of Parliamentary Entitlements Services to Senators and Members.	5 days
Non-Defence Domestic Property Portfolio Building Management Services.	1 week
Management and development of australia.gov.au portal website.	1 week
Communications Systems including MCN, TelePresence, FWAN.	1 day
Administration of the Secret Budget Network (BudgetLAN) network.	5 days
Management and development of Govdex websites.	1 week
Contract management and administration of the Intra-government Communications Network (ICON).	1 week
Supporting the government in the preparation and ongoing management of the Budget (along with the Department of the Treasury).	1 day
Providing policy advice on whole-of-government expenditure priorities and providing budget expense estimates and non-taxation revenue estimates updates, in cooperation with other agencies.	1 day
Distribution of Cabinet documents and coordination of departmental comments.	2 days
Payroll Processing.	2 days
Cash Drawdowns and Payments.	2 days
Control and monitor the movement of funds through the Official Public Account—Cash Management.	1 day
Budget, Mid-Year Economic and Fiscal Outlook (MYEFO) and Pre-Election Fiscal Outlook (PEFO) consolidation—Monthly and annual consolidated financial statements.	1 day
Administer the Parliamentary Contributory Superannuation Scheme (PCSS), the Governors-General pension scheme, the Judges' pensions scheme and superannuation arrangements for Federal Magistrates.	1 week
Maintaining the time-critical support function for whole of Australian government electronic tendering (AusTender).	N/A

Appendix 4: Department of Social Services' Critical Functions with a Major or Extreme Impact Rating

DSS used a rating scale to assess its priorities where a rating of '1' was considered to have an insignificant impact¹⁰⁶, and a rating of '5' was considered to have an extreme impact. The following table lists the 57 critical functions where DSS had assigned an impact rating of major or extreme. An extreme impact rating of '5' reflects situations resulting in multiple deaths, national public outrage, or critical business failure, preventing performance of core activities. A major impact rating of '4' reflects situations resulting in death, loss of significant proportion of financial assets, local public outrage and political criticism, a Parliamentary inquiry, breach of regulations, or a breakdown of key activities leading to reduction in business performance.

Business Activity/Process	Impact rating	Recovery time
Provide secretariat support for the standing council for community and disability services Social Security, Relationships and International Branch	5	<24 hours
Provide advice to Minister Social Security, Relationships and International Branch	5	<24 hours
Briefs and Ministerials Northern Territory Office—Katherine Indigenous Coordination Centre	5	<24 hours
Liaison role with DHS Social Security, Relationships and International Branch	5	<24 hours
Tuggeranong Office Park Data Centre Property, Environment, Procurement and Security Branch	5	<24 hours
Workplace health & safety of all regional place based staff Northern Territory Office—Katherine Indigenous Coordination Centre	5	<24 hours
Provide secretariat support to the Crisis Response Team Financial Management Branch	5	<24 hours
Briefs and Ministerial Western Australia State Office	5	1–2 days

106 For example, an insignificant impact might involve situations resulting in minor injury, internal dissent, or minimal impact on non-core operations.

Business Activity/Process	Impact rating	Recovery time
Intelligence coordination Queensland State Office	5	1–2 days
Briefs and Ministerial New South Wales/Australian Capital Territory State Office	5	1–2 days
Process payroll Financial Accounting Branch	5	1–2 days
Preparation of payment files for payroll function Corporate and Data Services Branch	5	1–2 days
FaHCSIA property management staff housing Northern Territory Office—Katherine Indigenous Coordination Centre	5	1–2 days
Assurance of accurate and timely payments for grants, including Social and Community Services workers award payments Program Establishment & Management Branch	5	1–2 days
Release of funds to Centrelink Financial Accounting Branch	5	3 days
Capacity Strengthening and Support Services to support shortlisted Remote Jobs and Communities Program applicants Northern Territory Office—Programs Branch	5	3–7 days
RJCP Community Development Fund Northern Territory Office—Programs Branch	5	3–7 days
Release regular payments (grants and invoices) Financial Accounting Branch	5	3–7 days
Community Development Employment Projects program transition to Remote Jobs and Communities Program Northern Territory Office—Programs Branch	5	5 days
Enable the provision of advice to Ministers and the Executive Ministerial, Parliamentary and Executive Support Branch	4	<24 hours
To enable costings to be created to respond to urgent need and to facilitate payments to customers by Department of Human Services Budget Development Branch	4	<24 hours
Issue management of food security risks Northern Territory Office—Community Stores	4	<24 hours
Rates Indexation Policy Modelling, Evaluation & Capability Branch	4	<24 hours

Business Activity/Process	Impact rating	Recovery time
Remote Staff Coordination South Team—Monitor duty phone for out of hours support and Emergency Position Indicating Radio Beacons activation Northern Territory Office—Southern Region Government Engagement Coordinators, Indigenous Engagement Officers	4	<24 hours
Provide timely advice to General Manager and Chief Operating Officer on the impact of disasters (or potential disasters) on FaHCSIA's staff and assets Financial Management Branch	4	<24 hours
Urgent ministerial support Family Payments and Child Support	4	1–2 days
National Partnership Agreement on Homelessness discussions Commonwealth State Relations Branch	4	1–2 days
Annual reporting of Ministerial grants Program Establishment and Management Branch	4	1–2 days
Formal external reporting and information about funded organisations Program Establishment and Management Branch	4	1–2 days
Issues management Western Australia State Office	4	1–2 days
Program management Northern Territory Office—Katherine Indigenous Coordination Centre	4	1–2 days
Issue and crisis management Victoria State Office	4	1–2 days
Issue and crisis management Tasmania State Office	4	1–2 days
Deliver major selection processes for new Personal Helpers and Mentors (PHaMs) services; PHaMs Employment services; new Family Mental Health Support Services; and expansion of Mental Health Respite: Carer Support Services Mental Health Branch	4	1–2 days
Enable the relocation of Ministers and key staff in support of the continuity of Government plan Ministerial Support Ministerial, Parliamentary and Executive Support Branch	4	1–2 days
Manage security electronic access control and alarm system for National Office and Network Property, Environment, Procurement and Security Branch	4	1–2 days

Business Activity/Process	Impact rating	Recovery time
Assistance to the Australian National Audit Office Financial Statements Audit of administered grants Program Establishment and Management Branch	4	1–2 days
Program guideline gateway to the Department of Finance and Deregulation Program Establishment and Management Branch	4	1–2 days
State Manager functions Northern Territory Office—Alice Springs Indigenous Coordination Centre	4	1–2 days
Government Engagement Coordinators/Indigenous Engagement Officers staff accommodation and vehicles Northern Territory Office—Katherine Indigenous Coordination Centre	4	1–2 days
Safety Breach (death or serious injury) Remote Housing Northern Territory Branch	4	1–2 days
Develop and undertake 2013 selections Program Office Branch	4	1–2 days
Building security (system) Northern Territory Office—Alice Springs Indigenous Coordination Centre	4	1–2 days
Building services/facilities Northern Territory Office—Alice Springs Indigenous Coordination Centre	4	1–2 days
Agreement renewals Western Australia State Office	4	3–7 days
Issues management New South Wales/Australian Capital Territory Office	4	3–7 days
Briefing for Minister and Executive attendance OECD Strategic Policy Branch	4	3–7 days
Provision of advice and recommendations to the Minister and the department in respect of the operation of the <i>Aboriginal Land Rights (Northern Territory) Act 1976</i> and other Commonwealth and NT legislation Northern Territory Office—Land Section	4	3–7 days
Progress development of Program Delivery Model work packages Program Office Branch	4	3–7 days
Agreement renewals and program payment releases to providers and State Government New South Wales/Australian Capital Territory Office	4	3–7 days

Business Activity/Process	Impact rating	Recovery time
Contract management Queensland State Office	4	3–7 days
Contract management—Release payments Northern Territory Office—Alice Springs Indigenous Coordination Centre	4	3–7 days
Contract management—Stakeholder engagement Northern Territory Office—Alice Springs Indigenous Coordination Centre	4	3–7 days
Production support major applications (e.g. FOFMS, SAP) IT Operations Branch	4	3–7 days
ICT Network support IT Operations Branch	4	3–7 days
Network Branch Manager functions Northern Territory Office—Alice Springs Indigenous Coordination Centre	4	3–7 days
Remote Staff Coordination South Team—Manage Australian Government complex accommodation bookings Northern Territory Office - Southern Region Government Engagement Coordinators, Indigenous Engagement Officers	4	3–7 days

Source: *DSS BCP*, June 2013, Appendix 1.

Index

A

Activation, 21, 23, 29, 37, 44, 51, 71,
74–76, 78–79, 85, 111

C

Contact list, 44, 50, 68, 70–71, 76–77, 88,
94

D

Dependencies, 19, 20, 53–55, 60–64, 66,
69, 72

Disaster recovery plan, 29, 31, 34, 40,
50, 84, 92, 96

E

Emergency management, 40–41, 50,
75–76, 88

I

Incident record, 41, 74–75, 77–78, 82, 85

M

Maximum allowable outage, 21–22, 45,
47, 51, 53–54, 56, 59–60, 65–68, 72, 75,
77, 92–93, 96, 107–108

P

Protective Security Policy Framework,
19, 22, 30–35, 38–39, 43, 48, 50, 53–54,
60, 68, 73, 87, 93–94, 96

R

Recovery kits, 39, 44, 70–71, 75–76

Recovery team, 77, 91

command team, 48, 69, 74–75, 78, 88

control team, 42, 48, 51, 70–71, 75–76,
87, 89, 91

crisis response team, 48, 75–77,
79–80, 92–93, 109

response team, 39, 48, 51, 61, 70–71,
75–76, 79, 87, 93, 95–96, 97

V

Vital records, 33, 53, 56, 60–64, 94

W

Workarounds, 55–56, 58, 60, 66, 68–69,
79

Series Titles

ANAO Report No.1 2014–15

Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2013 Compliance)

Across Agencies

ANAO Report No.2 2014–15

Food Security in Remote Indigenous Communities

Department of the Prime Minister and Cabinet

ANAO Report No.3 2014–15

Fraud Control Arrangements

Across Entities

ANAO Report No.4 2014–15

Second Follow-up Audit into the Australian Electoral Commission's Preparation for and Conduct of Federal Elections

Australian Electoral Commission

ANAO Report No.5 2014–15

Annual Compliance Arrangements with Large Corporate Taxpayers

Australian Taxation Office

ANAO Report No.6 2014–15

Business Continuity Management

Across Entities

Better Practice Guides

The following Better Practice Guides are available on the ANAO website:

Successful Implementation of Policy Initiatives	Oct. 2014
Public Sector Governance: Strengthening Performance through Good Governance	June 2014
Administering Regulation: Achieving the Right Balance	June 2014
Implementing Better Practice Grants Administration	Dec. 2013
Human Resource Management Information Systems: Risks and controls	June 2013
Preparation of Financial Statements by Public Sector Entities	June 2013
Public Sector Internal Audit: An investment in assurance and business improvement	Sept. 2012
Public Sector Environmental Management: Reducing the environmental impacts of public sector operations	Apr. 2012
Developing and Managing Contracts: Getting the right outcome, achieving value for money	Feb. 2012
Public Sector Audit Committees: Independent assurance and advice for chief executives and boards	Aug. 2011
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities: Delivering agreed outcomes through an efficient and optimal asset base	Sept. 2010
Planning and Approving Projects – an Executive Perspective: Setting the foundation for results	June 2010
Innovation in the Public Sector: Enabling better performance, driving new directions	Dec. 2009
SAP ECC 6.0: Security and control	June 2009
Business Continuity Management: Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
