The Auditor-General
Audit Report No.53 2002–03
Business Support Process Audit

Business Continuity Management Follow-on Audit

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 80714 0

Australian National
Audit Office

Canberra ACT
23 June 2003

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a business support process audit across agencies in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Business Continuity Management Follow-on Audit.*

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

Yours sincerely

P. J. Barrett
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

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

http://www.anao.gov.au

Audit Team

Richard Rundle
Samantha Montenegro
Ben Sladic

Contents

Abbreviations

ANAO	Australian National Audit Office
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BPG	Better Practice Guide
CEO	Chief Executive Officer
DRP	Disaster Recovery Plan
MAO	Maximum Acceptable Outage

Glossary

Where possible, definitions have been sourced from the ANAO's Better Practice Guide on Business Continuity Management, and the Australian and New Zealand Standard on Risk Management (AS/NZ 4360:1999). Further explanation and examples have also been provided for some of the key terms to assist the user of this report to understand the terminology.

Business Continuity Management (BCM)—The framework of controls implemented, and steps undertaken, by an organisation to manage its business continuity risks. The primary objective of these controls is to ensure the uninterrupted availability of its key business resources that support key (or critical) business processes.

Business Continuity Plan (BCP)—A collection of documents, which outline the organisation's preferred approach to dealing with disruptions to key business processes. The key documents that generally comprise the BCP include the: business group (or service area) recovery plans; disaster recovery plans; emergency response and evacuation procedures; backup and recovery procedures; and communication and media liaison strategies. Collectively, these documents detail information critical to determining the: declaration point of a disaster; immediate response procedures; minimum level of resources necessary to support a degraded level of service from the key business processes; method of operation in the interim period (between disaster declaration and the restoration of normal operations); and disaster recovery procedures necessary to restore or recover lost business functions.

Business continuity plan—Documents the objectives, scope, boundaries and resources of the project to establish the BCM framework.

Business group recovery coordinator—Coordinates the business group or service area recovery teams and reports to the Recovery coordinator.

Business Impact Analysis (BIA)—The BIA is undertaken for all key business processes and establishes the recovery priorities, should the processes be disrupted or lost.

Business interruption event/Outage—A business continuity risk event that has a business interruption consequence, causing a disruption to, or loss of, key business processes for a period of time that is unacceptable to the organisation.

Business operations—The total collection of business processes, which support the delivery of the organisation's outputs and outcomes. These may be strategic, operating or support processes.

Business processes—A series of business activities or actions combining to produce an identifiable output and/or result.

Continuity treatment—Treatments designed to minimise the effects of disruptions to each key business process.

Declaration point—The point where the timeframe for the restoration of the business function is greater than the MAO.

Disaster—An outage that exceeds the MAO.

Downtime—May occur as a part of normal operations where the impact simply reduces the effective utility of processes in the short term.

Emergency management—A range of controls and procedures to manage risks to the business associated with disasters and emergencies. It involves developing and maintaining arrangements to prevent or mitigate, prepare for, respond to, and recover from emergencies and disasters.

Event log—Documents the details of an outage. It should be used to review the adequacy of existing controls and identify areas for improvement.

Key business processes—Key business processes are those processes essential to the delivery of outputs and achievement of business objectives. Business activities and resources are the essential elements that combine to make up each key business process.

Maximum Acceptable Outage (MAO)—The MAO is the time it will take before a business interruption event threatens an organisation achieving its business objectives. The MAO defines the maximum time an organisation can survive without key business functions before business continuity plans and recovery procedures must commence.

Recovery and management teams—Business group or service area teams responsible for the implementation of BCP, and recovery of business processes, following an incident.

Recovery coordinator—Coordinates the various recovery and management teams and reports directly to senior management.

Recovery organisation—Describes the BCM structure in place within an organisation and consists of three main layers: Recovery coordinator; Recovery and management teams; and Recovery plan support processes.

Recovery plan—The plan that outlines the actions necessary to support the management and technical recovery plans, including human resource management and communication.

Resources—Resources are the means that support delivery of an identifiable output or result. Resources may be money, physical assets or, most importantly, people. Without resources, activities (and therefore processes) would fail.

Resumption planning—Planning for the resumption of services and associated functions following a disruption.

Risk event—Any non-trivial event that affects the ability of an organisation to achieve its business objectives.

Risk management—The systematic application of management policies, procedures and practices to the tasks of identifying, analysing, evaluating, treating and monitoring risk.

Risk register—Comprehensive inventory of risks across the organisation.

Risk treatment—Appropriate intervention strategies for dealing with risk. Treatments are designed to limit the likelihood or impact of the event on the resource at risk. These strategies may include administrative or security procedures, back-up and restoration procedures, or training and awareness programs for staff.

Senior management—The layer of management in an organisation that makes decisions about direction, focus, policy and corporate governance.

Summary and Recommendations

Summary

The importance of Business Continuity Management

ANAO Better Practice Guide

1. In January 2000, the ANAO published a Better Practice Guide *Business Continuity Management—Keeping the wheels in motion* [the Better Practice Guide].[1] The Better Practice Guide was published in response to concern over the ability of Commonwealth organisations to deliver services critical to the economic and social well-being of our society due to the impacts of business interruption events.[2]

2. Chapter 1 of this Report provides a more detailed discussion of the:

- history and purpose of the Better Practice Guide;
- key components of a fully operational Business Continuity Management (BCM) framework; and
- relationships between corporate governance, risk management, BCM and other related disciplines such as disaster recovery and emergency management.

3. The Glossary is also a useful point of reference, as it explains some of the terminology used in this Report.

This follow-on audit

4. The primary objective of this audit was to examine BCM arrangements across four Commonwealth organisations, to assess whether their existing BCM frameworks (or frameworks under development) exhibit the principles espoused in the Better Practice Guide.

5. The ANAO also made a number of suggestions for improvements to these organisations, where gaps were identified between existing BCM arrangements, or BCM framework development approaches, and the principles outlined in the Better Practice Guide. At the Commonwealth-wide level, the ANAO reviewed the continuing relevance of the principles presented in the Better Practice Guide.

---

[1] Australian National Audit Office, *Business Continuity Management—Keeping the wheels in motion*, Canberra, 2000.

[2] ibid., p 3.

Key findings

6. The following key findings are based on observations made in the organisations audited. They address the audit evaluation criteria, and reflect that the level of maturity of BCM in Commonwealth organisations is still in its formative stages.

Assessing business continuity risk

7. The ANAO found that all organisations had commenced, or completed, risk assessments that identified their business continuity risks. However, only two organisations had documented business continuity as a risk priority in their current organisation-wide risk management plans. The ANAO also found that some organisations assessed business continuity risks within 'silos', at the operating group level. There was an inability to demonstrate that these assessments were being considered at an organisation-wide level to ensure that priorities and treatments (controls and plans) were consistent.

8. Only one organisation could demonstrate that it had established a link between corporate governance, risk management and BCM.

9. All organisations could establish more effective management committees to oversight the BCM framework. They could also better clarify the responsibilities for undertaking business continuity development and implementation tasks.

10. The ANAO found that none of the organisations had documented a policy statement that fully articulated their expectations of a BCM framework.

Implementing the BCM arrangements

11. The ANAO found that only two organisations had identified, documented and prioritised their key business processes in sufficient detail to assist with BCM, and could provide evidence of senior management's review of this work.

12. The ANAO found that all organisations could improve the manner in which they undertake Business Impact Analyses (BIAs) and document their assessments. While three organisations had undertaken some work on their BIAs, they had not identified critical success factors, resource requirements, interim processing procedures and maximum acceptable outage periods for each of their key processes. In addition, organisations did not maintain sufficient documentation to ensure the validity or robustness of their assessments.

13. The ANAO found that all organisations could improve the manner in which they undertake and document their identification, evaluation and selection

of the most appropriate mix of controls and plans to manage their business continuity risks, not only for accountability purposes but also for the information of stakeholders.

Maintaining the Business Continuity Plan (BCP)

14. The ANAO found that only one of the organisations audited had drafted a BCP that identified the organisation's requirements and approach for the continuity of key processes in the event of a business interruption event. That organisation's BCP also outlined BCM responsibilities and detailed the disaster escalation procedures, which were supported through the use of event logs. The other organisations had developed guidance in relation to disaster recovery and emergency management requirements, but could not demonstrate that they had developed a BCP or identified organisation-wide interim processing procedures, at least for their own confidence.

15. Two organisations had attempted to create comprehensive references to other relevant controls and plans in their BCP, or disaster recovery and emergency management plans. However, some organisations had incomplete references and used inconsistent terminology across these plans, indicating a lack of management controls and review. In addition, the ANAO found that, for organisations with geographically dispersed locations, there were inconsistencies and inaccuracies in some site-specific plans and procedures. This may compromise the effectiveness of the controls and plans, due to confusion over applicability and responsibilities of those concerned.

16. None of the organisations had established:

- the disaster declaration point for the activation of their BCM arrangements;
- sufficient lists of resource requirements;
- the BCP's limitations and assumptions; and
- testing and maintenance schedules.

Organisations also needed to develop and provide BCM education programs to relevant staff.

17. None of the organisations audited were at the stage where they were testing and maintaining their BCPs as outlined in the Better Practice Guide. However, the ANAO found that organisations had developed procedures to periodically test aspects of their disaster recovery and emergency management arrangements. These testing arrangements, together with adherence to principles outlined in the Better Practice Guide, will complement testing arrangements for the BCPs, once they are developed.

Developments since the release of the Better Practice Guide

18. The Better Practice Guide has been available to Commonwealth organisations since January 2000. Organisations that had established their BCM arrangements (frameworks, controls and plans) prior to the release of the Better Practice Guide, may not exhibit some of the principles espoused in the Better Practice Guide. The ANAO has taken account of this when assessing organisations, and noted this in the individual conclusions for the organisations covered in this audit.

19. Organisations expressed some reservations with the level and nature of guidance available in the Better Practice Guide. In particular, they considered that the Better Practice Guide was directed at large-sized organisations, which have substantial resources (specifically, staff and budgets) available to address the extensive level of work recommended in the Better Practice Guide. They also indicated that they did not feel it was possible or practical to estimate the impact of a multitude of possible business interruption events, and how these events may impact on business operations (specifically, the resources applied).

20. The ANAO notes that the Better Practice Guide was developed to provide assistance to a variety of organisations (ranging from small to large-sized, and from policy to service delivery organisations). As such, the guidance contained within the Better Practice Guide may need to be considered in light of the size, operational requirements and priorities of the organisation.

21. The ANAO considers that the adequacy and appropriateness of the BCM arrangements should be reviewed regularly, in line with the organisation's requirements, priorities, and environment. In particular, organisations may also need to consider the role of BCM in managing the impacts of the emerging risks of international terrorism and threats against public officers and/or Commonwealth assets.[3] These reviews may lead to re-structuring or refinement of existing BCM arrangements.

22. The ANAO encourages organisations to refer to the Better Practice Guide and other recent relevant guidance (for example, from organisations such as Emergency Management Australia[4] and the Business Continuity Institute[5]) when establishing and reviewing BCM arrangements.

---

[3] Such as the 11 September 2001 and 12 October 2002 terrorist attacks, and the January 2003 Canberra bushfires.

[4] Emergency Management Australia, *Non-stop service: continuity management guidelines for public sector agencies*, Canberra, 1997.

[5] The Business Continuity Institute, *Business Continuity Management: Good Practice Guidelines*, 2002. Available at < www.thebci.org/frametrial.html>.

Overall conclusion

23. The ANAO concluded that the principles espoused in the Better Practice Guide remain relevant to Commonwealth organisations when considering business continuity risks. The Better Practice Guide also continues to provide useful information to assist organisations to establish and maintain BCM frameworks, controls and plans.

24. All organisations audited had implemented a number of preparatory controls to minimise the likelihood that their identified business continuity, and related, risks would impact adversely on their business operations. Most organisations rely on existing disaster recovery and emergency management plans to re-establish their operations in a timely manner following a business interruption event. However, these plans tend to be developed by, and therefore, focused on, specific operating groups and their processes (such as Information Technology [IT]) and securing resources following a business interruption (emergency response). They do not contain, or refer to, interim processing procedures designed to enable the uninterrupted availability of business resources and activities.

25. The ANAO concluded that organisations generally experienced difficulties when developing and implementing BCM arrangements due to:

- incomplete business continuity risk assessment and analysis processes;
- not clearly articulating the assumptions and limitations of the BCM arrangements in the BCM policy statement so the expectations regarding the applicability and adequacy of the BCM framework are realistic;
- not fully understanding the difference between the objectives of disaster recovery, emergency management and BCM, or how the work undertaken during each of these processes may best be related; and
- not maintaining adequate documentation in support of this work.

26. In addition, the ANAO concluded that one of the continuing problems with the approach to BCM observed in the organisations audited was that they did not recognise that BCM is an ongoing process. Organisations should be continually reviewing the effectiveness and efficiency of their BCM arrangements in light of changes to their operating and external environments.

27. Organisations have demonstrated that they are referring to, and in some instances applying, better practice guidance. However, they sometimes experience difficulty in undertaking the steps involved. The ANAO considers that BCM should not be a complex or cumbersome process for organisations. Fundamentally, organisations should be able to demonstrate that they have taken a structured approach to considering:

- the events (or risks) that may affect their business operations;
- how each event will impact business resources and activities; and
- how each event may be prevented or controlled.

Organisation responses

28. Each of the organisations in the audit was issued with a management report detailing conclusions against the principles outlined in the Better Practice Guide, including recommendations for improvement, where necessary. The organisations have agreed to their individual findings and recommendations, and have advised of action being taken to improve developing or existing BCM arrangements.

Supplement(s) to the Better Practice Guide

29. The ANAO intends to develop supplementary guidance during the 2003–2004 financial year to support organisations in the use of the Better Practice Guide. This guidance will reflect any updates to better practice principles, as well as incorporate more case studies and practical examples from private and public sector organisations to assist Commonwealth organisations with the application of the principles.

Recommendation

As a result of comparing existing BCM arrangements, and BCM development approaches, in the Commonwealth organisations examined, with currently identified better practice, the ANAO has included the following recommendation, which applies to all organisations.

Recommendation No.1

The ANAO recommends that Commonwealth organisations consider relevant better practice guidance when assessing their business continuity risks and developing their BCM arrangements (framework, controls and/or plans). In particular, organisations should ensure that they:

- identify, assess and prioritise business continuity risk as part of the organisation-wide risk management approach. This will aid in ensuring that they have established all events (or risks) across the organisation that may affect business operations, processes and resources, and that senior management support the treatment of identified risks;
- outline the assumptions and limitations of the BCM arrangements in the BCM policy statement so the expectations regarding the applicability and adequacy of the BCM framework remain realistic;
- maintain complete and current documentation of their understanding of their key business processes, business activities and resource requirements;
- undertake a business impact analysis to determine how each business continuity event will impact on their business processes, business activities and resources; and
- identify, evaluate, select and document an appropriate, supportable, and effective set of controls and plans, which are consistent with the organisation's operating and identified risk priorities.

Organisations also need to adequately document the analysis and findings from the steps in the BCM process, as well as regularly review and test the BCM arrangements to ensure that they remain relevant to the organisations' evolving operating environments and identified risk priorities.

Audit Findings and Conclusions

1. Introduction

This chapter explains the impetus for the development of the Better Practice Guide on Business Continuity Management (BCM), and outlines the relationship between corporate governance, risk management, BCM and other related disciplines, including disaster recovery and emergency management. It also provides an overview of the structure of this Report.

The Better Practice Guide

1.1 The Better Practice Guide[6] was published in response to heightened interest in business continuity issues, and the concern over the ability of Commonwealth organisations to provide continued service in the light of the Year 2000 bug. The Better Practice Guide also sought to assess and provide advice on all aspects of BCM efforts of organisations, with significant emphasis on:

- identification, analysis and prioritisation of business continuity risks as part of the organisation-wide risk management process;
- development, selection and implementation of treatments (controls and plans) to address the business interruption consequences that may arise from the realisation of a business continuity risk; and
- documentation, testing and revision of business continuity controls and plans.

1.2 The Better Practice Guide established that the objective of BCM is to ensure the uninterrupted availability of all key business resources required to support essential (or critical) business activities.[7] This is achieved by organisations building resilience (controls and redundancy) into business operations to prevent, or minimise, the likelihood of business continuity risks occurring and, also, developing plans that minimise the impact should they occur.

1.3 Consequently, BCM is not restricted to the disaster recovery issues traditionally associated with information technology. Instead, BCM involves the identification, analysis and prioritisation of business continuity risks across the organisation, and the development and implementation of preventative controls that can be routinely managed. It also involves the documentation, in a Business

---

6 Australian National Audit Office, op. cit.

7 ibid., p. 12.

Continuity Plan (BCP),[8] of procedures and strategies to deal with business interruptions to key business processes should the preventative controls fail.

BCM relationships

BCM, risk management and corporate governance

1.4 Effective governance makes management accountable to its many stakeholders, through appropriate management structures, reporting requirements, control structures, performance measures and the many other elements of corporate governance.[9]

1.5 Risk management is the term applied to a logical and systematic method of establishing the risk context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organisations to minimise losses and maximise opportunities. Risk management is considered to be an integral part of good management practice.[10]

1.6 Each Commonwealth organisation, as part of its corporate governance responsibilities and, more specifically, risk management practices, should establish an appropriate BCM framework to support its key business functions.[11] Within this framework, unacceptable business continuity risks[12] should be identified and managed with appropriate controls and plans.

---

[8] A collection of documents, which outline the organisation's preferred approach to dealing with disruptions to key business processes. The key documents that generally comprise the BCP include the: business group (or service area) recovery plans; disaster recovery plans; emergency response and evacuation procedures; backup and recovery procedures; and communication and media liaison strategies. Collectively, these documents detail information critical to determining the: declaration point of a disaster; immediate response procedures; minimum level of resources necessary to support a degraded level of service from the key business processes; method of operation in the interim period (between disaster declaration and the restoration of normal operations); and disaster recovery procedures necessary to restore or recover lost business functions.

[9] P Barrett, *Expectation, and Perception, of Better Practice Corporate Governance in the Public Sector from an Audit Perspective,* Address to the CPA Australia's Government Business Symposium, Melbourne, 2002.

[10] Joint Standards Australia/Standards New Zealand Committee on Risk Management, *Australian and New Zealand Standard 4360:1999—Risk Management*, Standards Australia, 1999, p. 1.

[11] While there is not a specific requirement under the legislation, it is an implied requirement for the agency head under the *Financial Management and Administration Act 1997*. The importance of risk management and business continuity planning has also been highlighted over the past 12 months in publications and briefings, including the Attorney-General's briefing papers of May 2002.

[12] These risks generally relate to the availability of resources such as staff, utilities or infrastructure.

BCM, emergency management and disaster recovery

1.7 The BCM framework should not be developed in isolation from the other activities which seek to minimise the likelihood, or control the impact, of adverse risk events. The controls selected to deal with business continuity risks may impact on, or be supported by, controls designed to treat other related risks faced by the organisation. Therefore, organisations need to have a sound understanding of the relationships between their:

- business operation and risk management priorities;
- key business processes, business process interdependencies and the resource requirements to support these processes; and
- existing management frameworks, controls and plans;

in order to determine whether they need to develop a BCM framework, including controls and plans which complement (but do not duplicate) other management frameworks.

1.8 The key components of a fully operational BCM framework include:

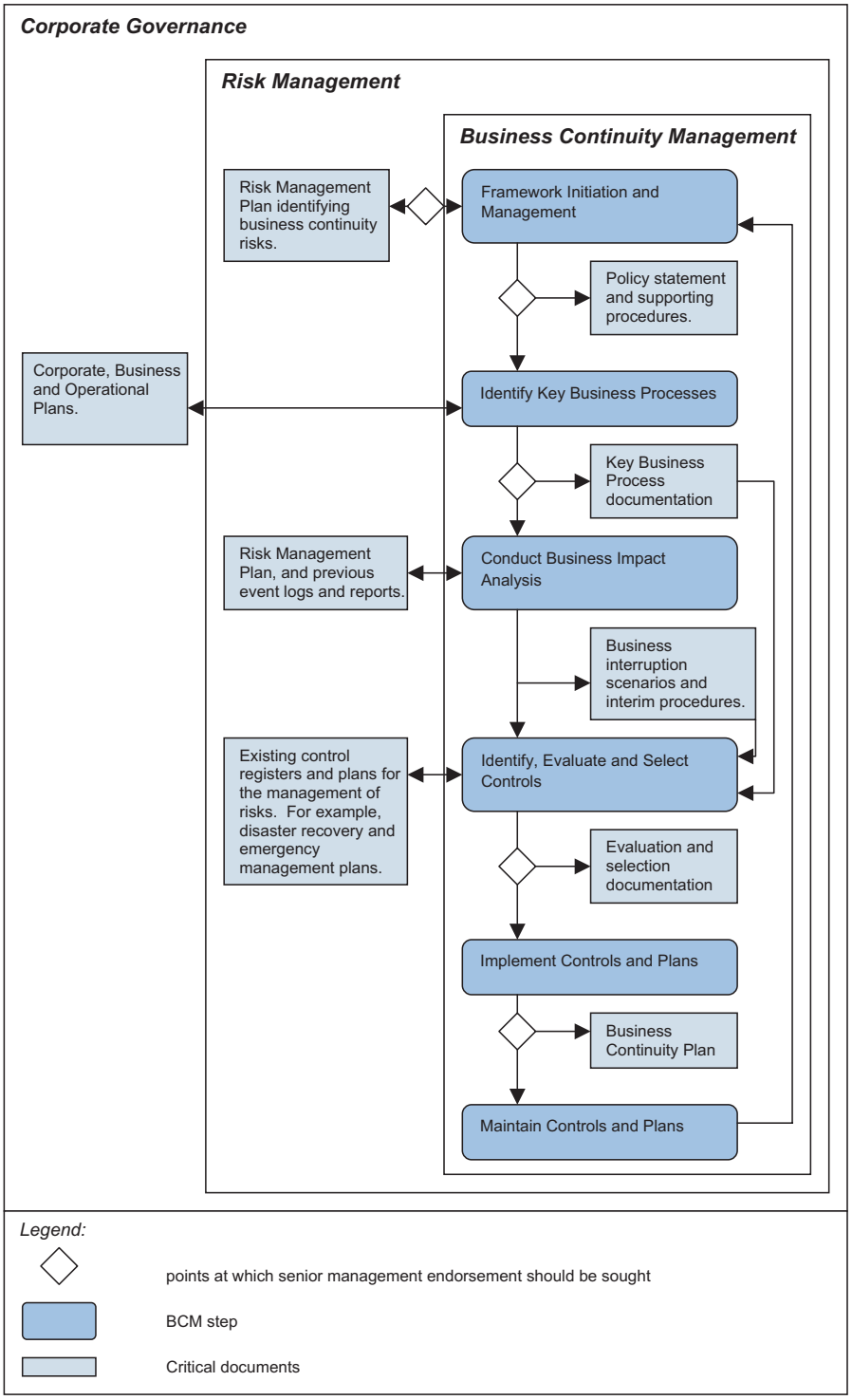
- a BCM policy statement and supporting procedures which outline the objectives, scope, assumptions, limitations, resources, responsibilities and management controls (for example, change controls and performance indicators) for the framework;
- the steps required for the organisation to move from the BCM framework to a fully developed BCP. These steps include: key business process identification; Business Impact Analysis (BIA); and control design and selection. In addition, as BCM is a dynamic discipline that is constantly evolving, organisations should establish regular testing and maintenance schedules for the controls and plans, as well as a schedule for reporting to senior management on the ongoing ability of the controls and plans to achieve the objectives of the BCM framework; and
- a BCP which includes, at a minimum, the following subsidiary plans:
  - operating group contingency plans, including interim processing procedures;
  - disaster recovery plans, including the IT disaster recovery plan;
  - business resumption plan; and
  - crisis management and/or evacuation plans.

1.9 The BCP should establish: the disaster declaration point and escalation procedures; provide templates to assist users to apply the treatments in the plan,

and to record the results; and document key contact points and resource information. The BCP should also cross-reference other relevant risk management and business continuity controls and plans, including the security plan, the backup and recovery procedures, the emergency response procedures, and the communications and media liaison strategies.

1.10 Figure 1, below, illustrates the relationships between BCM, risk management, corporate governance and other related disciplines.

Figure 1
BCM Relationships



Structure of this report

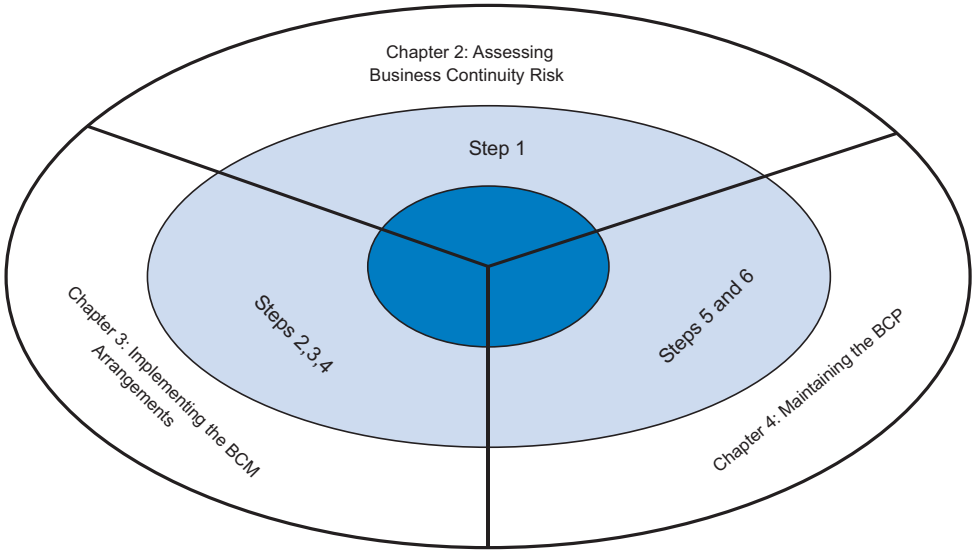
1.11 This Report has been structured to reflect the principles espoused in the Better Practice Guide. Specifically, the risk management process and six business continuity process steps[13] have been presented in three chapters as illustrated in Figure 2 below. Chapter 2 discusses how BCM fits into the broader corporate governance and risk management practices of the organisation, and explains that these practices should be the drivers for the development of BCM arrangements (specifically, the BCM framework, controls and plans).

1.12 Chapter 3 discusses the better practice steps organisations need to undertake to develop and implement the BCM arrangements including:

- business process identification and mapping for the purpose of establishing an organisation-wide profile and prioritisation of key business processes;
- business impact analysis of the business continuity risks; and
- identifying and evaluating possible controls and plans to manage the business impacts identified.

1.13 Chapter 4 discusses the maintenance of the BCP and associated plans.

Figure 2
Report Structure



[13] Australian National Audit Office, op. cit., p. 30.

2. Assessing Business Continuity Risk

This chapter outlines the key relationships for BCM and explains that these relationships are necessary to: justify the need for BCM; obtain appropriate senior management endorsement for a BCM framework and supporting procedures; and highlight the importance of BCM throughout the organisation. In addition, information critical to the objectives, scope and boundaries of the BCM framework should flow from the risk management program.

Introduction

2.1 Business Continuity Management (BCM) is one aspect of risk management, and through this is an important contributor to corporate governance. Establishing a clear link between BCM and corporate governance will directly influence the success and effectiveness of the BCM arrangements.

2.2 For business operations that are large, and rely on the interaction of many business groups and processes, good management practice indicates that a sound management framework is necessary to control these relationships. In order to develop an effective BCM framework, an organisation should establish the objectives, scope and boundaries of its proposed framework in a policy statement for clear direction. The policy statement should also outline roles and responsibilities, management controls (including performance measures and change control procedures), and the key deliverables of the BCM development and implementation efforts. Senior management should endorse the development of the BCM framework, and approve the policy statement and supporting procedures, to ensure that a BCM framework appropriate to the organisation's needs will be developed.

2.3 It is also important to recognise that the BCM framework, controls and plans (including the BCP) will generally be closely related to disaster preparedness and recovery, and emergency response and management arrangements. This link should be evident in the risk management and BCM framework documentation.

Audit findings—assessing business continuity risk

2.4 To make an assessment as to how well organisations were assessing business continuity risk, the ANAO examined whether:

- business continuity risk was assessed as part of organisation-wide risk management; and
- the objectives, scope and boundaries of the BCM framework were documented in an approved policy statement and supporting procedures.

2.5 A discussion of the findings across the four organisations audited is provided to highlight:

- examples of the adoption of sound or better practices; and
- opportunities for the adoption of other better practices.

Corporate governance, risk management, BCM and other related disciplines

2.6 The relationship between corporate governance, risk management, and BCM can be explained as follows: business continuity risk should be considered as part of organisation-wide risk management; risk management is an integral part of an organisation's management and control structures; and, therefore, of sound corporate governance. These relationships, and their relationship to the other related disciplines were explained in Chapter 1.

2.7 To ensure that organisational objectives are being met, and priorities are being addressed in an appropriate order, an organisation-wide view of risks and controls is necessary.[14] Integration of business continuity risk within the broader risk management and control frameworks allows an organisation to identify and prioritise the functions and activities that need to be controlled across the organisation. This will assist the organisation to utilise scarce resources to the greatest benefit. Prioritisation of business risks, business processes and business resources is discussed in further detail in Chapter 3.

Audit findings

Linking corporate governance, risk management and BCM

2.8 Most organisations in the audit could improve the link between their corporate governance, risk management and BCM processes. Only one organisation was capable of providing evidence that a relationship exists. However, the benefits that could be achieved by that organisation from this relationship would improve with more detailed and regular performance assessment and management reporting of the success of its implemented arrangements.

---

[14] P Barrett, op. cit.

2.9 Another organisation had established (in 1997) that BCM was a component of risk management and, therefore, of its corporate governance framework. However, it also recognised that its arrangements have become out-dated over time. As a result, the organisation has commenced a review of its risk, emergency and business continuity arrangements. A significant amount of work has been undertaken by this organisation to: explore its options for management control; identify, document and prioritise risks to the organisation; and develop an integrated set of disaster preparedness, emergency response and business continuity documents. As part of this review process, the organisation also plans to incorporate recent developments and better practice principles in risk management and BCM.

2.10 The other two organisations were undertaking projects at the time of the audit to document, strengthen and formalise risk management. They indicated that one of the primary objectives of this process was to establish a central co-ordination point for risk management in their organisations. This will assist the organisations to obtain a consistent and full understanding of risks, as well as to prioritise risks at the organisation-wide level. They both anticipated that BCM would be a key risk mitigation strategy for their organisations.

Risk management and BCM risk assessments

2.11 All organisations indicated to the ANAO that they had current organisation-wide risk management plans, and that these had been developed using a logical and systematic methodology for identifying, analysing, assessing, treating and monitoring risks. In addition, the ANAO noted that all organisations had involved operating groups in their most recent risk identification and assessment processes, thereby increasing the likelihood that all critical risks (within operating groups and across the organisation) had been identified, and that operating groups would accept (and have a sense of ownership for) the risks identified.

2.12 The audit identified that there were a number of weaknesses with the approaches adopted by the organisations to explore and document their understanding of their business continuity risk environments in their risk management plans. These included:

- two organisations predominately focused on business continuity risks associated with Information Technology (IT), without considering other business interruption events. Only two organisations considered organisation-wide business continuity risks to the organisation's infrastructure, or their people, as part of the risk management process;

- two organisations relied on self-assessment processes to determine whether existing controls were adequate to limit their exposure to business continuity risk. One of these organisations assessed its existing controls in a more favourable light than an independent reviewer had. The result was that business continuity risk was initially inappropriately assessed as low and, therefore, this organisation did not undertake work in a timely manner to address business continuity risk. The other organisation in this category observed and reported on significant deficiencies in risk management practices and business continuity controls. However, it did not follow through on its recommendations in a timely manner; and
- two organisations had not fully communicated broader staff responsibilities for risk management or BCM.

Corporate governance

2.13 All organisations were either reviewing, or were in the process of developing, their control frameworks and management oversight functions for BCM. Two organisations indicated that they were examining how the BCM framework would integrate with risk management and their corporate governance frameworks. In particular:

- only two organisations had defined the roles, responsibilities and actions that would apply if the BCM arrangements were activated. However, one of these organisations had not yet implemented its framework. The other was in the process of refining its roles and responsibilities;
- none of the organisations had established control frameworks that could effectively hold responsible officers accountable for their risk management and business continuity activities. This has resulted in the organisations having less structured and diligent approaches to deal with risk;
- three organisations were not able to demonstrate any link between the risk management, business planning and corporate planning processes; and
- all organisations could improve the nature and frequency of management reporting on BCM. Only two organisations were able to evidence periodic management reporting to the executive or management about oversight of risk and BCM. However, no performance measures were established to guide reporting or indicate how successful or otherwise, they had been. Even when deficiencies in the existence or application of BCM arrangements were identified, the responsible officers were not held accountable for resolving the deficiencies in a timely manner.

BCM initiation

2.14 Framework Initiation is identified as the first step of BCM in the Better Practice Guide.

> A [BCM] plan should be prepared documenting the objectives, scope and boundaries of business continuity. The manager, or management committee, responsible for the project should approve the plan, including a budget. The plan need not be overly large or complex, but needs to reflect the size and complexity of business continuity issues in the organisation. Team roles and responsibilities should also be established, and relevant reference material or existing documentation collected at this stage. The plan should continue to develop as more about the organisation and its risks is learned and reflect the organisation's approach to risk management.[15]

2.15 The need for the development of a BCM framework should be an outcome of the risk management process (where organisations should have identified the need to manage risks associated with business continuity). The development of a BCM framework and supporting procedures serves as an integral part of the risk mitigation strategy (along with sound internal controls in other areas such as security). It is critical to obtain senior management endorsement for the proposed BCM framework, to ensure that:

- the BCM framework is consistent with the organisation's priorities for risk management and its existing control frameworks;
- sufficient resources are made available for each stage in the development, implementation and maintenance of a sound and robust framework; and
- the importance of the process is communicated and understood throughout the organisation.

Audit findings

2.16 One organisation indicated that it had completed the first phase in developing a BCM framework, but was unable to provide evidence that it had documented a plan. Instead, it produced a number of control matrices that were used by the project team to record and monitor progress against timelines and deliverables. This organisation indicated that the need for the BCM framework was established during the external audit process. As a result, the charter for undertaking this work rested with the corporate area. However, the ANAO found that this resulted in BCM framework development being undertaken as part of the corporate budget. As such, it had to compete with other corporate activities for resources and time. The statement of objectives and scope for this

[15] Australian National Audit Office, op. cit., p. 31.

organisation's BCM framework was provided to senior management for their endorsement six months after the project had started.

2.17 Two organisations indicated that they were in the pre-planning stages for the development of a BCM framework. Both organisations had identified the need to establish organisation-wide BCM arrangements during their risk management processes (approximately two years earlier). At the time of the audit, one of these organisations had undertaken work to establish the current status of business continuity and risk management across its organisation. It had also prepared a high-level briefing that outlined the purpose of BCM, and had presented this to senior management seeking support. Support was provided. A consultant has been engaged to assist with: determining the BCM framework scope; undertaking a business identification and impact assessment; and documenting a BCM framework project plan. The second of these organisations has yet to commence work on its BCM framework, in accordance with its annual work program. However, it has taken advantage of opportunities to build resilience into its operations over the past two years. The organisation has also indicated that it will use the ANAO's guidance, and any of its existing relevant analysis, documents and procedures, during this process.

2.18 The other organisation was revisiting its existing BCM framework and supporting arrangements at the time of the audit, as these were developed prior to the release of the ANAO's Better Practice Guide and the release of the Australian and New Zealand Standard 4360: 1999, on risk management. This organisation has been able to identify a number of opportunities to improve its existing arrangements. The ANAO noted that it was the only organisation that had documented the objectives, scope, project timeframe and outcome of the initial BCM framework development process in a project plan. This plan received the endorsement of senior management prior to the commencement of the project, and was distributed to relevant stakeholders as part of the development process.

2.19 The ANAO notes that the organisations which are in the pre-planning phase of the development of BCM frameworks have indicated their intention to complete comprehensive BCM framework plans.

Conclusion

2.20 The ANAO concluded that all organisations covered could improve the linkages between their corporate governance frameworks, risk management, BCM and other related disciplines. Specifically, organisations should identify BCM as their primary risk mitigation strategy to deal with business continuity risk. They should also clarify the scope and boundaries of BCM, disaster recovery

and emergency management within the risk management framework. Organisations will achieve greater benefits from their BCM arrangements if they establish and apply adequate management controls and reporting requirements to their BCM arrangements, and maintain adequate documentation of this work, both for accountability and facilitation of their own arrangements.

2.21 The ANAO was particularly concerned by the lack of reporting on costs, outcomes and timelines associated with BCM arrangements. The ANAO found that some organisations were satisfied to include the cost of BCM in the corporate budget, even though they had indicated that the BCM framework was being adopted as a cost effective risk mitigation strategy for the whole organisation. This also resulted in extended development or review processes as the BCM framework, risk management and other corporate activities competed for resources and timelines.

2.22 As most organisations were in the early stages of establishing the objectives, scope and boundaries of their BCM framework projects, there were a number of opportunities for improvement across the organisations examined. In particular, organisations had not developed a sufficiently detailed business case, project proposal, or project plan, to support the development and implementation of their BCM frameworks. This meant that it was difficult for them to focus their efforts on manageable components of work; adequately quantify the resources required; and obtain sufficient buy-in from all areas of the organisation. Organisations also needed to finalise roles and responsibilities under the new frameworks, as well as illustrating how the frameworks and lines of accountability link to existing disaster recovery and emergency management arrangements.

3. Implementing the BCM Arrangements

This chapter explains why it is important for an organisation to understand its business operations in order to deal effectively with business continuity risks. It outlines the relationship between business process identification and mapping, and the assessment of business interruption events on business operations. This understanding is necessary for organisations to design, select and implement the most appropriate controls and plans to protect its key business processes.

Introduction

3.1 In order for an organisation to determine the most appropriate focus, and extent of coverage, for its BCM arrangements, it is critical that the organisation understands its business objectives, outcomes and operating environment. This will involve the organisation:

- identifying key business processes including their inputs, outputs and resource requirements;
- mapping interdependencies between the processes, as well as between these processes and the organisation's outcomes; and
- prioritising the processes based on their impact on the achievement of the organisation's objectives.

3.2 Once the organisation has a sound understanding of its objectives, outcomes and the supporting processes, it will be able to effectively assess the impact of potential business continuity risks. This assessment is typically undertaken as part of the Business Impact Analysis (BIA), which is specifically designed to assess the impact of the loss of key processes or resources on the achievement of business objectives or outcomes. As part of this analysis, the organisation should identify critical success factors, existing controls and maximum acceptable outage (MAO) periods[16] for their key processes or resources. This understanding will enable them to assess whether their existing controls and plans are sufficient to minimise the likelihood or impact of potential continuity risks, or whether other controls need to be implemented.

3.3 As with overall risk management, the organisation will need to revisit, on a periodic basis, the identification and mapping of its key processes and the

[16] The MAO is the time it will take before a business interruption event threatens an organisation achieving its business objectives. The MAO defines the maximum time an organisation can survive without key business functions before business continuity plans and recovery procedures must commence.

BIA. Therefore, organisations need to maintain sufficiently detailed documentation including business process maps and/or listings, BIA worksheets and assessments, and control registers that detail control design and operation. This documentation will assist the organisation to assess, prioritise and review periodically the operating environment and the effectiveness of implemented controls.

Audit findings—implementing the BCM arrangements

3.4 To make an assessment as to how well organisations were implementing the BCM arrangements, the ANAO examined whether:

- key processes, activities and resources had been identified, mapped and prioritised;
- a BIA had been conducted to identify critical success factors, MAO periods, and impacts so that appropriate interim processing procedures could be developed; and
- possible controls had been identified, assessed and selected for the purpose of implementing appropriate preparatory and reactive controls and plans.

3.5 A discussion of the findings across the four organisations audited is provided to highlight:

- examples of the adoption of sound or better practices; and
- opportunities for the adoption of other better practices.

Business process identification, mapping and prioritisation

3.6 Key Business Processes Identification is identified as the second step of BCM in the Better Practice Guide.

It is important, in preparation for the BIA, that management has a clear and agreed understanding of the organisation's business objectives and outputs, and the key business processes which ensure these objectives are met and outputs are achieved. A structured approach to this step requires organisations to:

- establish and rank key business processes;
- map activities undertaken within each process; and
- match resources to activities.[17]

[17] Australian National Audit Office, op. cit., p. 32.

3.7 Therefore an organisation will need to identify, document and map its understanding of its processes, as well as the activities which comprise each process and the resource requirements for those activities (including people, infrastructure, assets and supplies, and finance). This information should be available from the corporate, business and operational planning processes. The organisation will then have the necessary information to categorise the processes into those that are essential to the achievement of business outcomes (key processes) and those that are not. Prioritisation of the key processes then enables the organisation to apply its limited resources in the most effective manner. It is, therefore, a key component of good management practice.

3.8 It is also critical for the organisation to obtain senior management endorsement for the prioritised list of key processes, as this will ensure their buy-in and support for the BCM steps that follow. In addition, this documentation and mapping will need to be revisited periodically to ensure that it continues to provide a reliable and accurate basis for the BCM arrangements.

Audit findings

3.9 All organisations audited had established and documented their organisational objectives and outputs in their critical planning documents. It was also possible to identify the operating groups and the responsibility for major operating functions from the organisational charts provided.

3.10 All organisations had identified the operating groups that supported the delivery of organisational outputs. They indicated that the operating groups had documented their processes, activities and resource requirements in work plans. However, the ANAO found that there was only limited documentation of this work. Organisations appeared to rely largely on dated assessments, or verbal assurances given by operating groups, that the necessary business process identification and mapping work had been completed to support the business continuity (and broader) management objectives of the organisation.

3.11 Of the four organisations audited, one indicated that it would develop an organisation-wide listing of key processes and resource requirements. Another organisation indicated that, due to the dynamic nature of its operations, it was more practical for its operating groups to establish and prioritise a list of key activities and potential resource requirements at the time of the business interruption event. However, the ANAO considers that this approach may not provide a comprehensive identification, and understanding, of the operations and process interdependencies. In addition, it may mean that senior management are unaware of, or do not have an opportunity to endorse, the prioritised list of key processes. This may result in insufficient management support and

resourcing in a disaster, when management decides the prioritisation determined by the operating group does not match the organisation-wide priorities.

3.12 The ANAO considers that all organisations could significantly improve the frequency of review of business process listings and mappings, as well as the controls surrounding this process (including maintaining adequately detailed documentation and obtaining senior management sign-off). Most organisations had not formally linked this review process to the annual business planning or risk management review cycles. The ANAO considers that they would benefit from doing so.

Conducting a BIA

3.13 The BIA is identified as the third step of BCM in the Better Practice Guide.

> ...information [from the key business process identification] must be analysed, and the operational and financial impacts that would result from disruptions to, or loss of, a business process assessed. From this, the [MAO] can be determined for the critical processes and resources. The analysis should be based on an outage in which all activities and resources (including the actual work place) are not available. Assuming the worst case outcome (total loss of the process and/or resources), will ensure all impacts arising from an outage are considered regardless of the risk likelihood...[as] treatments for each [business continuity] event need to be determined.[18]

3.14 As indicated above, an organisation will need to identify, document and map its key processes prior to undertaking a structured BIA. Other information relevant to the BIA may be found in the risk management plan and procedures that document existing preventative and mitigating controls, and the documentation that establishes the statutory, legislative and stakeholder requirements of the organisation. This information will strengthen the analysis by enabling the consideration of the impacts on the critical success factors, MAO periods, and existing control frameworks of business interruption events. As part of this analysis, the organisation should also seek to identify alternative interim processing procedures; quantify the costs associated with these procedures; and review the backlog of work that may arise during the period these procedures are used. This work should be documented to facilitate an analysis and review of the findings.

3.15 As with the other steps of BCM, the BIA will need to be revisited periodically to ensure that it continues to provide a reliable and accurate basis for the maintenance of the BCM framework.

---

[18] Australian National Audit Office, op. cit., p. 36.

Audit findings

3.16 Three of the four organisations audited had completed some analysis of the impact of a business interruption event of one or more of their key processes. Two of these organisations had performed this analysis both at the organisation-wide and operating group levels, while the third organisation had only performed this analysis at the operating group level. The ANAO found that the organisations that had undertaken an analysis of impacts at the organisation-wide level were able to demonstrate that they had considered impacts on infrastructure and human resources, whereas the organisation that undertook an analysis at the operating group level had only documented the impact on outputs. The other organisation in the audit had not yet reached this stage in the development of BCM arrangements, but had considered loss of resources as part of its emergency management activities.

3.17 Two organisations had identified some of their critical success factors, resource requirements, interim processing procedures and vital records. One of these organisations had also:

- attempted to quantify the minimum resource requirements necessary to perform interim processing procedures, and the backlog in processing that may arise during this period;
- established MAOs for non- IT and IT-related processes; and
- provided evidence that it had consulted operating groups in order to determine MAOs.

3.18 The ANAO found that organisations did not maintain adequate documentation in support of the BIA. In particular:

- three of the organisations were not able to provide the ANAO with BIA worksheets, analysis of the findings or conclusions drawn;
- it was not evident that organisations had considered all of the relevant documentation and information during the BIA process (suggesting an ad hoc approach had been employed);
- two organisations had only documented MAOs for their critical IT systems. In one of these organisations, the MAOs appeared to be determined by the IT operating group in isolation from the other operating groups' requirements; and
- none of the organisations had adequately documented their interim processing procedures, the cost of these procedures, or all of their resource requirements.

3.19 As a result, it was not possible to determine whether the BIAs had been undertaken to finality. In addition, the ANAO was unable to determine whether this documentation was being revisited periodically, or in a timely manner.

Identifying and selecting continuity treatments

3.20 Design Continuity Treatments is identified as the fourth step of BCM in the Better Practice Guide.

> This step identifies the treatments to address, and to minimise the effects of, disruptions to each critical business process for which an MAO has been established. The treatment analysis identifies the requirements to ensure continued availability of critical processes and resources during outages. These requirements are based on the rankings [and analysis] agreed in the BIA...[i]n selecting alternative activities and/or resources, it is critical the following areas are addressed as part of the business continuity planning process in respect of each identified disruption, regardless of the organisation's objectives, size or complexity:
>
> - people;
> - facilities (including buildings and equipment);
> - telecommunications;
> - information systems; and
> - business activities.
>
> For all critical activities and resources, it is necessary to identify other arrangements that may be used in their place, should they be lost.
>
> The outcome of the treatment analysis will form the basis of the business continuity plan.[19]

3.21 The second and third steps of BCM (Key Business Process Identification and BIA, respectively) provides the information necessary to enable the organisation to identify and design possible continuity treatment options, and evaluate these treatment options to select the most appropriate mix of preventative and mitigating (reactive) treatments (referred to as controls and plans in this report).

3.22 Aspects of cost, impact and timeframe are critical to the evaluation of possible controls and plans. The organisation needs to balance the cost of its BCM arrangements against the:

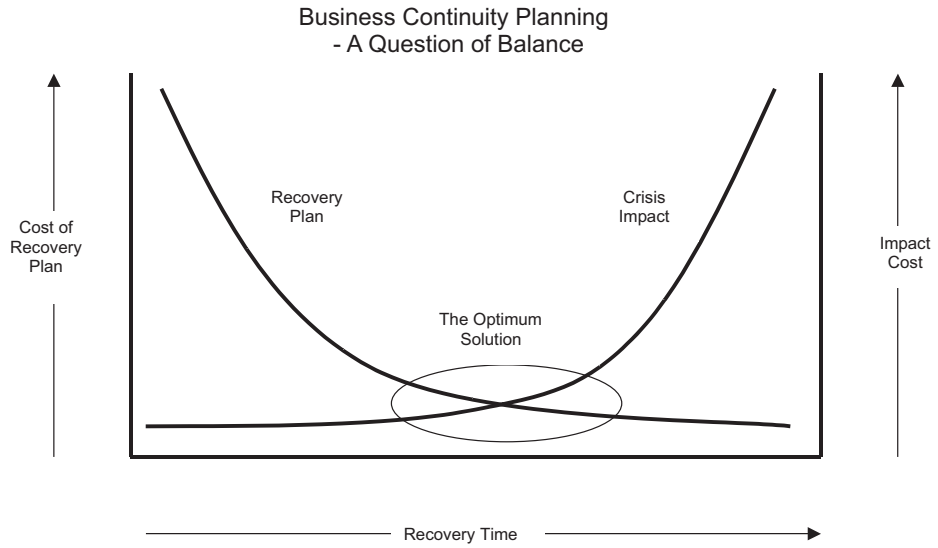
---

[19] Australian National Audit Office, op. cit., pp. 39–40.

- anticipated impacts of a business interruption event; and
- acceptable timeframe for recovery (refer to Figure 3 below).

3.23 However, it is important to recognise that the ability to continue operations in the event of a business interruption event is the most important consideration in business continuity planning. BCM is primarily concerned with preserving the ongoing viability, reputation and relationships with stakeholders of the organisation. This is achieved through demonstrating good management controls, including effective risk, disaster recovery and business continuity planning.

Figure 3
BCM Balance Diagram



Source: Paul Viciulis, Optus

3.24 This work should be documented to facilitate an analysis and review of the findings. As with the other steps discussed above, the treatment identification and evaluation documentation will need to be revisited periodically to ensure that the selected mix of treatment options continues to provide the most appropriate coverage.

Audit findings

3.25 Two organisations had prepared some documentation outlining possible controls and plans, and the associated resource requirements. However, this information did not enable the ANAO to determine whether an appropriate evaluation had occurred on the basis of organisational priorities, existing controls,

cost efficiency and operational effectiveness. In addition, only a few business interruption scenarios were considered by these organisations. As well, very limited documentation of the analysis was available.

3.26 The other two organisations were not yet at this stage in the development of their BCM arrangements. However, both were aware of the need to identify and evaluate business interruption events. In addition, one of these organisations had demonstrated that it had completed a detailed analysis for crisis management events, and planned to apply a similar approach during the BCM framework development.

3.27 The ANAO acknowledges that, as most organisations were in the early stages of developing their BCM frameworks, they had not yet had the opportunity to undertake a BIA and properly evaluate controls and plans. However, the lack of documentation on the identification and mapping of business processes, as well as for the analysis of activities such as business recovery, suggests that organisations have not been active in their approach to these steps in BCM. As a result, the ANAO suggests there are a number of opportunities for the adoption of better practice principles by organisations covered in the audit.

Conclusion

3.28 All organisations have opportunities to improve their approach to, and the quality of documentation in support of: business process identification and prioritisation; the BIA; and treatment option design and evaluation. In particular, organisations could do more to demonstrate that they have:

- identified their processes and resource requirements;
- mapped interdependencies between processes (as well as to organisational objectives);
- prioritised key processes based on this understanding;
- undertaken a structured and comprehensive BIA to determine the impact business interruption events may have on key processes;
- identified possible controls and plans to minimise the impact of potential business interruption events; and
- evaluated possible controls and plans against MAOs, existing controls, organisational priorities and cost information to select the most appropriate mix of preventative and reactive controls and plans.

4. Maintaining the Business Continuity Plan

This chapter outlines the importance of maintaining a documented and current Business Continuity Plan (BCP). It discusses the nature and frequency of testing and review needed to maintain the BCP as a relevant and useful document.

Introduction

4.1 Once an organisation has selected the most appropriate mix of controls and plans, it should communicate the agreed arrangements to its staff. This is typically achieved through the documentation of controls and procedures in plans. These are generally presented in a BCP, and should be supported by the development and provision of business continuity education programs.

4.2 It is important for the organisation to establish the relationship between its BCP, and other relevant documentation on preventative and reactive controls (including the backup procedures, security requirements and the disaster recovery plan). The organisation should also develop templates to assist its staff with the application of the principles in the BCP, and to ensure that adequate information is captured during a test of the BCP, or during any business interruption event, that will facilitate an analysis of the effectiveness of controls at a later date. This information, combined with the results of periodic structured testing and maintenance of the BCP, will enable the organisation to preserve the BCP's relevance to the organisation.

Audit findings—maintaining the business continuity plan

4.3 To make an assessment as to how well organisations were maintaining their BCPs, the ANAO examined whether:

- the organisation had documented and implemented its chosen preparatory and reactive controls and plans. This should include the development of a BCP and the documentation of assigned responsibilities; and
- the organisation regularly tests and reviews the controls and plans (including the BCP) to ensure currency and completeness. This review is linked with ongoing risk management and BCM to ensure the controls and plans address current business and risk priorities.

4.4 A discussion of the findings across the four organisations audited is provided to highlight:

- examples of the adoption of sound or better practices; and
- opportunities for the adoption of other better practices.

Implementing and documenting continuity controls and plans

4.5 Implementing Continuity Treatments is identified as the fifth step of BCM in the Better Practice Guide.

> Selection of continuity [controls and plans] will lead to:
>
> - implementation of procedures to support recovery from a disruption to business; and
> - documentation of the recovery arrangements.
>
> Procedures implemented to support recovery will need to be both preparatory and reactive.
>
> Three of the most important [preparatory] controls include back-up processes, records management and formal contingency arrangements with external parties.
>
> Documentation of the recovery arrangements to be implemented after [a business interruption event] has occurred is the role of the Business Continuity Plan.[20]

4.6 The BCP is generally structured as a compilation of individual operating group recovery or contingency plans, brought together with an overarching management plan to coordinate the former. It should address business interruption events from the initial disaster response to the point at which normal operations are resumed. Therefore, it is critical that the BCP defines the disaster declaration point and establishes the phases of recovery. It should also provide templates to assist with the recording of important information during a business interruption event.

4.7 In addition, other documents that explain the operation of controls implemented to mitigate other business risks may be directly relevant to BCM (for example, emergency management arrangements), or need to be maintained during a business interruption event (for example, a security breach). Therefore, an organisation needs to ensure it establishes adequate cross-referencing between the BCP and other relevant documents. This also applies to any contractual arrangements (for example, with an IT outsourcer).

---

[20] Australian National Audit Office, op. cit., p. 45.

Audit findings

4.8 Only one organisation had documented a whole-of-organisation BCP. This document was developed over a seven-month period, and involved extensive consultation and review with operating groups. The document was in draft at the time of audit fieldwork. The ANAO found that the draft BCP reflected the structure recommended in the Better Practice Guide. It comprised an overarching policy statement, a series of operating group response plans, and a series of continuity treatment plans. It also included relevant information on contacts and suppliers, and provided a series of templates to assist with the capture of critical information.

4.9 Another organisation had developed a series of emergency and disaster preparedness, response and recovery plans. These documents were drawn together by an overarching framework document, which explained their relationship to one another. All of these documents are maintained centrally by the organisation. Each site maintains a copy of their site-specific set of emergency and disaster preparedness, response and recovery plans. The ANAO noted, however, that these plans do not contain event logs, information on determining the disaster declaration point, or a reference to interim processing procedures.

4.10 The other two organisations do not currently have documented BCPs. Both of these organisations rely heavily on their IT and, as a result, have developed extensive documentation in support of IT disaster recovery.

4.11 All organisations had developed and implemented adequate back-up procedures and were developing vital records management and communication management programs. However, all organisations needed to do more work to establish: the disaster declaration point for their business operations; sufficient inventory lists of resource requirements; the BCP's limitations and assumptions; and testing and maintenance schedules. Three of the organisations will also need to develop appropriate education programs for their BCPs to ensure that the BCP is effectively adopted by the organisation.

4.12 In addition to the findings observed during this audit, a recent survey[21] of 50 Commonwealth organisations revealed that only 56 per cent reported that they had documented a BCP. In addition, only 54 per cent of these organisations had integrated the BCP with their risk management plan. This reflects the low level of maturity in addressing this discipline. The ANAO also noted that, in developing the BCPs, the organisations covered in the audit indicated that they tended not to recognise the role of property and business interruption insurance.

---

[21] The results of which will be presented in the impending report on Risk Management and Insurance in Commonwealth organisations, to be tabled in July 2003.

Testing and maintaining the business continuity controls and BCP

4.13 Test and Maintain the Plan is identified as the final step of BCM in the Better Practice Guide.

> Review of the BCP is essential to ensure that it reflects the organisation's objectives, its key business functions, the corresponding processes and resources, and an agreed priority for recovery. Testing and maintenance of the recovery process documented in the BCP will provide management assurance that the plan is effective—that is, it will ensure continuity of business should key functions be lost.
>
> The major components of the BCP should be tested annually and updated based on the results of each test...There are several approaches that may be adopted to test the plan.
>
> Administrative procedures and guidelines should be developed to provide for periodic testing and documentation maintenance of the [plans].[22]

4.14 Organisations should develop structured periodic testing scenarios so that the results of tests are valid, timely and useful. They will also need to capture relevant information from the tests to use in the review process, and to report results to management. In addition, a maintenance schedule and procedures should be prepared to ensure the timely, controlled and structured review and, amendment of, the BCP.

Audit findings

4.15 None of the organisations audited was at the stage where they could test and maintain their BCPs. However, all organisations did have procedures in place to periodically test aspects of their disaster recovery and emergency response arrangements. The ANAO considers that the organisations could use these testing arrangements, together with principles outlined in the Better Practice Guide, to develop appropriate testing arrangements for the BCPs. Organisations also need to ensure that they maintain adequate documentation of the test results and analysis of this work. Only two organisations could provide any documentation in relation to test results for business recovery capabilities.

4.16 Three organisations had established periodic (generally annual) maintenance requirements for their disaster recovery and emergency response arrangements. The other organisation indicated that it was developing a maintenance schedule. Again, organisations need to ensure that they maintain adequate documentation of the results and analysis of this work, and should

[22] Australian National Audit Office, op. cit., pp. 62–64.

establish strong links between the maintenance schedules and the business planning and risk management processes.

4.17 The ANAO acknowledges that, as most organisations in the audit were in the early stages of the development of BCM arrangements, they had not yet had the opportunity to fully document BCPs, or develop and implement testing and maintenance schedules for the proposed BCP. However, the lack of documentation in support of other business recovery processes, suggests that organisations need to be more diligent in their approach to testing and maintaining critical documents. As a result, the ANAO considers there are a number of opportunities for adoption of better practice principles by the organisations covered in the audit.

Conclusion

4.18 All organisations have opportunities to improve the level of documentation of controls and plans in support of BCM. They also need to improve their approach to, and the quality of documentation in support of, the testing and maintenance of those controls and BCPs. Organisations need to demonstrate that they have:

- determined an appropriate and comprehensive testing strategy for the BCP that incorporates all major components and plans;
- documented the results of tests so that they may be used constructively in updating and maintaining the BCP; and
- established an appropriate maintenance schedule that is adequately linked to the business planning and risk management processes.

Canberra ACT
23 June 2003

P. J. Barrett
Auditor-General

Series Titles

Audit Report No.1 Performance Audit
Information Technology at the Department of Health and Ageing
Department of Health and Ageing

Audit Report No.2 Performance Audit
Grants Management
Aboriginal and Torres Strait Islander Commission

Audit Report No.3 Performance Audit
Facilities Management at HMAS Cerberus
Department of Defence

Audit Report No.4 Audit Activity Report
Audit Activity Report: January to June 2002
Summary of Outcomes

Audit Report No.5 Performance Audit
The Strategic Partnership Agreement between the Department of Health and Ageing and the Health Insurance Commission
Department of Health and Ageing and the Health Insurance Commission

Audit Report No.6 Performance Audit
Fraud Control Arrangements in the Department of Veterans' Affairs

Audit Report No.7 Performance Audit
Client Service in the Child Support Agency Follow-up Audit
Department of Family and Community Services

Audit Report No.8 Business Support Process Audit
The Senate Order for Department and Agency Contracts (September 2002)

Audit Report No.9 Performance Audit
Centrelink's Balanced Scorecard

Audit Report No.10 Performance Audit
Management of International Financial Commitments
Department of the Treasury

Audit Report No.11 Performance Audit
Medicare Customer Service Delivery
Health Insurance Commission

Audit Report No.12 Performance Audit
Management of the Innovation Investment Fund Program
Department of Industry, Tourism and Resources
Industry Research and Development Board

Audit Report No.13 Information Support Services
Benchmarking the Internal Audit Function Follow–on Report

Audit Report No.14 Performance Audit
Health Group IT Outsourcing Tender Process
Department of Finance and Administration

Audit Report No.15 Performance Audit
The Aboriginal and Torres Strait Islander Health Program Follow-up Audit
Department of Health and Ageing

Audit Report No.16 Business Support Process Audit
The Administration of Grants (Post-Approval) in Small to Medium Organisations

Audit Report No.17 Performance Audit
Age Pension Entitlements
Department of Family and Community Services
Centrelink

Audit Report No.18 Business Support Process Audit
Management of Trust Monies

Audit Report No.19 Performance Audit
The Australian Taxation Office's Management of its Relationship with Tax Practitioners
Australian Taxation Office

Audit Report No.20 Performance Audit
Employee Entitlements Support Schemes
Department of Employment and Workplace Relations

Audit Report No.21 Performance Audit
Performance Information in the Australian Health Care Agreements
Department of Health and Ageing

Audit Report No.22 Business Support Process Audit
Payment of Accounts and Goods and Services Tax Administration in Small Commonwealth Agencies

Audit Report No.23 Protective Security Audit
Physical Security Arrangements in Commonwealth Agencies

Audit Report No.24 Performance Audit
Energy Efficiency in Commonwealth Operations—Follow-up Audit

Audit Report No.25 Financial Statement Audit
Audits of the Financial Statements of Commonwealth Entities for the Period Ended 30 June 2002
Summary of Results

Audit Report No.26 Performance Audit
Aviation Security in Australia
Department of Transport and Regional Services

Audit Report No.27 Performance Audit
Management of Commonwealth Guarantees, Warranties, Indemnities and Letters of Comfort

Audit Report No.28 Performance Audit
Northern Territory Land Councils and the Aboriginals Benefit Account

Audit Report No.29 Audit Activity Report
Audit Activity Report: July to December 2002
Summary of Outcomes

Audit Report No.30 Performance Audit
Defence Ordnance Safety and Suitability for Service
Department of Defence

Audit Report No.31 Performance Audit
Retention of Military Personnel Follow-up Audit
Department of Defence

Audit Report No.32 Business Support Process Audit
The Senate Order for Departmental and Agency Contracts (Spring 2002 Compliance)

Audit Report No.33 Performance Audit
Management of e-Business in the Department of Education, Science and Training

Audit Report No.34 Performance Audit
Pest and Disease Emergency Management Follow-up Audit
Department of Agriculture, Fisheries and Forestry—Australia

Audit Report No.35 Performance Audit
Fraud Control Arrangements in the Australian Customs Service

Audit Report No.36 Performance Audit
Monitoring of Industry Development Commitments under the IT Outsourcing Initiative
Department of Communications, Information Technology and the Arts

Audit Report No.37 Performance Audit
Passport Services
Department of Foreign Affairs and Trade

Audit Report No.38 Performance Audit
Referrals, Assessments and Approvals under the Environment Protection and Biodiversity Conservation Act 1999

Audit Report No.39 Performance Audit
Navy Operational Readiness
Department of Defence

Audit Report No.40 Performance Audit
R & D Tax Concession
Department of Industry, Tourism and Resources, the Industry Research and Development Board and the Australian Taxation Office

Audit Report No.41 Performance Audit
Annual Reporting on Ecologically Sustainable Development

Audit Report No.42 Performance Audit
Managing Residential Aged Care Accreditation
The Aged Care Standards and Accreditation Agency Ltd

Audit Report No.43 Performance Audit
The Sale of Sydney (Kingsford Smith) Airport

Audit Report No.44 Performance Audit
Review of the Parenting Payment Single Program
Department of Family and Community Services
Centrelink

Audit Report No.45 Business Support Process Audit
Reporting of Financial Statements and Audit Reports in Annual Reports

Audit Report No.46 Performance Audit
Australian Industry Involvement Program
Department of Defence

Audit Report No.47 Performance Audit
Implementation and Management of the Indigenous Employment Policy
Department of Employment and Workplace Relations

Audit Report No.48 Performance Audit
Indigenous Land Corporation—Operations and Performance Follow-up Audit
Department of Immigration and Multicultural and Indigenous Affairs

Audit Report No.49 Performance Audit
Management of the Navigation Aids Network
Australian Maritime Safety Authority

Audit Report No.50 Information Support Services
Managing People for Business Outcomes, Year Two
Benchmarking Study

Audit Report No.51 Performance Audit
Defence Housing and Relocation Services
Department of Defence

Audit Report No.52 Performance Audit
Absence Management in the Australian Public Service

Better Practice Guides

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

Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997
Audit Committees	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996