IMPORTANT UPDATE

Australian National Audit Office

# Business Continuity Management

## Building resilience in public sector entities


Better Practice Guide | June 2009

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Foreword

Providing continuity in the face of a disruptive event is an important issue to be considered by boards, chief executives and senior management in public sector entities,[1] not-for-profit organisations and businesses. There are sufficient examples in today's world to demonstrate that events that can seem unlikely do happen. Many services delivered by public sector entities are essential to the economic and social well-being of our society - a failure to deliver these could have significant consequences for those concerned and for the nation.

The previous version of this guide, *Business Continuity Management: Keeping the wheels in motion (2000)* assisted entities to plan for the continued delivery of critical business processes in the event of business disruption. This is more simply referred to as business continuity.

Business continuity management is an essential component of good public sector governance. It is part of an entity's overall approach to effective risk management, and should be closely aligned to the entity's incident management, emergency response management and IT disaster recovery. Successful business continuity management requires a commitment from the entity's executive to raising awareness and implementing sound approaches to build resilience. The importance of becoming a resilient entity is integral to contemporary business continuity practices, and we have named this guide *Business Continuity Management: Building resilience in public sector entities.* This edition refreshes and updates the contents of the previous guide.

While practices described in this publication generally provide guidance to entities, it is important that each entity assesses the extent to which the information provided is relevant, appropriate and cost-effective in light of its own individual circumstances.

This guide has been prepared with contributions and insights from a number of entities and businesses. The assistance of Ernst and Young in updating this guide is also recognised and appreciated.

Ian McPhee

Auditor-General

June 2009

*An ounce of prevention is worth a pound of cure.*

*- Benjamin Franklin.*

[1] For the purposes of this guide, the term entity is used to collectively refer to an Agency, Commonwealth authority and subsidiary, and Commonwealth company and subsidiary, as defined in the *Auditor-General Act 1997*.

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Contents

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Introduction

# IMPORTANT UPDATE

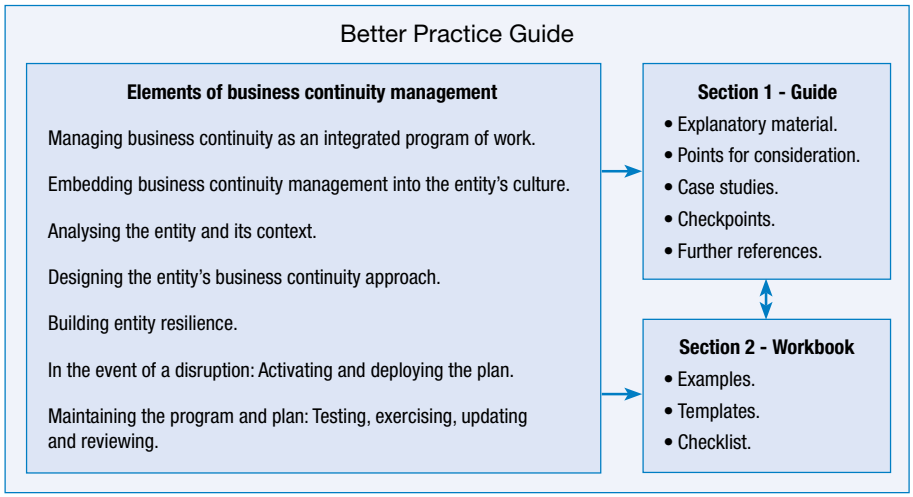
**IMPORTANT UPDATE**

# Introduction

## Structure

*Business Continuity Management: Building resilience in public sector entities* is divided into two sections, the Guide (this section) and the Workbook. Both sections are structured according to the seven elements of a better practice business continuity management program identified by the Australian National Audit Office (ANAO). Figure 1 depicts the structure of the better practice guide.

**Figure 1 - Structure of the better practice guide**




## Key concepts

Business continuity management is an essential component of good public sector governance. It supports and sustains the entity's business strategy, goals and objectives in the face of disruptive events.[2]

There are a number of interrelated activities that work together to prevent and manage a significant business disruption event. These include:

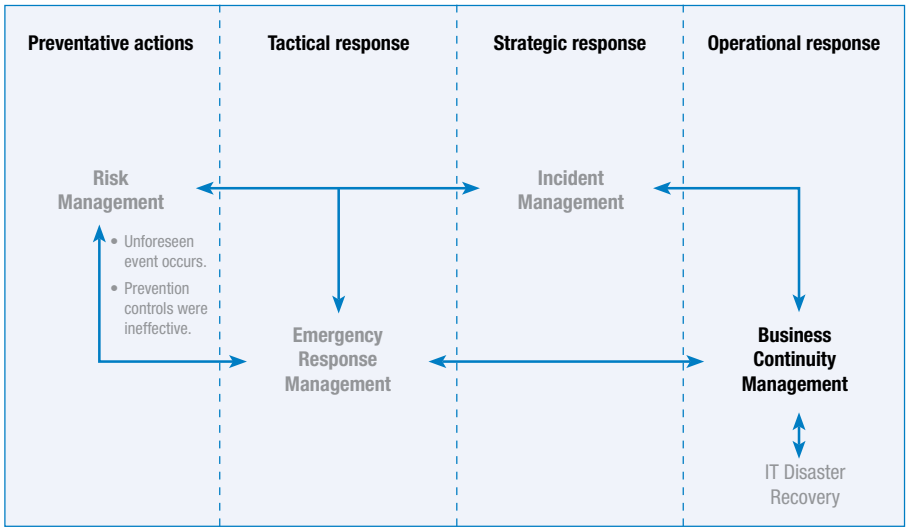
- business continuity management (encompassing Information Technology (IT) disaster recovery);
- risk management;
- emergency response management; and
- incident management.

[2] A disruptive event may be an acute, creeping, or sustained event. A fire is an example of an acute disruptive event, a series of minor IT system failures culminating in the failure of a large or primary system is an example of a creeping disruptive event, and a pandemic is an example of a sustained disruptive event.

**IMPORTANT UPDATE**

The integration of these activities is a success factor for building entity resilience. These activities provide the tactical, strategic and operational response to a business disruption. Figure 2 depicts the relationship between these key concepts.

**Figure 2 - The relationship between risk, emergency response, incident and business continuity management in managing a business disruption**




Note: These management activities are scalable, depending on the operating context of the entity. It may be that in small, non-complex or less time-critical entities, some or all of these activities are combined. In entities that are large, complex, or geographically dispersed, the use of separate emergency response, incident management and business continuity management teams increases the need for clear roles and responsibilities, and effective communication.

Business continuity management is the focus of this guide.

## Business continuity management

Business continuity management 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.[3] It is the capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a disruptive event.

Business continuity management treats the negative consequences of an event, and can create opportunities for benefit and gain. Entities that respond positively to a disruptive event can position themselves to recover quickly and improve their long term business performance.

*When written in Chinese the word crisis is composed of two characters. One represents danger and the other represents opportunity.*

*- John F. Kennedy.*

Business continuity management prepares the steps the entity will take to recover and return to normality. It involves designing business processes and information architecture to limit single points of failure, and developing support area and business unit contingency plans and business resumption plans. It also includes defining escalation procedures, and obtaining contact details for key personnel and for other entities where an important interdependency exists. The business continuity management process includes establishing the maximum periods (known as the maximum tolerable period of disruption) for which critical processes can be disrupted or lost altogether, before it threatens the achievement of entity objectives.

[3] Resilience comes from tackling the likelihood as well as the consequences of disruptive events. Therefore it is important to have both effective risk management and business continuity management frameworks in place.

**IMPORTANT UPDATE**

Business continuity is initiated when a risk occurs that has a significant business disruption consequence.[4] These disruptive events may be low frequency, but they have severe consequences for the entity. Business disruption events need to be distinguished from other business interruptions such as those arising from systems downtime or failures that may occur as a part of normal operations, such as a brief loss of a communications link. A business disruption is an event where normal operational management is suspended.

## *Benefits and costs*

Business continuity management acts to mitigate the negative consequences of a disruptive event, and may also deliver business improvements. The benefits to an entity of an effective business continuity management program may include:

- the continued delivery of Australian Government services to clients (citizens and interdependent entities) in the event of a business disruption;
- the ability to proactively identify the consequences of a business disruption;
- having in place an effective response to a business disruption which minimises damage to the entity;
- reduced costs of operating during a business disruption, and more cost effective recovery;
- management of uninsurable risks, and compliance with insurance policies;
- compliance with regulatory requirements (where applicable);
- enhancing its reputation by demonstrating to stakeholders a credible response;
- increased interdisciplinary and inter-agency teamwork;
- improved efficiency and effectiveness of business-as-usual operations;
- the ability to use negative events as opportunities to improve business processes;
- identifying key interdependencies that may not have otherwise been apparent; and
- building resilience that facilitates managing and recovering from a business disruption event.

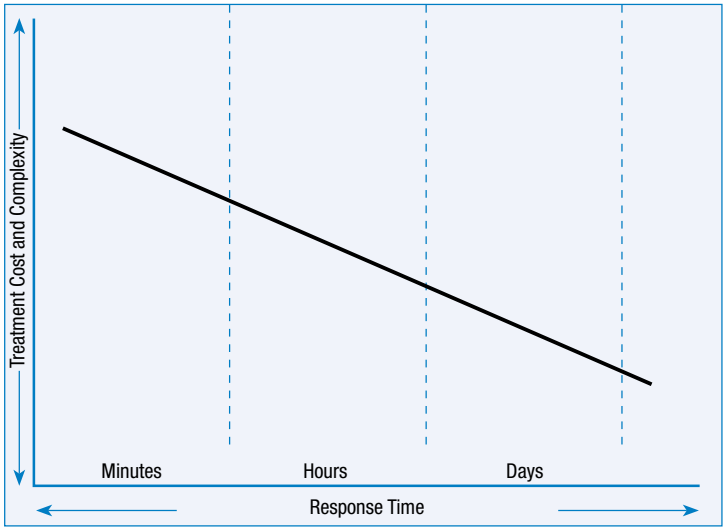
When determining the entity's business continuity strategy, it is important to consider the costs as well as the benefits of the potential continuity treatments. A cost benefit analysis compares the benefits and costs incurred.

Typically, the lower the maximum tolerable period of disruption, the more costly and complex the recovery treatment is likely to be (see Figure 3). This is particularly true when the recovery of technology is involved. It is important to establish a realistic representation of the recovery requirements of the entity.

[4] Entities may wish to activate their business continuity plan in anticipation of an event. An entity's business continuity plan may be activated concurrently with other plans, such as the emergency response plan, or the incident management plan. Entities with multiple levels of response planning need to consider and provide guidance to staff on formally activating the business continuity plan, and when to move from an emergency response to a business continuity response.

## IMPORTANT UPDATE

**Figure 3 - Trade-off between speed and cost of recovery**




Source: Adapted from Ernst and Young.

**Case Study – Business continuity management delivers improved business processes**

The State Library of Victoria is a public sector entity which aims to ensure that the documentary resources of significance relating to Victoria and Victorians are collected, preserved and made available and that Victorians have access to worldwide information resources. Over the past two years, the library has embarked upon a major initiative to:

- undertake a strategic risk assessment and business impact analysis across its full range of services and operations;
- develop a risk management framework and integrated reporting tools;
- train 'risk champions' to guide and manage the development of business continuity plans at the local work group level;
- integrate risk priorities into its internal audit program of review and action; and
- embed the practice of business continuity management into the day-to-day business of the Library, enabling efficiencies and improvements in the way it works.

An initial risk assessment of the Library's financial operations, systems and processes, resulted in a range of control improvements being identified that would deliver business efficiencies on an ongoing basis. Amongst these measures were:

- development of comprehensive documentation of all financial and budget processes and completion of a gap analysis across its operations, to support business continuity management;
- identification of core systems and operations for business continuity management and implementation of processes to ensure continuity of services – for example payroll and banking services;
- identification of enhancements to current e-commerce systems to achieve workload efficiencies and strengthen internal controls; and
- an update of policies and procedures.

Source: State Library of Victoria.

**IMPORTANT UPDATE**

## *Resilience*

One measure of a successful business continuity management program is organisational resilience. Resilient entities continue to meet organisational objectives when faced by major challenges such as natural disasters, crime, equipment failures or even terrorist attack. Resilience takes a holistic approach to help entities survive turbulent times, by integrating risk, emergency response, incident and business continuity management. Resilience arises from a combination of culture and attitude, process and framework.[5]

## *Lifecycle*

Business continuity management does not have a discrete start and end; it is a continuous and iterative process. Better practice entities manage business continuity on an ongoing basis, integrated with corporate management practices.[6]

## *IT disaster recovery*

IT disaster recovery is a term used to describe the operational response associated with the recovery of technology-based resources. Typically, these include computerised information processing systems and telecommunications. IT disaster recovery involves defining the overall strategy for recovering these resources and the activities required to implement the strategy, including timelines for recovering each specific technology component as required by the business. The availability of appropriately skilled personnel, and sourcing of specialist equipment in the event of a business disruption are two areas requiring particular attention, as business areas may make incorrect assumptions regarding these. IT disaster recovery is a part of an entity's business continuity strategy.

*Appendix 5: IT Disaster Recovery* provides more information on IT disaster recovery.

# Risk management

All entities face a variety of risks. Better practice entities manage these risks through adopting a structured, systematic process to identify and treat risks, and by implementing appropriate controls (risk treatments) that act to reduce the likelihood of disruptive events occurring.[7] However, there is no such thing as zero risk, and controls cannot guarantee that disruptive events will not occur. Controls may be ineffective, or unanticipated and unlikely events may occur.

**Therefore, for effective risk management it is important that entities design and implement controls that mitigate the likelihood that disruptive events occur, and controls that will operate once such an event has occurred.**

It is important that preventative treatments for risks align with the treatments that are part of business continuity management.

*See Appendix 6: Risk Management* for more information on risk management.

*In simple terms, a key strategic risk for any [entity] is that they will be unable to remain operational. An appropriate treatment for that risk would be to implement strategies designed to reduce the likelihood of events occurring that could lead to the disruption of operations. Additionally, it would also be necessary to produce plans of action for implementation if the disruptions do occur. All of these actions are designed to mitigate or at least reduce the risk of the [entity] ceasing to operate – they are designed to manage the continuity of the business.*

*- Standards Australia, Business Continuity Management Handbook 221:2004, 2004, p. 7.*

[5] Attorney-General's Department, Trusted Information Sharing Network, *Resilience Community of Interest,* 2008. http://www.tisn.gov.au/ [accessed 20 October 2008].

[6] The Australian *Handbook HB221:2004,* the draft Australian Standard on Business Continuity Management, the UK's *BS2599:2006,* the American *NFPA 1600,* and the Singaporean *SS540:2008* all promote a program management approach to manage business continuity.

[7] The accountability framework created by the *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act 1997* provides Chief Executives, senior management and staff with the building blocks to effectively manage risk.

**IMPORTANT UPDATE**

## Emergency response management

Emergency response management is the activity that takes place immediately after an incident has occurred. It can also be referred to as the tactical management of the situation. The primary concern of the emergency response is the safety of people. During an incident, emergency response may include evacuation of a building, liaison with emergency services, initial assessment of damage that has occurred and implications for the entity.

Emergency response management involves managing an emergency that affects the entity (for example one of the entity's buildings has flooded and requires evacuation). This is a different activity to community emergency response management, which involves the entity managing the impact of an emergency on the community (for example a town has flooded and residents require evacuation, shelter, food, and monetary payments to be organised by entities). In some cases, an entity may be required to manage both an emergency response - and activate its business continuity plan - and manage a community emergency response (for example if a flood affected the entity's building and the town).

Managing a community emergency is not within the scope of this better practice guide, however *Analysing the entity and its context* discusses the challenge of managing business continuity while simultaneously managing a community emergency response.

*See Appendix 2: Emergency Response Management* for more information on emergency response management.

*It is not the strongest species that survive, nor the most intelligent, but the ones most responsive to change.*

*- Attributed to Charles R. Darwin.*

## Incident management

Incident management is the overall management of the incident and includes the strategic decision making process. It includes obtaining information about the incident, making the decision about whether an incident is escalated to a business disruption, and invoking the business continuity plan(s) when necessary. The management of communication with stakeholders, staff and other interested parties such as the media is a focus area.

**In small, non-complex or less time-critical entities, emergency response management and incident management is often combined into a single set of activities, and performed by the same team.**

**In entities that are large, complex, or geographically dispersed, the use of separate emergency response, incident management and business continuity management teams increases the need for clear roles and responsibilities, and effective communication.**

*See Appendix 3: Incident Management* for more information on incident management.

## Developments in business continuity management since *Keeping the wheels in motion* was published in 2000

*Since Business Continuity Management: Keeping the wheels in motion* was published in 2000, there have been a number of fresh challenges for business continuity management affecting Australian public sector entities. Examples include the requirement to prepare for a pandemic,[8] whole-of-government responses

[8] See *Commonwealth Government Action Plan for Influenza Pandemic,* 2007, The Deputy Secretaries Interdepartmental Committee on Influenza Pandemic Prevention and Preparedness.

**IMPORTANT UPDATE**

to 'wicked' problems,[9] recent government reviews,[10] an increased need to work with other entities in order to manage interdependencies, and an improved understanding of the importance of building entity resilience. New Australian and international standards and guidance documents that provide direction for managing a business continuity program have also been developed.

**The ANAO does not recommend which standard an entity should adopt, nor does it endorse any specific standards.**

Key contemporary Australian business continuity references include:[11]

- *Business Continuity Management, Prudential Standard* LPS 232, 2007, Australian Prudential Regulation Authority.
- *Business Continuity Management (authorised deposit-taking institution), Prudential Standard* APS 232, 2005, Australian Prudential Regulation Authority.
- *Business Continuity Management (general insurer), Prudential Standard* APS 222, 2005, Australian Prudential Regulation Authority.
- *Connecting Government: Whole of government responses to Australia's priority challenges,* 2004, Management Advisory Committee.
- *Handbook: A practitioners guide to business continuity management,* HB 292-2006, 2006, Standards Australia.
- *Handbook: Business Continuity Management,* HB 221:2004, 2004, Standards Australia.
- *Handbook: Executive guide to business continuity management,* HB 293-2006, 2006, Standards Australia.

A number of countries have published standards on business continuity management. These include the United Kingdom and the United States of America.[12] Selected international business continuity references are provided in *Appendix 7: Australian and International References*.

Better practice entities are aware of business continuity management standards and guidance documents that are relevant to their operating context, and use this information to tailor their business continuity management approaches.

There are also a number of entities working to build the business continuity capability of the Australian Government, and to foster increased inter-entity co-ordination. The Attorney-General's Department is the lead agency responsible for promoting resilience (including business continuity management) in the Australian Government. The Attorney-General's Department provides accredited business continuity

[9] An example of a 'wicked problem' is climate change. See *Tackling Wicked Problems: A Public Policy Perspective,* 2007, Management Advisory Committee.

[10] For example, *Review of the Australian Government's use of information and communication technology,* August 2008, Sir Peter Gershon CBE FERng and the Attorney-General's Department's *Whole-of-Government Review of E-Security* conducted in 2008.

[11] These references were current at the time of publishing this guide.

[12] At the time of publishing this guide, a draft-for-public-comment Australian business continuity management standard (issued by Standards Australia), and a draft-for-public-comment international business continuity management standard (issued by the International Standards Organization) were expected to be released in 2009.

**IMPORTANT UPDATE**

management training, and has created a resilience 'community of interest'.[13] Comcover benchmarks entities progress in establishing their business continuity frameworks, and provides training to staff from Australian public sector entities on business continuity management. The Australian Government Information Management Office is responsible for the establishment of a single policy framework for the continued delivery of Government services in the event of a disruption and/or failure of Government-operated Information and Communication Technology.

## Generic characteristics of business continuity management in public sector entities

Better practice entities understand the key characteristics of business continuity management and building entity resilience. They implement a program that is relevant, appropriate and cost effective, in light of the entity's circumstances and operating context. For example, entities that are small, non-complex and perform less time-critical functions have different business continuity requirements and will apply business continuity management differently to entities that are large, complex, and perform time-critical functions.

The ANAO's analysis of public sector business continuity implementation has identified some generic characteristics associated with better practice business continuity management programs.[14] These are depicted in Table 1. This is not a prescriptive 'black and white checklist' for a business continuity management program – as noted throughout this better practice guide, the development and implementation of a business continuity program needs to be relevant to the entity's operating context.

[13] This training and community of interest is currently run through Emergency Management Australia.

[14] There are several models in the marketplace (for example the Capability Maturity Model Integration and the Control Objectives for Information and Related Technology) which also provide assessment criteria for business continuity implementation, and the impact on business objectives of IT weaknesses.

**Table 1 - Characteristics of better practice business continuity management in public sector entities**

Notes: Basic level characteristics are generally found in small, non-complex or less time-critical entities. In addition to the basic level characteristics, mature level characteristics are found in mature, large, complex, geographically dispersed or critical entities. Throughout this better practice guide, there is a series of checkpoints, where entities can check their progress against the characteristics.

| Characteristics | Basic level criteria | Mature level criteria | Chapter reference in this guide |
|---|---|---|---|
| 1. A business continuity management framework is in place. | • Accountability and responsibility for key areas (for example IT disaster recovery, business resumption) were defined at the time that the framework was implemented.<br>• There are clearly defined and approved management processes to manage business continuity.<br>• The framework includes a business impact analysis.<br>• The framework addresses roles, tasks, and responsibilities of internal and external providers (for example interdependencies).<br>• The framework links with the entity's risk assessment and management strategy.<br>• The framework includes a policy for testing and exercising business continuity. | • The entity maintains a register of changes to the business continuity program that may result from outcomes of corporate risk assessment procedures and the outcomes of continuity testing and compliance/monitoring reviews.<br>• The business continuity plan is periodically updated to reflect and respond to changes in the entity or to government requirements.<br>• The entity has defined roles for the business continuity program's:<br>– sponsorship (organisational and financial support);<br>– ownership (direct accountability and responsibility for program execution and support); and<br>– custodianship (responsibility for the co-ordination of business continuity management tasks). | **Managing business continuity as an integrated program of work** |

IMPORTANT UPDATE

| Characteristics | Basic level criteria | Mature level criteria | Chapter reference in this guide |
|---|---|---|---|
| 2. Training and awareness of business continuity has been conducted. | • Response/recovery team members have received training.<br>• All staff received training or were required to attend an awareness session at the time the initial framework was implemented. | • New starter/induction/Human Resource policies require attendance at an awareness session on risk management, incorporating business continuity.<br>• Staff are trained on business continuity plans, IT disaster recovery plan and pandemic plan.<br>• An awareness program to advises staff of the broad nature of business continuity. | **Embedding business continuity management into the entity's culture** |
| 3. A risk assessment has been conducted. | • A risk assessment for each core business function and IT service has been undertaken, to identify the assets, threats, vulnerabilities and controls in place for each activity. | • There is a direct link between the entity's risk management and business continuity management processes and activities.<br>• Disruption scenarios, to which the entity may be vulnerable, including the effect of interdependencies with third parties/ suppliers, have been identified and prioritised.<br>• The entity has considered the 'detectability' of an event.<br>• The entity has 'scheduled' recurring risk assessments and business impact analyses. | **Analysing the entity and its context** |
| 4. A business impact analysis has been conducted. | • Recovery objectives and priorities for business and technology have been established and there is an associated justification for each.<br>• Interdependencies of processes have been identified. | • Critical resources, facilities, equipment, vital records, data and infrastructure have been identified and catalogued. | |

IMPORTANT UPDATE

| Characteristics | Basic level criteria | Mature level criteria | Chapter reference in this guide |
|---|---|---|---|
| 5. Preparatory controls have been implemented. | • The continuity strategies that best meet the entity's needs have been implemented based on a cost-benefit analysis. | • Costs and benefits are re-assessed on a periodic basis. | **Designing the entity's business continuity approach** and **Building entity resilience** |
| 6. The entity has documented, and the executive has endorsed, its business continuity plans and framework. | • The business continuity plan is documented and endorsed.<br>• The business continuity plan is up-to date.<br>• For larger agencies, the entity level plan is supported by a number of operational level business continuity plans. | • Response, recovery and restoration procedures are documented, approved by senior management, and communicated to staff to enable effective continuity operations.<br>• There is pandemic planning.<br>• There is IT disaster recovery planning. | |

IMPORTANT UPDATE

| Characteristics | Basic level criteria | Mature level criteria | Chapter reference in this guide |
|---|---|---|---|
| 7. Business continuity testing and exercises and have been conducted. | • Testing and exercising of certain scenarios has occurred. | • The entity has identified the benefits of continuously improving business continuity strategies and plans.<br>• Validation and regular testing of continuity strategies is a key component of the entity's corporate risk assessment framework.<br>• The testing and exercising schedule for business continuity plans, IT disaster recovery plans, and pandemic plans is documented.<br>• Testing and exercising for business continuity and IT disaster recovery are integrated.<br>• Critical business processes have been tested and exercised.<br>• The entity has utilised a range of test and exercise options, and has incorporated actual data or real-world conditions and engaged suppliers/vendors as required.<br>• Plans are updated and revised following testing and exercising. | **Maintaining the program and plan: Testing, exercising, updating and reviewing** |
| 8. The entity monitors business continuity. | • An internal audit or external review of the implemented framework has been undertaken. | • Compliance with the business continuity framework, and the framework's alignment with industry standards/government requirements is periodically reviewed based on an internal policy. | |

Source: ANAO analysis of audits of the Financial Statements of General Government Sector Agencies, various years.

**IMPORTANT UPDATE**

# Managing business continuity as an integrated program of work

Initiation

> Ongoing management

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**



# Managing business continuity as an integrated program of work

This section provides guidance for entities on developing a business continuity plan (if one is not already in place) and then embedding and integrating the ongoing management of the business continuity program into business-as-usual governance activities.[15]

*The time to repair the roof is when the sun is shining.*

*- John F. Kennedy.*

## Initiation

The business continuity plans of entities are typically developed using a project management approach. This approach requires determining the objectives, scope, and boundaries of the business continuity project, a manager or management committee responsible for the project, and budget allocated to the project. The project reflects the size and complexity of business continuity issues in the entity.

### *In-house v contracted development of the business continuity program*

***A key consideration of entities at this stage is the decision whether to develop the business continuity plan and program internally, or engage a consultant to assist with all or part of the process. Both options have advantages and disadvantages.***

***Entities may have more 'ownership' of internally developed business continuity plans, and the preparation of the business continuity plan is itself a valuable process for the entity. As Dwight D. Eisenhower pointed out: plans are worthless but planning is everything.***

***However, it may be difficult to find internal resources with the same level of experience and skill in implementing business continuity as a consultant.***

***A cost effective option for entities may be to use the experience of other Australian Government entities. For example, staff from the business continuity team in the Department of Families, Housing, Community Services and Indigenous Affairs have assisted the Department's portfolio agencies such as Aboriginal Hostels Limited and the Equal Opportunity for Women in the Workplace Agency to develop their business continuity plans. Staff from the business continuity team in the National Library of Australia have assisted state libraries by sharing their business continuity plan and discussing experiences.***

***Alternatively, entities may find a blended team of staff and consultants may be the most appropriate skill set to develop the business continuity program. Entities such as Comcover and the Attorney-General's Department (through Emergency Management Australia) are also able to provide training and information to assist entities in preparing their business continuity management program and plan.***

[15] A program is a flexible organisation created to coordinate, direct, and oversee a series of related projects and activities in order to deliver outcomes and benefits related to the organisation's strategic objectives (Office of Government Commerce, *Managing Successful Programs*, United Kingdom, 2007, p. 4).

**IMPORTANT UPDATE**

## Ongoing management

*[Business continuity program] management enables the business continuity capability to be both established (if necessary) and maintained in a manner appropriate to the size and complexity of the organization.*

*- British Standard, Business Continuity Management – Part 1: Code of practice, BS25999-1:2006, 2006, British Standards Institution, p. 8.*

The cornerstone of effective ongoing management of business continuity in an entity is developing and implementing a robust governance framework. Entities that have done this well have integrated business continuity management into their existing governance framework. Governance aspects of the business continuity management program to consider include:

- sponsorship;
- ownership;
- custodianship;
- stakeholder relationships;
- planning;
- performance monitoring;
- evaluation and review; and
- enterprise information architecture.

### *Sponsorship*

Executive leadership is crucial to the success of the business continuity capability. This sponsorship needs to manifest itself in both actions and words. In better practice entities, the executive:

- maintains an awareness of business continuity management, and receives business continuity management training;
- contributes to business continuity awareness raising in the entity;
- participates in business continuity testing and exercising;
- appropriately resources the business continuity function;
- endorses a business continuity management policy; and
- endorses key business continuity documents such as the business impact analysis and business continuity plan.

**The Workbook contains a checklist of governance questions for the executive to consider. See p. 93**

**The Workbook contains a checklist of governance questions for the committee responsible for overseeing business continuity management to consider. See p. 94**

### *Ownership*

In better practice entities, a person or committee with appropriate seniority is nominated as having direct responsibility for business continuity program execution and support.[16] The accountable party provides overall direction and drive for the program, and their responsibilities may include establishing milestones and performance reporting requirements, authorising new versions of the business continuity plan, and approving the test and exercise schedule and scenarios.

**The Workbook contains an example of responsibilities for various business continuity roles. See pp. 95-98**

### *Custodianship*

Responsibility for the day-to-day implementation and coordination of business continuity management tasks needs to be assigned to one or more individuals. The custodian(s) tasks generally include updating documentation, promoting awareness across the entity, administering the test and exercise program,

[16] Some larger agencies have developed an internal risk and business continuity governance committee. This committee then reports to the Executive and/or the Audit Committee.

**IMPORTANT UPDATE**



and coordinating reviews of the business impact analysis. It is important that the custodian(s) receive training on their specific role, as well as good practice in business continuity management generally. In smaller entities, the custodian typically also has a role in the business continuity plan such as the incident manager, or recovery coordinator.

## *Stakeholder relationships*

Business continuity management is not an isolated process. To develop a resilient entity, consideration needs to be given to involving internal stakeholders (for example security management, emergency response management, business process owners, and service owners) and external stakeholders (for example interdependent organisations, unions, and clients) at key stages of the program. This may include involving them in planning, testing and exercising, and awareness raising activities.

## *Planning*

The business continuity plan should be subject to systematic review. Integrating the update of the business continuity plan into the entity's annual planning cycle ensures this is done annually and creates efficiencies. Contact details should be updated more frequently. A schedule of testing and exercising should also be developed. Better practice agencies have developed a 'universe' to ensure comprehensive testing and exercising of all processes, and that test and exercise types occurs at regular intervals over several years.

## *Performance monitoring*

A structured and regular system of performance monitoring supports the effective management of a business continuity program. Entities need to have systems in place for at least annual reporting to the person or committee responsible for overseeing business continuity management. As the frequency of business continuity reporting depends on the nature of the entity and other risk reporting, more frequent reporting (such as on a biannual or quarterly basis) may be appropriate for some entities. This reporting includes the status of the business continuity plan and follow-up of post incident reviews from any exercises that have been conducted or any incidents that have occurred during the period. Better practice entities also report on performance indicators, such as the availability of service delivery channels, the timeliness of restoring critical business processes when a business disruption event occurs, and customer/stakeholder satisfaction. Many agencies also choose to report business continuity management to the audit committee as a distinct agenda item (separately from risk management activities).

## *Evaluation and review*

Better practice entities periodically evaluate compliance with the business continuity framework and the framework's alignment with industry standards, based on an internal policy. This may be through an internal audit or external examination of the implemented framework. Business continuity arrangements and plans should be reviewed both on a periodic basis and as a result of 'trigger' events. Some examples of review triggers are changes to the entity's outcomes and outputs, machinery-of-government changes, major changes to personnel or technology, a change in physical location, or following a test, exercise or an actual business disruption that has highlighted deficiencies.

*An Audit Committee's responsibilities, in relation to risk management, would generally be to review … whether a sound and effective approach has been followed in establishing the entity's business continuity planning arrangements, including whether disaster recovery plans have been tested periodically.*

*- ANAO Better Practice Guide, Public Sector Audit Committees, 2005, p. 10.*

*The [Audit] committee should, at least once a year, report to the Chief Executive/Board on its operation and activities during the year. The report could include … summary of the committee's assessment of the entity's risk and control framework, including the entity's business continuity preparedness, and details of emerging risks facing the entity.*

*- ANAO Better Practice Guide, Public Sector Audit Committees, 2005, p. 21.*

**IMPORTANT UPDATE**

### *Enterprise information architecture*

Consideration should be given to the way in which the information architecture of the entity is designed. Especially in respect to technology, it is important that entities consider whether their information architecture can be changed or improved to a) minimise the impact of a business disruption; and b) reduce the costs of risk treatments. For example, information architecture may be improved by reducing reliance on a single place of employment through remote access.

## Implementing a business continuity management program - Checkpoint 1

Entities that are developing a business continuity management program for the first time, or reinvigorating an existing program, will find it useful to monitor their progress One method of doing this is by checking progress against better practice implementation characteristics.

| Checkpoint 1 | Generic characteristics of better practice business continuity management in public sector entities | Completed | Level of implementation |
|---|---|---|---|
| | Characteristic 1: A business continuity management framework is in place. | Yes / No | Basic / Mature |

Table 1 on page 9 of this better practice guide provides details on the implementation characteristics.

**The Workbook contains an example business continuity management framework diagram.**
**See p. 99**

**Further references**

- *Governance, risk management and control assurance* HB 254-2005, Standards Australia, 2005.
- *Implementation of Programme and Policy Initiatives Better Practice Guide,* 2006, Department of the Prime Minister and Cabinet and Australian National Audit Office.
- *Implementation of Programme and Policy Initiatives Pocket Guide,* 2006, Department of the Prime Minister and Cabinet and Australian National Audit Office.
- *Managing Successful Programs,* 2007, United Kingdom, Office of Government Commerce.
- *Public Sector Governance,* Better Practice Guide Volumes 1 & 2, 2003, Australian National Audit Office.
- *Public Sector Audit Committees,* Better Practice Guide, 2005, Australian National Audit Office.

**IMPORTANT UPDATE**

# Embedding business continuity management into the entity's culture

Executive sponsorship

Integrating business continuity management within change management

Training and raising awareness

# IMPORTANT UPDATE

**IMPORTANT UPDATE**

# Embedding business continuity management into the entity's culture



This section provides guidance to entities on embedding business continuity management into their organisational culture.

Successful business continuity management relies on expertise from within the entity – it is the people that understand the entity – its objectives, processes and risks.

Throughout business continuity management processes, there are opportunities to embed business continuity management into the entity's culture, to ensure it becomes part of the entity's core values and business-as-usual management.

## Executive sponsorship

As mentioned earlier, executive sponsorship is a key input to the success of the business continuity capability. Successful business continuity management requires a commitment from the executive to raising awareness and implementing sound approaches to build resilience.

One way the executive can promote business continuity within the entity is through an endorsed business continuity management policy. A business continuity management policy sets out the entity's agreed priorities, the business continuity management framework, and responsibilities for the program. **The policy needs to be appropriate to the entity's scale, complexity and the nature of its operations.**

While a 'top-down' approach is necessary for embedding business continuity management into an entity's culture, this will work best when also accompanied by a 'bottom-up' approach, as described in the following case study.

*Resilience is not a plan, or a checklist. The capacity of resilience is found in an organisation's culture, attitudes and values. In creating appropriate knowledge, culture, attitudes and values, an organisation builds its capacity to survive the turbulence created by low frequency and high consequence risks.*

*- National Organisational Resilience Framework Workshop - The Outcomes, 5–7 December 2007, Emergency Management Australia.*

**The Workbook contains an example table of contents for a business continuity management policy, and examples of statements of a business continuity policy. See pp. 101-102**

**IMPORTANT UPDATE**

*[The Management Advisory Committee] expects senior executives to play a strong role in fostering a diverse workforce with the necessary skills and aptitudes for future organisational capability and resilience.*

*- Management Advisory Committee, Managing and Sustaining the APS Workforce One APS One SES, 2005, p. 5.*

**Case Study – Combining a 'Top-Down' and 'Bottom-Up' approach to embedding business continuity management into the entity's culture**

For the purposes of its internal business continuity management planning, a public sector entity uses both a 'top-down' and 'bottom-up' approach to embedding business continuity management into its culture.

**Top-down** – The entity has created a Risk Management Committee, which is responsible for overseeing the department's strategic risks, and monitoring divisional risk management and business continuity activity. The committee is chaired by a Deputy Secretary and includes senior executives and representatives from each division. It liaises closely with the Audit Committee. With respect to business continuity, the committee has endorsed the critical business processes arising from the business impact analysis, overseen the implementation of recommendations flowing from the entity's business continuity exercises, and approved the update of business continuity plans (including the pandemic plan). The Secretary approves the exercising schedule, and the Secretary and Executive Management Team have participated in discussion-based business continuity exercises. This participation and visible support from the Secretary and senior executives clearly establishes business continuity as an entity priority.

**Bottom-up** – The entity has developed an internal Risk and Business Continuity Network. This is an informal, but structured network, consisting of staff with a business continuity role. It is also open to anyone who has an interest in business continuity generally. The network played a key role in the conduct of the business impact analysis. Business continuity staff have accreditation through the Attorney-General's Department's (Emergency Management Australia's) training program at Mt Macedon, and business continuity awareness is included in induction material for new staff. Business continuity information is also available on the entity's intranet and is embedded into the regular risk management training staff receive.

Source: ANAO analysis of entity information.

## Integrating business continuity management within change management

The business continuity plans and business impact analysis should be revalidated when an entity's circumstances have significantly changed from when they were initially developed. Considering business continuity implications as part of an entity's change management process assists in embedding business continuity management into the entity's culture. Some examples of changed circumstances that warrant review and revalidation of the business continuity arrangements include:

- significant changes to the entity's external environment;
- machinery-of-government changes;
- changes to the entity's outcomes and outputs;
- changes to the entity's risk profile;
- implementation of a new business process or activity;

**IMPORTANT UPDATE**

- initiation of a new major project;
- outsourcing of an existing process or activity, or entering into a major contract;
- internal restructuring;
- major changes to personnel or technology;
- changes in physical location (for example a new building);
- a key new interdependent relationship; and
- following an exercise or a business disruption event that has highlighted deficiencies.

Maintaining the business continuity program through periodic reviewing is discussed on page 65 of this better practice guide.



## Training and raising awareness

Training and awareness activities form important components of managing a business continuity program. Such activities assist in providing an understanding of, as well as developing skills and competencies in, business continuity management.

### *Training*

Training is a key component to the management of a business continuity program.

**Active participation in business continuity exercises is a key method of developing staff skills and competencies.** It is often necessary to provide staff with theoretical training.

Effective training is tailored to the needs of the target audience. For example:

- the executive - require training in business continuity program management; business continuity standards, guidelines and applicable legislative requirements; and incident management training as appropriate;[17]
- business continuity custodians – require training in business continuity program management; business continuity standards, guidelines and applicable legislative requirements; conducting a business impact analysis; mitigating single point of failure risks; developing and maintaining a business continuity plan; and running tests and exercises; and
- staff with a business continuity role – require training in the skills necessary to undertake their business continuity role. For example, incident managers may require media communications training, while recovery coordinators may require training in managing teams, operating in stressful situations, or negotiation skills.

[17] Standards Australia has produced a *Handbook: Executive guide to business continuity management HB 293-2006,* to provide senior management with an overview of the key concepts and processes required to implement and maintain a robust business continuity management program.

**IMPORTANT UPDATE**

Examples of business continuity training provided by Australian Government entities are listed below.

**Australian Government Business Continuity Training Providers**

| | |
|---|---|
| **Attorney-General's Department** | **http://www.ag.gov.au** |
| **Emergency Management Australia** | **http://www.ema.gov.au** |

The Attorney-General's Department (currently through Emergency Management Australia) hosts an accredited five day course in Mt. Macedon on business continuity management. The course covers business continuity management concepts and principles, and the relationship between business continuity, emergency management and risk management. The program stresses a strategic perspective with high level communication and liaison requirements.

**Comcover** **http://www.finance.gov.au/comcover**

Comcover provides a free one day course for staff from Australian public sector entities on business continuity management. The course is designed to provide an understanding of the key elements of a business continuity plan; explain business continuity management in the context of the Australian public sector; and describe the process of risk management and its relationship with effective business continuity planning. Comcover also hosts a series of benchmarking forums following the completion of the annual benchmarking program. These forums are aimed at providing the opportunity for public sector entities to share the experiences of others in implementing an enterprise-wide risk management framework.

*When planning for a year, plant corn. When planning for a decade, plant trees. When planning for life, train and educate people.*

*- Chinese proverb.*

## *Raising awareness*

An ongoing education and information program for staff can raise and maintain awareness of business continuity management and why it is important to the entity. Staff particularly need to be aware of the crucial role they play in maintaining the delivery of products and services, and that business continuity management has the ongoing support of the executive. Better practice entities include business continuity issues in induction training for new staff.

Effective communication can instill confidence in stakeholders of the entity's ability to cope with business disruption events. Better practice entities extend their business continuity awareness activities to interdependent organisations, such as suppliers and other portfolio entities.

The British Standard, *Business Continuity Management – Part 1: Code of practice, BS25999-1:2006* (p. 41) recommends the following activities for awareness raising:

- a consultation process with staff throughout the entity concerning the implementation of the business continuity management program;
- discussion of business continuity management in the entity's newsletters, briefings, induction program or journals;
- inclusion of business continuity management on relevant web pages or intranets;
- learning from internal and external incidents;

## IMPORTANT UPDATE

- business continuity management as an item at team meetings;
- exercising continuity plans at an alternative location; and
- visits to any designated alternative location (for example a recovery site).

**Case study – Awareness Raising**

A medium size public sector entity uses passive and active methods to increase staff awareness of business continuity management. It has a business continuity 'portal' on its intranet (with plans, contacts, training, and links to external information), a risk management community of practice (with regular internal and external speakers on topics such as business continuity) and regularly includes communiqués in its internal newsletter. The entity's business continuity management team have found the key to awareness raising is to make information relevant to staff. An example of a communiqué is:

*Business Continuity: An Introduction*

*Have you ever wondered what would happen if you lost access to your personal drive? For a day? A week? Longer?*

*How would your business team operate if half your staff/colleagues could not make it to work (due to illness, severe transportation problems etc). For a day? A week? Longer?*

*Business Continuity is the planning process that aims to create a logical, documented, set of procedures and plans that aims at ensuring that critical business processes are maintained at all times, or at least recovered as quickly as possible in the event of a serious event.*

*The Entity's Risk Management Team is charged with implementing this planning process.*

*The annual review of the plans is currently being coordinated by the Entity's Business Continuity Manager. The review involves contacting each business team and identifying critical business functions, the resources required to support the functions and the development of mitigating procedures and recovery strategies.*

*Look out for more information on business continuity in future articles on Insight.*

*In the mean time if you require further information please feel free to contact The Entity's Business Continuity Manager.*

Source: ANAO analysis.



**The Workbook contains an example program for business continuity training and awareness. See p. 103**

**IMPORTANT UPDATE**

## Implementing a business continuity management program - Checkpoint 2

| Checkpoint 2 | Generic characteristics of better practice business continuity management in public sector entities | Completed | Level of implementation |
|---|---|---|---|
| | Characteristic 2: Training and awareness of business continuity has been conducted. | Yes / No | Basic / Mature |

Table 1 on page 9 of this better practice guide provides details on the implementation characteristics.

IMPORTANT UPDATE

# Analysing the entity and its context

Identify critical business processes

Undertake a business impact analysis

# IMPORTANT UPDATE

**IMPORTANT UPDATE**

# Analysing the entity and its context

This section provides guidance on how entities can analyse their operations and environment. This involves the identification of critical business processes, and the activities and resources that support them. The identification of internal and external interdependencies is also important. Once all of these elements have been identified, it is possible to analyse the consequences of a business disruption. This process is commonly referred to as a business impact analysis.

## *Whose input is needed?*

***Business continuity management is not an isolated process, to be conducted by a single team in the corporate area. Rather, it is essential that representatives from across the entity are involved. In addition to representatives from operational areas, internal stakeholders in the business continuity management program may include:***

- ***Information technology / information systems.***
- ***Risk management.***
- ***Emergency response management.***
- ***Property services / facilities and security.***
- ***Internal audit.***
- ***Occupational health and safety.***
- ***Finance / insurance.***
- ***Media/ communications.***



## *Link with risk management*

Better practice entities are able to demonstrate a direct link between the entity's risk management and business continuity management processes and activities. One way to do this is to share (or co-create) entity information that is necessary for both risk management and business continuity management. For example, a risk assessment for each core business function and IT service, which identifies the assets, threats, vulnerabilities and controls in place for each activity, would assist in analysing the entity and its context from a business continuity perspective. Disruption scenarios, to which the entity may be vulnerable, including the effect of interdependencies with third parties/suppliers are another valuable piece of information.

*Business continuity management is all about understanding the subject matter and applying common sense.*

*- Continuity Central, Business continuity quotations: volume two.*

## Identify critical business processes

The critical business processes of the entity are those processes essential to achieving business objectives. A structured approach to identifying critical business processes requires entities to:

- define critical business processes;
- categorise and rank critical business processes;
- identify interdependent business processes; and
- determine the minimum requirements for each critical business process.

**IMPORTANT UPDATE**

## *Define critical business processes*

It is important to have a clear and agreed understanding of the entity's business objectives, and the critical business processes which ensure those objectives are met.

Good starting points to achieve this understanding are high-level planning documents such as corporate plans, business plans and operational plans. These plans have already documented the entity's business objectives and assessments of key risks.

### *Is a process really critical?*

***It is important for the business continuity management program that the critical business processes are identified.***

***While entities may begin with identification of all business processes, it is necessary to distil these down into a prioritised list of critical processes. That is, those processes which have to be performed in order to enable the entity to meet its most important objectives.***

***Other processes will need to be recovered in the event of a business disruption, and may require advance arrangements to be put in place. However, the focus of business continuity management is preventing, and recovering from, disruptions to critical business processes.***

***There may be an interdependent and synergistic relationship between processes. Therefore, if a non- critical business process is an input into a critical process, it should also be treated as a critical process.***

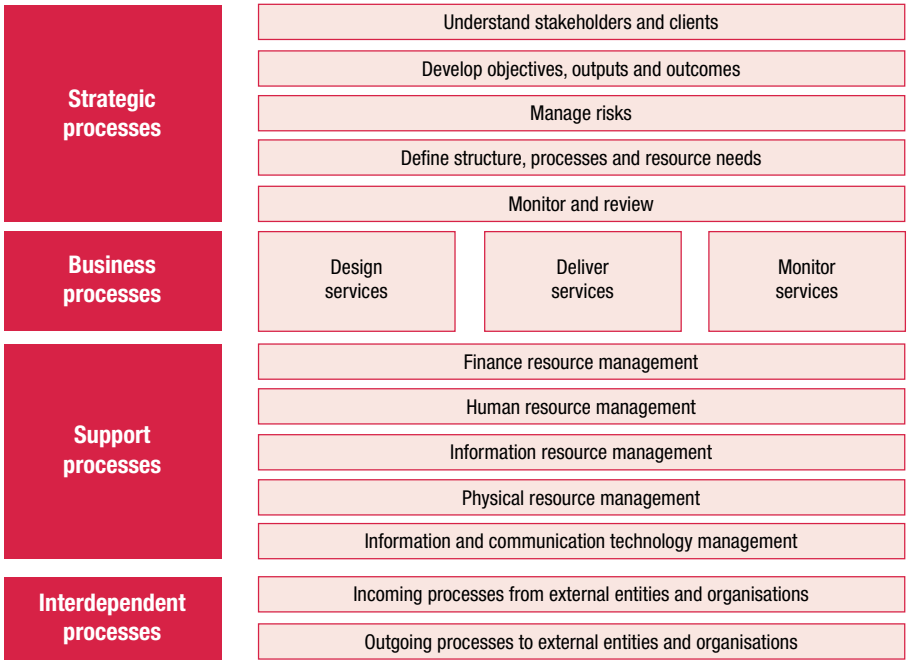
***The definition of what constitutes a critical business process depends on the context and circumstances of the entity. In some cases, the entity may only have one or two critical processes.***

***When determining critical processes, staff may feel threatened, particularly if their role is identified as being part of a non- critical process. Alternatively, they may incorrectly categorise non-critical processes as critical, due to the importance these processes have in their immediate work environment. It is important for management to be sensitive to this sentiment.***

To assist in achieving consistency in terminology and common agreement in process definition, entities may wish to utilise a business process classification scheme. Classification schemes provide generic categorisations of business processes common to entities. An example of a classification scheme is provided in Figure 4. This diagram outlines the high level business processes categorised between strategic, business (operational), support and interdependent processes. Within each process classification are a number of major business processes.

**IMPORTANT UPDATE**

**Figure 4 - Example of a process classification scheme**




## *Categorise and rank critical business processes*

Critical business processes need to be ranked in order of their importance to the entity. This ranking reflects the importance of the business process to achieving business objectives. The ranking of critical business processes may consider such issues as:

- failure to meet statutory obligations for service delivery;
- failure to meet key stakeholder expectations;
- loss of cash flows essential to business operations;
- the degree of dependency on business processes by internal business units or clients;
- cumulative damage to the entity by the disruption to the critical process; and
- reputational consequences.

To determine the ranking, it is important that the concerns of executive and senior management are obtained regarding business priorities and continuity issues. Structured interviews and/or facilitated group meetings are tools for gathering this information.

In a small or non-complex entity it may be possible to gather this information from one group meeting. This has the added advantage of ensuring participants are aware of all entity priorities and can agree on the ranking of critical processes, together with their corresponding activities and resources.

In a larger or complex entity it will generally be necessary to conduct a series of interviews or facilitated group sessions. In either event, it is important that the information collected through these approaches is reported back to the participants for their confirmation.

**IMPORTANT UPDATE**

**Executive endorsement**

Executive endorsement of the critical processes is necessary before proceeding to the next stage.

## *Identify interdependent business processes*

*The APS operates in a rapidly changing, devolved environment which demands significant organisational agility and responsiveness, and a flexible, collaborative approach to public administration.*

*- Management Advisory Committee, Managing and Sustaining the APS Workforce One APS One SES, 2005, p. 2.*

An interdependency is a reciprocal relationship. It involves a reliance, directly or indirectly, of one process, activity or resource upon another. An entity could be dependent on receiving a process or information from another entity or organisation as an input to one of its critical business processes. Conversely, external entities and organisations may be dependent on the output of the entity to deliver a critical business process.

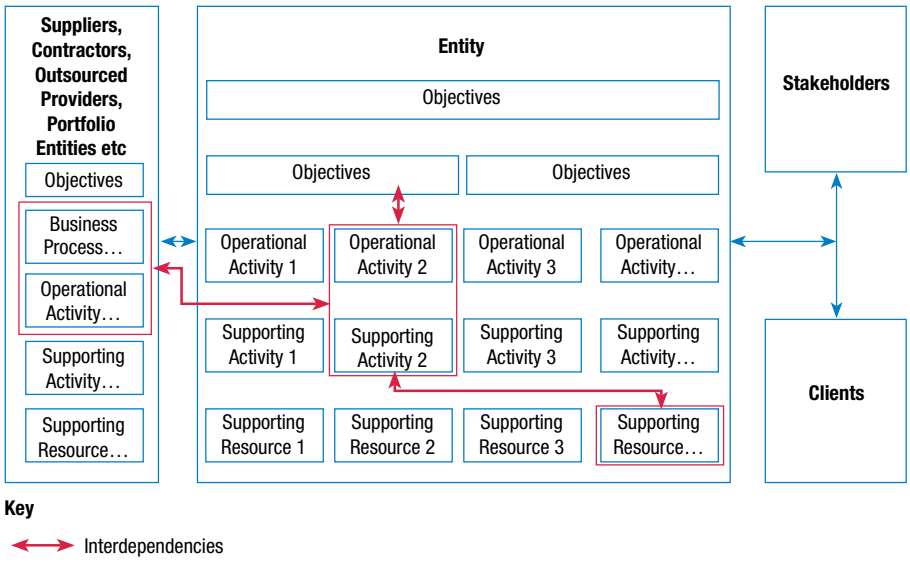
When attempting to understand their critical business processes, entities need to define external interdependent processes. This means understanding key personnel, key failure points, contractual obligations, service level agreements and memorandums of understanding. Considerations include customers, suppliers, portfolio agencies, contractors and regulators.

Entities may use the determination of interdependencies as an opportunity to gather information such as addresses, contact phone numbers (business and after hours) and email addresses of key personnel in the external agency, to input into the business continuity plan. This contact information will need to be updated on a regular basis.

In larger entities, consideration should also be given to internal interdependent processes between business units.

Figure 5 depicts one way of thinking about and identifying interdependencies in an entity.

**Figure 5 - Identifying interdependent business processes**




Source: Adapted from *Understanding the organisation in the light of BS 25999-2,* Malcolm Cornish FBCI, BCI Symposium 18-19 October 2007.

**IMPORTANT UPDATE**

## What level of business continuity assurance should an entity seek for an external entity it is reliant on?

**In some cases, it may be appropriate for the entity to review the external entity's business continuity plan and arrangements. For relationships with private organisations, this may necessitate prior inclusion of a relevant clause in contracts.**

**The National Blood Authority (NBA) requires suppliers to manage risk and business continuity as standard clauses in all of its contracts. As outlines below:**

*The Supplier must within 30 Business Days of the Commencement Date, provide to the NBA a Risk Management Plan that complies with the requirements of this clause. After the Risk Management Plan is approved by the NBA, it will become part of this Deed.*

*The Supplier agrees to implement the Risk Management Plan to manage the risks in relation to the Product, including but not limited to risks listed the Risk Management Schedule. In addition, the Parties at all times, to the extent possible, agree to comply with the requirements or procedures identified in the Risk Management Plan.*

*The Supplier must notify the NBA of:*

- *any new risks which arise during the Term of which it becomes aware, which are not appropriately or adequately dealt with in the Risk Management Plan;*
- *any changes to existing risks in the Risk Management Plan during the Term; and*
- *the Supplier's proposed method for dealing with any new risks or changes to existing risks which arise during the Term.*

*The Parties must conduct negotiations in good faith to update the Risk Management Plan to implement processes to manage new or changed risks which arise during the Term (including any risks which are identified by the NBA and notified to the Supplier from time to time).*

*Risk Management Schedule*

*The Supplier must implement and maintain appropriate risk management strategies that will identify, mitigate and control all risks which may affect the supply of the Products including but not limited to risks of:*

- *failure of subcontract arrangements (including alternative subcontract arrangements, performance guarantees etc);*
- *failure to supply Products (including alternative supply arrangements);*
- *product recall (including strategies to retrieve recalled products and to supply replacement products);*
- *unauthorised access or use of, loss or destruction of, or damage to, Products (strategies to immediately identify damaged products and replace damaged products);*
- *delivery failure (strategies to immediately identify delivery failure and implement alternative suitable delivery arrangements);*
- *theft of Products (appropriate security arrangements including security of premises and delivery arrangements and arrangements to provide replacement of product); and*
- *fraud.*

*The Risk Management Plan must also incorporate a disaster/emergency action plan, which sets out:*

- *the steps which the Parties will take in the event of a disaster or emergency occurring;*
- *the responsibilities of each Party, particularly the Supplier, and the tasks to be performed; and*
- *a procedure for, with the written approval of the NBA, introducing new, or revising existing, risk management strategies to take account of new or changed risks.*

Source: National Blood Authority

**Entities should seek appropriate legal advice before including business continuity clauses in contracts.**

## IMPORTANT UPDATE

**Case study – Interdependencies**

The NSW Police Force is Australia's largest policing organisation, with approximately 20 000 employees (including 15 000 sworn officers) and 500 police stations.

**Developing a business continuity framework** - In 2008 the NSW Police Force won an Australian Business Award for 'Innovation' for developing their business continuity framework. The framework adopts an innovative approach to business continuity planning, through a logical step-by-step sequence designed to identify and prioritise the entity's operating activities, and develop solutions to six generic disruption scenarios. The framework is a consequence based approach, rather than being incident driven. Also, rather than focusing on the length of time for which the entity might operate without critical resources, the framework allows the entity to identify the critical operating activities, and focus their efforts on maintaining these activities, as distinct from routine or discretionary activities. The framework includes a simple *8 Step Guide to Business Continuity Plan Development and Maintenance,* which was deployed to local police areas. Step one involved local areas identifying all of their business unit's activities, and classifying them as 'Critical', 'Routine' or 'Discretionary'. This step is similar to a traditional business impact analysis. The second step involved grouping critical, routine and discretionary activities, and identifying the partnership dependencies that exist for the activities.

**Identifying interdependencies** - Examples of interdependencies that were identified included major custody stations' reliance on Corrective Services staff to handle prisoners, reliance on laboratories for processing crime scene DNA, and reliance on energy providers to power facilities.

**Involving interdependent organisations in business continuity management** - Local police commands and specialist business units were encouraged to involve representatives from partnership entities to be involved in the development of workarounds for their business continuity plan. For example, representatives from NSW Maritime Services, three ports corporations, volunteer marine rescue groups, the Australian Maritime Safety Authority and AusSAR were involved in the development of the Marine Area Command's workarounds for its critical activities of Emergency Response, Port Security, Boat Safety and Search & Rescue, when its own capacity is rendered ineffective due to the unavailability of such essential operational elements as vessels/crew or suitable command facilities. This process included identifying suitably trained staff to supplement police crews, suitable vessels which can be 'loaned' or seconded to police duties, establishing appropriate responses by other organisations in lieu of police resources for port security, and establishing secondary Emergency Operations Centres and Search and Rescue Coordination Centres.

Source: ANAO analysis.

**IMPORTANT UPDATE**

## *Whole-of-Government Critical eServices*

The Department of Finance and Deregulation, through the Australian Government Information Management Office, has been charged with the establishment of a single policy framework for the continued delivery of government services in the event of a disruption and/or failure of government-operated information and communications technology. The development of this framework was in progress at the time of publication of this guide. The framework will assist Australian Government entities in understanding and developing business continuity and disaster recovery approaches to supporting the delivery of information and communications technology services.

The *Trusted Information Sharing Network Resilience Community of Interest* within the Attorney-General's Department found that resilient organisations understand business impacts, their upstream and downstream dependencies, and establish supportive partnerships with stakeholders in their supply chain, sector and community.

## *Determine the minimum requirements for each critical business process*

It is important to identify the activities and resources supporting critical business processes. These may be the activities and resources of a single operational area in the entity, or may be the activities and resources of a number of operational areas, which combine to produce the output.

A thorough understanding of activities and resources is necessary to identify internal interdependencies. Some activities may rely on the outputs from other activities from within the entity (commonly referred to as enabling outputs), or even from outside the entity. For example, e-business solutions rely not only on the internal network but also on the Internet Service Provider.

To gain the necessary level of understanding of activities and interdependencies, it is important to meet with operational and support area managers to discuss their own understanding of the activities. This may be supplemented by reference to process maps and other systems documentation obtained from procedure manuals or internal audit.

**IMPORTANT UPDATE**

**The Workbook contains a checklist and template for identifying critical business processes.**
**See pp. 105-107**

## Undertake a business impact analysis

A business impact analysis determines and documents the impact of a business disruption event to each critical business process. It considers disruptions to the activities and resources that support the critical business processes.

Before undertaking a business impact analysis, the information required includes:

- endorsed documentation of critical business processes;
- a list of the activities and resources crucial to the critical business processes;
- interdependencies within and between internal activities and resources;
- interdependencies within and between external entities; and
- a priority ranking of the processes, activities and resources which represents the entity's agreed view.

This information must be analysed, and the operational and financial impacts that would result from disruptions to, or loss of, a critical business process assessed.

### *Determine maximum tolerable period of disruption*

The maximum tolerable period of disruption can be determined for the activities and resources. That is, how long can the critical business process survive without the activity and/or resource before it will have a detrimental effect?

**IMPORTANT UPDATE**

## Setting realistic maximum tolerable periods of disruption

***The establishment of maximum tolerable periods of disruption is an important component of designing appropriate continuity treatments. Defining maximum tolerable periods of disruption that are a shorter timeframe than necessary may result in an increase to the cost and complexity of providing continuity treatments than would otherwise be needed.***

***An important part of the business impact analysis process is to challenge maximum tolerable periods of disruption to confirm that these are realistic, and that they represent the longest acceptable time that the entity can continue without this service. For example, it may be unrealistic for support departments such as Marketing or Training to set a very short maximum tolerable period of disruption.***

***Consideration of manual processing alternatives will assist in setting the maximum tolerable periods of disruption to more appropriate levels. An example of this is where the Finance area processes staff payroll at the end of each month. It may be the Finance area's view that the maximum tolerable period of disruption for this process is 48 hours, while during the three days preceding pay day it reduces to six hours. A pragmatic view would be to set the maximum tolerable period of disruption to 48 hours. If there is an interruption during the three busy days, the entity can establish a manual process such as approaching the bank to pay all staff the same amount as last month. Adjustments can then be made retrospectively.***



### *Determine the recovery time objective*

At this stage, entities also determine the recovery time objective. That is, a target time period set for resumption of product or service delivery, recovery of an IT system or application, or resumption of performance of an activity after a business disruption.

If the recovery time objective for an IT system or application is greater than the maximum tolerable period of disruption determined by the business, the entity will need to design a manual processing capability to provide continuity during the time discrepancy. Alternatively, an additional investment of resources may be required to reduce the recovery time objective.

Where critical business processes have been outsourced, or entities rely on activities that have been outsourced, the maximum tolerable period of disruption and recovery time objectives of the outsourced process also need to be assessed. Use of *force majeure*[18] clauses by external parties must also be considered in the context of service restoration and maximum tolerable period of disruption times.

**The Workbook contains a checklist and template for undertaking a business impact analysis. See pp. 108-113**

### *Determine the recovery point objective*

With respect to the recovery of electronic data, it is better practice to determine the recovery point objective. That is, at what point in time prior to the business disruption, should the data be restored to (for example one hour earlier, one day earlier, one week earlier). The recovery point objective subsequently determines the backup strategy for the system or application data. Again, this is considered in terms of the Enterprise Information Architecture. See *Appendix 5: IT Disaster Recovery* for more information.

A documented report of the business impact analysis is a key component of business continuity management, and may be required to satisfy audit requirements.

[18] *Force majeure* is an unexpected and disruptive event that may excuse a party from a contract.

**IMPORTANT UPDATE**

*When anyone asks me how I can best describe my experience in forty years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like. But in all my experience, I have never been in any accident....or of any sort worth speaking about. I have seen but one vessel in distress in all my years at sea. I never saw a wreck nor was I ever in any predicament that threatened to end in disaster of any sort.*

*- Attributed to Captain Edward John Smith of the Titanic.*

## *Disruption scenarios*

When an entity undertakes a risk management process it is important to identify those events, which if they were to occur, might affect the entity achieving its objectives. Often scenario analysis is used as part of risk identification.

These scenarios may be based on previous experiences of the entity or of similar entities. While business continuity management is concerned with taking action after the event (for example it assumes that a business disruption event has occurred and it is not primarily aimed at preventing the disruption), it is still beneficial to the entity to consider some generic scenarios that may occur as these may require specific continuity preparations and responses.

Realistic disruption scenarios may include frequently occurring events such as IT system failure, electrical supply failure, industrial action, transport system failures and bad weather.[19]

Some scenarios which may affect the options chosen to minimise consequences of a business disruption are discussed below.

## *Pandemics*

Many business continuity plans assume that some parts of the entity are unaffected, and can provide the required capacity for the entity to provide critical services. They also assume the business disruption event is short and recovery can begin quickly. These assumptions are not likely to hold in the case of a pandemic – therefore, a different continuity response is required. See *Appendix 4: Pandemics* for more information. Pandemic preparations may be utilised in a non-pandemic business continuity event. For example, an Australian epidemic, a war, or a prolonged strike may all prevent the entity from accessing personnel over a sustained period of time.

## *Managing a business disruption event and a simultaneous increase in demand for services*

Some entities have responsibilities to the community which will increase during the time of a community emergency (for example human services, police and emergency services entities). In cases where an event causes both an entity emergency and a community emergency, an entity may be required to manage both an emergency response (and activate its business continuity plan) and manage a community emergency response. For example, following Cyclone Larry in Queensland in 2006, the Centrelink office in Innisfail suffered damage and was closed to make repairs, and many Queensland Centrelink staff personally suffered damage to their property.[20] In addition to managing the business continuity implications of the cyclone on its own operations, Centrelink managed its emergency community recovery response. Over 500 claims for assistance were received for a range of payments, hotline services were provided via the call centre network, and processing centres were established in Cairns, Brisbane and Maryborough.[21]

**It is important that an entity differentiate its obligation to respond to community emergencies from the need to respond to a business disruption to its own operations.**

At the time of publishing this Guide, the ANAO was conducting two performance audits into Centrelink's business continuity management (Part A) and Centrelink's emergency management and community recovery (Part B).

[19] *Scenarios identified may also be used to conduct business continuity exercises.*

[20] *Cyclone Larry veterans on the ground helping NSW flood victims,* Centrelink, Queensland Media Release, Monday, 25 June 2007.

[21] *Centrelink submission to Comcover's Awards for Excellence in Risk Management 2007.*

**IMPORTANT UPDATE**

## *Supporting Ministers and the Executive*

Some entities have responsibilities under the Australian Government's plan for ensuring the continuity of executive government. This is a whole of government continuity plan, developed by the Department of the Prime Minister and Cabinet, and managed by the Attorney-General's Department. If an entity has particular responsibilities under this plan, it will be advised of these. In addition, these entities have an extra impetus to ensure the continuity of their business operations.

**The Workbook contains a template for identifying disruption scenarios. See p. 114**

Continuity of executive government information must be appropriately classified and securely stored. This means that entities may choose to maintain a separate document, or an appendix detached from the business continuity plan, so that the higher security classification of the information does not prevent access to the business continuity plan by staff members when it is needed.

## *Analysis of operational and financial impacts*

A series of business impact analysis interviews with managers responsible for activities and resources may be the quickest way to analyse the operational and financial impacts of a business disruption.

The analysis should be based on a business disruption event in which all activities and resources (including the work place) are not available. Assuming the worst case outcome (total loss of the process and/or resources), will ensure all impacts arising are considered regardless of the risk likelihood, at least in the first instance.

An approach founded on the likelihood of a risk occurring will fail to propose a treatment for highly unlikely events, despite their consequences.

One of the strengths of risk management is that it is not only about identifying negative impacts, but is also about identifying opportunities. When analysing impacts, entities need to be mindful to also look for opportunities.

**Executive endorsement**

Before proceeding, executive endorsement is needed for the business impact analysis report. This report identifies prioritised critical business processes, interdependencies, activities and resources, and includes:

- maximum tolerable periods of disruption;
- recovery time objectives; and
- recovery point objectives.

*During a disruption, impacts generally increase over time and affect each activity differently. Impacts might also vary depending on the day, month or point in the business lifecycle.*

*- British Standard, Business Continuity Management – Part 1: Code of practice, BS25999-1:2006, 2006, British Standards Institution, p. 17.*

**IMPORTANT UPDATE**

## Implementing a business continuity management program – Checkpoint 3

| Checkpoint 3 | Generic characteristics of better practice business continuity management in public sector entities | Completed | Level of implementation |
|---|---|---|---|
| | Characteristic 3: A risk assessment has been conducted. | Yes / No | Basic / Mature |
| | Characteristic 4: A business impact analysis has been conducted. | Yes / No | Basic / Mature |

Table 1 on page 9 of this better practice guide provides details on the implementation characteristics.

**Further references**

- e-government **http://finance.gov.au/e-government**
- Trusted Information Sharing Network Resilience Community of Interest **http://www.tisn.gov.au**

IMPORTANT UPDATE

# Designing the entity's business continuity approach

Identifying and evaluating options to minimise the effects of a business disruption

> Value creation and development

Limitations

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Designing the entity's business continuity approach

This section provides guidance on how to design the entity's business continuity approach to minimise the effects of disruptions to each critical business process for which a maximum tolerable period of disruption and recovery time objective has been established.

*We can't solve problems by using the same kind of thinking we used when we created them.*

*- Albert Einstein.*

Minimising the effects of disruptions to critical business processes involves:

- identifying and evaluating options to minimise the effects of a business disruption; and
- selecting alternative activities and resources.

## Identifying and evaluating options to minimise the effects of a business disruption

For each of the critical business processes identified and ranked in the business impact analysis, options are needed to:

- reduce the likelihood and consequence of the disruption to the activities and resources on which the critical processes rely; and
- implement alternative activities and resources to be used following a business disruption and activate plans to recover and restore normal operations.

Evaluating options available to ensure the continuation of business will identify alternative activities and resources to be used if a business disruption event occurs. Alternative activities and resources may be a combination of different services or redundancy retained 'just in case' (for example a hot, warm or cold site).[22]

Variations to, or redesign of, existing activities and resources should be considered as a means of reducing the exposure to, or consequence of, the disruption of a critical business process.

In selecting alternative activities and/or resources, it is important the following activities and/or resources are addressed as part of the business continuity planning process:

- people;
- facilities (including buildings and equipment);
- technology (including IT systems/applications);
- telecommunications; and
- vital records.

[22] Alternative sites provide a data centre and work area held in readiness for use during a business continuity event. A 'hot' site is fully equipped and provides immediate access (for example the data centre is permanently connected to the entity's primary or back-up systems, there are operational workspaces, printers, telephones etc), a 'warm' site is partially equipped (for example, the data centre is capable of accessing the entity's system, but the data processing and work area needs to be configured), and a 'cold' site is a basic work area with data centre access that needs to be configured to resume operations (for example it has electrical and telephony connections, but no equipment – such as a hotel's conference facilities).

**IMPORTANT UPDATE**

## *People*

People, including contract personnel, are the vital resource in ensuring continuity of business. An unexpected loss of key/experienced personnel, or a team, can have significant consequences for an entity's capacity to achieve its objectives.

The business continuity approach needs to include treatments for people, which incorporates:

- communication strategies – communication channels and messages for different groups such as continuity team members, entity staff, external stakeholders, and the general public;
- human resource issues, including;
  - short-term replacements and training;
  - sustained reduced staff capacity disruptions (for example, due to a pandemic occurring); and
  - employee payroll;
- issues relating to the specific business disruption; and
- the psychological effects of the disruption on staff morale – this may include trauma counselling for staff both during and after the event.

**Case Study – Human resource issues**

The State Library of Victoria is a public sector entity which aims to ensure that the documentary resources of significance relating to Victoria and Victorians are collected, preserved and made available and that Victorians have access to worldwide information resources. In the course of its business continuity planning, it identified an inherent risk in ensuring sufficient access to a skilled team of specialists to assist in the conservation and preservation of its unique cultural heritage material in the event of a disaster, or major incident that affected the integrity of the Library's collections. As a result of undertaking a business impact analysis and developing a business continuity plan, the library has effected increased cross agency collaboration. A memorandum of understanding has been entered with allied organisations that will enable the shared use of expertise and resources in the event of major emergencies affecting the State's unique cultural heritage. By using expertise in allied organisations the number of experts available in the event of a major emergency was increased five-fold without any additional cost. Issues regarding cross party indemnification have also been resolved, and work practices to give effect to this plan have been established.

Source: State Library of Victoria.

**IMPORTANT UPDATE**

**Table 2 - Example treatment options for people (including contract personnel)**

| Treatment | Description |
|---|---|
| Succession plans | A prescribed plan of action to replace key staff if they are unavailable. This may include identifying understudies in the entity, or agreements with professional contracting agencies or with other entities to source qualified staff at short notice. |
| Skills management plans | For identified understudies, make key information and the entity's knowledge is available so they can assume a new role with as little lead-time for learning as possible. |
| Key person insurance | Insure against the financial consequences of loss of key staff. This approach may recover the costs associated with loss of key staff but it is only a solution to a symptom of losing staff - proactive staff management practices are always preferable. |

## *Facilities (including buildings and equipment)*

It will assist entities to pre-prepare processes and treatments for assessing damage, salvage and restoration of equipment and buildings. These address the buildings in which the business processes operate and the equipment and resources contained within those premises. The treatments also aim to ensure timely restoration or relocation so critical business processes can be moved back to the restored premises or be relocated to new premises and continue essential business processes. Where relocated accommodation is to be provided by a third party, the treatment plan needs to include a regular communication schedule with the provider, to ensure the facilities are still available, and meet the requirements of the entity.

Some issues to consider include:

- arrangements and procedures for relocating facilities;
- provision for backup processing services;
- agreements and activities required to transfer functions;
- administrative details such as spare IT equipment, cheque printing, stationery, paper manuals, access to key procedures and contacts, and storage of spare keys to access offsite material; and
- documented procedures to support business facility recovery and restoration.

Following a major disruption, facility recovery treatments aid the entity in supplementary staffing, movement or relocation of staff, procedural and administrative changes, and site and infrastructure modifications.

**IMPORTANT UPDATE**

**Case Study – Facilities issues**

It is important to understand that there is no 'one size fits all' treatment for business continuity risks. Entities need to consider their unique circumstances and operating context when developing and implementing treatments. Some examples of the approaches different entities have taken to ensure continuity of facilities include:

- the Reserve Bank of Australia has identified its processes as being of extremely high criticality, and following a cost-benefit analysis of its options, has implemented a purpose-built 'hot site';
- the Treasury has implemented a memorandum of understanding (MOU) with one of its portfolio agencies that is located several kilometres away. This MOU allows the Treasury to use that agency's facilities in the event of a business disruption; and
- for entities that have multiple sites, such as the Australian Securities and Investments Commission and the Department of Health and Ageing, a site pairing system has been implemented. This allows pairs of regional offices (for example Darwin and Alice Springs, Perth and Adelaide) to work together in developing their continuity plans, and to act as alternative sites if one of the regional offices be affected by an incident that affects its ability to conduct business as usual, and it's business continuity plan is invoked.

Source: ANAO analysis.

## *Remote access*

Remote access services have evolved beyond an after-hours business tool to become an integral part of day-to-day business operations. Similarly, mobile devices used to access corporate data and information have also evolved. Entities are increasingly benefiting from the extensive use of devices such as laptops, high data-rate mobile phones and personal digital assistants to enhance the remote access capability of their staff.

In the context of business continuity management, remote access provides the ability to use information and communications technology systems to sustain critical business processes or functions from a remote location, for an extended period of time. An example of an extended period of time is a prolonged situation such as a human influenza pandemic. A remote location is a place other than the principle place of employment for the employee. This may include:

- alternative offices or a disaster recovery site in accordance with business continuity arrangements;
- field staff operating via mobile communication devices;
- an employee's home environment; or
- conference facilities.

Variables that may affect the resilience of remote access strategies and the underpinning telecommunications network in a prolonged emergency may include:

- network congestion caused by increased use of telecommunications and internet services during a prolonged emergency; or
- possible failure of infrastructure due to a lack of maintenance or damage.

Further references on remote access are provided at the end of this chapter.

**IMPORTANT UPDATE**

### *Technology (IT systems/applications)*

Information systems manage the entities physical records (for example correspondence, project and management files) and electronic records on computing facilities (for example email, electronic policy and procedure manuals, forms and images). Treatments that deal with the continuity of technology can include:

- preventative controls such as robust systems and application design, fault-tolerant hardware, uninterruptible power supplies, and monitoring facilities;
- use of secure and fire-proof in-house storage facilities;
- agreements and activities required to transfer processing to other locations;
- provision for backup processing facilities (electronic and manual);
- off-site storage of data;
- the ability of vendors to supply equipment if the entity does not hold spares, or the equipment is rendered unavailable due to the crisis/incident; and
- continuity of protection of classified information.

**Table 3 - Example treatment options for facilities, telecommunications and systems**

| Treatment | Description |
|---|---|
| Purchase or lease | Pay for extra office space, IT infrastructure, redundant capacity communications. |
| Contingency arrangements | Enter an agreement with an outside vendor to provide service in the event of a business disruption (for example hot site, warm site, and cold site). |
| Mutually beneficial agreements | Enter into an agreement with another entity to use part of their facilities in the event of a disaster. These types of agreements can be entered into with other entities to achieve the other options (for example purchasing a hot-site agreement together). |

## Telecommunications

Telecommunication is essential for the continuity of business functions. Better practice continuity approaches include treatments that address recovery from loss or disruption of voice and data communications, both within and outside the entity. In many entities, voice networks are more important than data networks.

Treatments that deal with communication continuity can include:

- human resource procedures and administration required to support the business function;
- vendor and carrier negotiations in which contractual or service level agreements are made with telecommunication vendors;
- alternate path design and switching services redundancy being built into communications networks which enable communications to be diverted to other locations if, and when, necessary;

**IMPORTANT UPDATE**

- backup equipment and software which includes backing up Private Automatic Branch Exchange data, network software and acquiring necessary redundant equipment;
- default Public Switched Telephone Network failover for entities that use Voice over Internet Protocol; and
- uninterruptible power supplies and monitoring facilities which help prevent system loss during power failures.

### *Vital records*

As part of the business impact analysis, vital records supporting the critical business processes are identified. Restoring vital records requires that a suitable records management program is in place. This includes the management of hardcopy and electronic records data and archiving policies for both forms of records.

Record management procedures are part of the entity's overall information management strategy. Continuity issues in record management extend beyond just keeping business processes in place. Record management has long-term implications for the entity and continuity strategy considerations include:

- legal requirements and exposures;
- adverse affects on reputation through inability to deliver information;
- inefficiency across all processes in locating and utilising information;
- political ramifications of non-delivery of a service or information;
- stakeholder dissatisfaction;
- decision-making processes which will be affected; and
- records destroyed outside of a valid Records Disposal Authority by the business disruption event.

## *Interdependencies*

### *Internal interdependencies*

As a business disruption may affect more than one business process, the treatments developed for each critical process need to be consolidated and, ultimately, individual business process plans combined into an entity-wide plan.

While this is the final step in determining treatment options, the concept of coordination drive the entire approach. This is crucial to effective business continuity management as it recognises the interdependencies between business processes within the entity.

Business process approaches address the activities and responsibilities of a business function. The aim is to continue critical business processes from the point of the business disruption event to the point when operations are returned to normal.

**IMPORTANT UPDATE**

**Table 4 - Example treatment options for business processes**

| Treatment | Description |
|---|---|
| Alter current arrangements | Current processes and resources can be changed as a cost-effective solution. For example, splitting data processing between two offices, so that in the event of a loss of one site, the other site is still functioning. Remote access can provide an effective temporary solution. |
| Alter current processes | Current (or even non-current) service providers may be willing to give a guaranteed level of service in a disaster situation to enable restoration of resources at a reasonable cost. |

## *External interdependencies*

Where reliance is placed on outsourced providers, contracts with parties that provide outsourced services must be robust and contain clauses that define required service levels (including the required maximum tolerable period of disruption, recovery time objective and recovery point objective) that the service should be recovered to in the event of a disruption. Entities need to obtain comfort that the outsourced provider is able to meet these requirements. As outsource providers may service several clients, entities need to be aware of the priority given to them by the provider, and the triage processes the service provider uses when restoring services. This may include the right to audit the business continuity arrangements of the third party within any contractual agreement. As noted earlier, the use of *force majeure* clauses by external parties needs to be considered when an outsourced provider is used.

## *Selecting alternative activities and resources*

A cost-effective strategy for recovery, satisfying the requirements of the business, should be selected from the options identified. To enable this choice to be made, it is necessary that each option be costed.

Costs include:

- direct costs - such as purchase price for extra equipment; and
- indirect costs -such as cost to establish and maintain new equipment.

All costs need to be carefully considered as indirect costs such as maintenance can often exceed direct purchase costs.

In many cases it is possible to defer all of the costs, or a significant portion, until an event occurs and the continuity plan is activated. For example, the majority of costs associated with moving business operations to a warm or cold alternative site would occur only when a relocation is performed.

**Executive endorsement**

The selected alternative activities and resources should be documented along with the rationale for their selection. The executive should endorse the continuity approach (or at least the underlying principles) prior to the implementation of preparatory controls.

**The Workbook contains checklists for selecting activities and resource alternatives, alternative processing service contract considerations, backup processing and offsite storage, IT disaster recovery, and a template for evaluating recovery treatment options. See p. 116-119**

**IMPORTANT UPDATE**

## Value creation and development

Disruptive events may produce opportunities which can be identified and seized. The event may provide an opportunity to change a process, or take advantage of the event's effects. Looking for opportunities to create and develop value through business continuity management is vital to becoming a resilient entity.

## Limitations

Better practice business continuity management programs recognise the factors that may limit recovery from a business disruption event. These factors are documented and brought to attention of management.

**The Workbook contains an example of factors which may limit an entity's continuity approach. See pp. 120-121**

## Implementing a business continuity management program – Checkpoint

The checkpoint for this chapter is combined with the following chapter *Building Entity Resilience,* and is provided at the end of that chapter.

**Further references**

**Remote access**

- *Remote Access: A Tool to Support Business Continuity,* 2008, Attorney-General's Department, Trusted Information Sharing Network.

**Records management**

- *Archives Act 1983* and other legislation such as the *Freedom of Information Act 1982,* the *Privacy Act 1988,* the *National Security Information Act 2004,* the *Electronic Transactions Act 1999,* the *Evidence Act 1995,* the *Crimes Act 1914,* the *Public Service Act 1999,* the *Financial Management* and *Accountability Act 1997 and the Commonwealth Authorities and Companies Act 1997.*
- *Australian Government ICT Security Manual (ISM),* ACSI 33, 2008, Department of Defence, Defence Signals Directorate.
- Australian Public Service Commission's publications, including the *Foundations of Governance.*
- Australian Government Information Management Office's requirements for such matters as online services and protective markings on emails, as well as its suite of better practice checklists on information, communication and technology related subjects.
- *Information and documentation - Records management - Part 1: General,* ISO 15489 -1:2001 and *Information and documentation - Records management - Part 2: Guidelines,* ISO/TR 15489-2:2001 (also known as AS ISO 15489).
- Management Advisory Committee Report, *Note for file: A report on recordkeeping in the APS.*
- National Archives of Australia e-permanence suite of products and guidance materials.
- The Department of the Prime Minister and *Cabinet's Cabinet Handbook and Federal Executive Council Handbook.*
- The Protective Security Coordination Centre's *Commonwealth Protective Security Manual* (PSM), Protective Security Policy Committee of the Attorney-General's Department.
- The Senate's Procedural Order No. 8 *Indexed Lists of Departmental and Agency Files.*

**IMPORTANT UPDATE**

# Building entity resilience

Implementing preparatory controls

Preparing the business continuity plan(s)

# IMPORTANT UPDATE

**IMPORTANT UPDATE**

# Building entity resilience

This section provides guidance for entities on how to implement preparatory and reactive procedures to minimise business disruptions and support recovery. This involves:

- implementing preparatory controls; and
- preparing the business continuity plan(s).

## Implementing preparatory controls

Preparing for recovery involves putting in place controls that will mitigate the consequences of a business disruption to a level acceptable to the entity if it occurs. Preparatory controls may also be put in place to prepare the entity to take advantage of a business disruption event.

**The Workbook contains a checklist for ensuring strategies are implemented. See p. 122**

Some important preparatory controls include back-up processes, records management (see *Undertake a Business Impact Analysis* for discussion on vital records), formal contingency arrangements with external parties, and pre-establishing a specialised team to be used during a business disruption event.

### *Back-up processes*

Activating a business continuity plan requires access to information and resources supporting critical business processes. In the event of a business disruption it may still be possible to obtain these from the entity's premises, but this will not always be the case.

Reliable off-site storage and backup procedures will ensure information essential to continue critical business processes is available as, and when, needed.

Resources required for recovery such as documentation, forms, supplies, data and programs should be obtained and kept at a secure off-site facility. Copies of the business continuity plan and relevant documents can also be provided on secure portable storage (for example a secure USB key) which is able to be kept with individuals.

It is important that off-site storage facilities have suitable environmental and security controls and the resources and information are protected from unauthorised access, modification, disruption or use during storage.

Off-site storage procedures may be modified to align routine operational requirements with those identified in recovery strategies so that resources stored off-site, are available for routine and recovery situations.

### *Arrangements with external parties*

It is necessary to formalise appropriate arrangements with vendor(s) selected as alternative suppliers. Entities need to:

- ensure for each treatment selected, the likely costs are the most commercially viable;

**IMPORTANT UPDATE**

- identify other requirements or changes to be made in order for the treatments to be effective;
- change off-site storage procedures as identified;
- review contracts to ensure they demonstrate better practice for contract management as well as comply with the Commonwealth Procurement Guidelines; and
- finalise contracts.

## *Establishing business continuity (recovery) teams for a business disruption*

Following a disruptive event, a specialised entity structure, which varies from the entity's structure during periods of normal operations, is established. This structure is invoked upon declaration of a business disruption event that is expected to exceed the maximum tolerable period of disruption.

Depending on the size, complexity, and criticality of the entity, this structure may include one or more of the following:

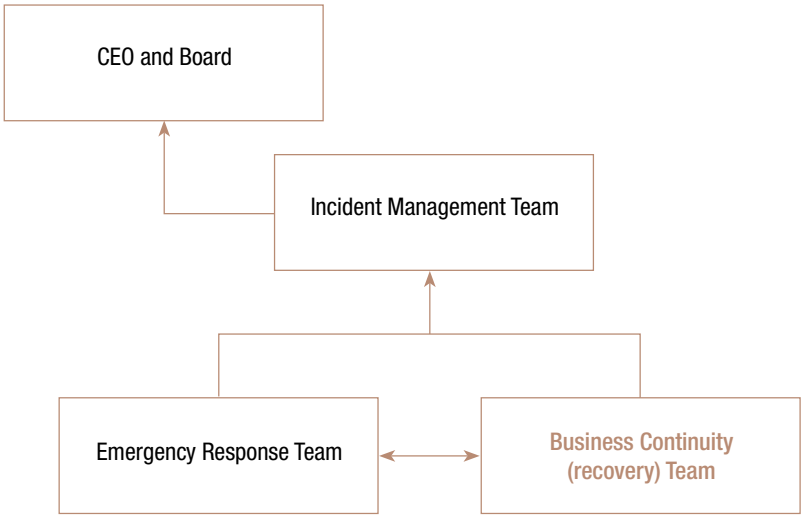
- emergency response management team;
- incident management team; and
- business continuity (recovery) team.

**The Workbook contains examples of pre-prepared media communications.**
**See p. 126**

A key consideration in the development of the specialised structure is the role of the entity's executive during a business disruption. It is often the case that the executive wishes to take the ministerial and media communication/liaison role.

An example of the relationship between the teams during a business disruption event is provided in Figure 6.

**Figure 6 - Example of the relationship between teams during a business disruption**



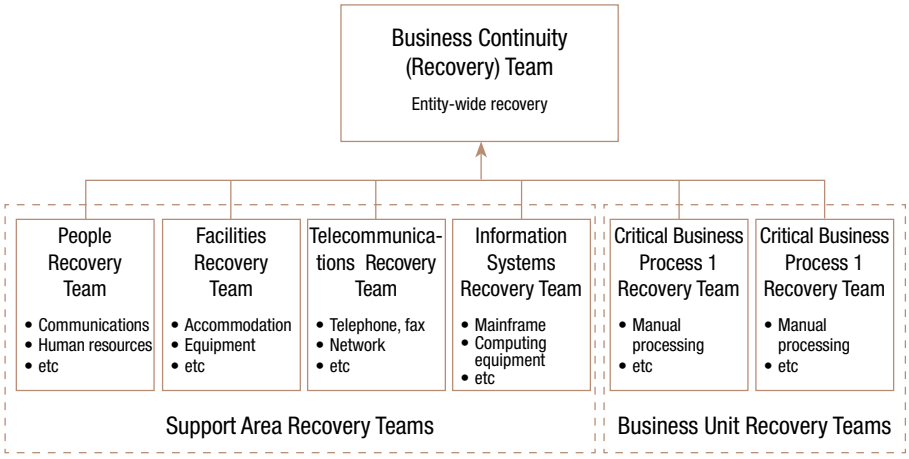

Note The focus of this guide is business continuity management.

For a smaller, non-complex, or non time-critical entity, the emergency response and incident management teams may be combined into one team. In entities that are large, complex, or geographically dispersed, the use of separate emergency response, incident management and business continuity management teams increases the need for clear roles and responsibilities, and effective communication.

**IMPORTANT UPDATE**

In a large entity, each team might constitute a number of sub-teams, which focus on a specific area. In a small entity, there might be a single person performing the role for each area. The business continuity sub-teams may be geographically or individual building site based, or include a team for each of the areas addressed when designing the entity's continuity approach. An example of business continuity (recovery) teams during a business disruption event is provided in Figure 7.

**Figure 7 - Example of teams during a business disruption**




Note For a smaller non-complex, or non time-critical entity, all of the recovery roles may be combined into one team, with a single person responsible for each role. The use of business continuity sub-teams increases the need for clear roles and responsibilities, and effective communication.

For each team and subteam, a team leader is identified as being responsible for that area. Alternative people to fill each role should also be identified.

Entities use a variety of terms to name the business continuity teams and roles, including 'Recovery Team' or 'Business Continuity Team' and 'Recovery Coordinator' or 'Business Continuity Coordinator' or 'Business Continuity Manager'. Regardless of the terminology, it is important to ensure reporting lines and responsibilities are clear when the specialised structure is activated. The entity should clearly understand and document the roles and responsibilities of the different teams and team members.

**IMPORTANT UPDATE**

## Kits

***Better practice entities prepare kits in advance of a business disruption. This enables information and resources to be readily available during a business disruption event. Kits should be securely stored if they contain sensitive information, however they need to be readily available. Entities may consider preparing multiple kits for different teams (for example, incident management team, entity-wide business continuity management team, business area or service unit teams), and storing some kits at an off-site location. A kit may include:***

- ***Storage box – consider using a waterproof or fireproof box.***
- ***Emergency response management plan.***
- ***Incident management plan.***
- ***Business continuity plan(s).***
- ***Event log templates.***
- ***Mobile phone, battery charger.***
- ***Power extension cords.***
- ***Floor plans.***
- ***Torches.***
- ***Stationery.***
- ***Taxi vouchers.***
- ***Cheque book.***
- ***Long life food, water.***
- ***Contact lists – continuity teams, all staff, stakeholders, external interdependent entities, insurance.***
- ***Secure USB or external hard drive that is pre-loaded with information.***
- ***Disposable camera – for recording evidence/insurance claims.***

***Kits need to be periodically reviewed and updated.***

***Source: Adapted from A Practitioners Guide to Business Continuity Management Handbook 292:2006***

## *Continuity team members*

Personnel need to be identified for the business continuity (recovery) teams. The make-up of the team may be based on consideration of an individual's personal characteristics as much of their position within the entity. Leaders and members of a recovery team need the following personal attributes:

- effective people and communication skills;
- the ability to work well under stress and balance competing priorities;
- a good understanding of the entity;
- an ability to work well in teams; and
- respect within the entity.

Team members must understand, and be capable of carrying out, what is required of them in a business continuity situation and must be aware of the possible disruptive consequences of their actions or inaction. This requires explicit communication and coordination through job descriptions, awareness programs, special training and testing and exercising of plans.

**The Workbook contains an example of aresponsibilities for various business continuity roles. See pp. 95-98**

**IMPORTANT UPDATE**

### *Entity staff*

People are the major focus of a business disruption. Equipment, infrastructure and facilities may all be operational but if people cannot reach their work place, or perform their jobs, critical business processes will cease or be disrupted.

Human resource management can be a challenge to successfully activating the contingency plan. For example, if the business continuity plan calls for staff to move to another location, some staff such as primary carers, part-time students, and members of volunteer services, may not be available.

## Preparing the business continuity plan(s)

Documentation of the recovery arrangements to be implemented after a business disruption has occurred is the role of the business continuity plan.

*We don't have a plan, so nothing can go wrong.*

*- Spike Milligan.*

There is no 'one-size-fits-all' approach to developing a business continuity plan. The size and structure of business continuity plans will ultimately be determined by the entity's environment and requirements.

Better practice business continuity plans produced consist of action-oriented procedures, based on the approved recovery treatments and alternative activities and resources identified.

If the structure that is created for operating during a business disruption event consists of multiple teams or includes sub-teams, it is important that each team has its own plan with action-oriented procedures and contact lists. If there are multiple plans, it is also necessary to have an overarching entity-wide plan to coordinate the sub-plans. Thus the suite of planning documentation may include an emergency response management plan, an incident management plan, an entity-wide business continuity plan, and several business continuity sub-plans.

As the focus of this guide is business continuity management, the development of the entity-wide business continuity plan and the business continuity sub-plans is discussed. However the principles involved in preparing these plans are applicable to the other plans.

No matter how well designed an entity's business continuity plan may seem, it is essential to train staff and conduct testing and exercises. Training is discussed on page 19 and testing and exercising is discussed on page 61 of this better practice guide.



**The workbook contains an example table of contents for a business continuity plan, and a pandemic plan.**
**See pp. 123-124**

### *The entity-wide business continuity plan*

The entity-wide business continuity plan combines individual support area and business unit recovery plans into one coordinated plan. The recovery steps common to support areas and business units are combined into this plan (for example to inform staff of the business disruption event). The entity-wide business continuity plan also addresses the issues to which the entity, as a whole, must respond following the declaration of a business continuity event.

### *Activation*

As well as combining the individual support area and business unit plans, the entity-wide business continuity plan contains the criteria for activating the plan. Declaration of a business continuity event is a decision for the incident or business continuity manager, or other designated staff, based on entity-specific information. Table 5 provides an example of a written activation procedure.

**IMPORTANT UPDATE**

**Table 5 - Example of a written activation procedure**

| Declaration of a business continuity event |
|---|
| The process for declaration of a business continuity event falls within the following parameters:<br>• Where the business disruption is limited in nature and can be managed at a local or regional level without the use of Corporate powers, such as sending staff home or committing significant sums of money, the Regional Business Continuity Manager (or Deputy) can activate the Business Continuity Management Team.<br>• Where the business disruption is limited to a location or region and may reasonably lead to the use of Corporate powers a business continuity event will be declared, and the Business Continuity Management Team activated, by the agreement of any two of:<br>o The Regional Business Continuity Manager (or their Deputy);<br>o The National Business Continuity Manager;<br>o The Director of Property Services; and<br>o The Chief Finance Officer (or their deputy).<br>• Where the business disruption has, or may reasonably have, an effect on the organisation nationally the business continuity event will be declared, and the Business Continuity Management Team activated by:<br>o The agreement of the Chief Finance Officer, (or their deputy) with either the National Business Continuity Manager or the Director of Property Services; and<br>o The Commissioner or a Second Commissioner.<br>• Where the business disruption relates to an IT disaster recovery process the IT Disaster Recovery Manager can declare a business continuity event and activate the IT Disaster Recovery team.<br>At the point of declaration of a crisis the management of the affected area is transferred to the leader of the Business Continuity Management Team. |

Some entities have found it useful to include an activation diagram at the start of their business continuity plan. An example of an activation diagram is provided in the section *In the event of a disruption: Activating and deploying the plan.*

**The Workbook contains example activation diagrams. See pp. 129-130**

A key step in the activation process is to estimate how long it is before the business function can be restored. That is, 'is recovery time greater than the maximum tolerable period of disruption?' Guidelines to estimate the duration of a business disruption event need to be established.

**IMPORTANT UPDATE**

## What constitutes a business disruption event?

***As noted at the start of this guide, a business disruption is not just an event that reduces the effectiveness of systems, but an event that is extraordinary, causes a loss of critical business processes and impairs the entity's capacity to achieve it's objectives. It is an event or situation that exceeds the maximum tolerable period of disruption. A business disruption event is an event where normal management is suspended.***

***A disruptive event may be an acute, creeping, or sustained event. A fire is an example of an acute disruptive event, a series of minor IT system failures culminating in the failure of a large or primary system is an example of a creeping disruptive event, and a pandemic is an example of a sustained disruptive event.***

***A complete loss of all business processes, activities and resources may be referred to as a disaster.***

***An example of what is NOT a business disruption event would be the case of legal action in progress or a resultant decision. While there may be a resource, financial and public image effect (which may be regarded as a crisis or incident to management), it is a management issue not a continuity issue due to the fact that critical business processes are not affected.***

### *Event log*

Including an event log template in the recovery plan facilitates recording the events for later debriefing and review. An event log allows the recovery coordinator, secretariat or other staff to record details of the event. This can be used to brief other recovery teams, executive management and the media so there is a consistent description of the event.

**The Workbook contains event log templates. See p. 135**

### *Support area and business unit recovery plans*

A recovery plan should be developed for each support area and business unit identified in the recovery strategy. This plan considers the people in the recovery teams and assigns individual responsibility for each action (between team leaders, team members and other teams) as well as timing and expected outcomes for each action.

The steps required for recovery of a business process are documented in order of precedence. This order reflects any interdependencies between steps. The recovery steps also need to consider issues reflecting interaction with other support areas, business units, and recovery teams. In establishing the recovery steps for each support area and business unit it is important that communications, including information flows, are fully effective.

**The Workbook contains a template for business unit and support area recovery steps. See p. 134**

Following completion, it often becomes apparent that many of the recovery plans have some recovery steps in common. These steps can be integrated and assigned to one recovery team (usually that team which needs to complete that recovery step first). The other recovery teams can still include the recovery steps in their plans, noting that the responsibility for completing the step has been assigned to another recovery team.

**IMPORTANT UPDATE**

## *Format and contents of business continuity plans*

**A better practice business continuity plan is a short and succinct document.** A business continuity plan does not need to contain contextual information (such as background, executive summaries) as this was part of the development and approval process and should be stored on official files. Some entities have chosen to prepare a separate business continuity framework document to contain this information. The plan simply starts at the point at which the plan has been invoked and guides the reader through each step in the response and recovery process.

### *Principles for writing a business continuity plan*

- ***Accessibility – plans should be readily accessible, stored in electronic and hardcopy formats, and stored at a number of locations.***
- ***Brevity – avoid lengthy documents.***
- ***Clarity of language - use plain English, avoid jargon and acronyms.***
- ***Complementary – related plans should integrate with, and cross reference each other.***
- ***Flexibility – avoid focusing on scenarios, as this may limit usability if a different situation occurs.***
- ***Security classification – balance the need for staff to access the document in a continuity situation, with the need to safeguard personal and other confidential information.***
- ***Simplicity – use diagrams, flow charts, checklists, which are easy to understand and follow.***
- ***State the obvious – in a continuity situation, staff may be acting out of role, or may have impaired judgement.***

***Source: Adapted from A Practitioners Guide to Business Continuity Management Handbook 292:2006***

The format and content of the business continuity plan is extremely important. In a disaster situation, the reader can pick up the document having not read it (although it is preferable that they have), and be presented with action-oriented points they can follow. References and contacts may be included as an attachment, or in-line with the action steps.

Entities use a variety of methods to make the business continuity plan more usable. For example, some use tabs to divide sections, or colour code plans and/or sections, so that staff performing a particular role can easily navigate to the information that is relevant to them.

## *Contact lists*

Throughout the recovery process it will be necessary to contact a range of people and entities. Comprehensive contact lists should be established and maintained. Contact lists to be established may include:

- emergency services contact lists;
- emergency response team, incident management team, and business continuity (recovery) team contact lists;
- stakeholder contact lists;
- interdependent external entities and organisations; and
- staff lists with after hours contact details (if too large, details of where to locate a copy).

## IMPORTANT UPDATE

It is essential these lists be kept up to date. Normal operating procedures need to assign responsibility for maintaining lists including updating the recovery versions.

**The Workbook contains an example of a wallet book contact list. See p. 125**

Some entities maintain their internal and external contact lists as a separate appendix or attachment in the business continuity plan. This allows for easy updating of just the contacts section on a periodic (say, monthly) basis, rather than waiting for the **annual review** of the plan.

If entities wish to incorporate personal contacts such as home telephone numbers, personal mobile phone numbers and personal email addresses, it is important to comply with privacy obligations by obtaining the consent of the person before using personal information, and to securely store this information.

A number of entities also produce a wallet card containing contact information of key business continuity personnel. This business card size card may also contain high-level continuity information such as the activation process.

**Case Study: Contacting business continuity and other staff in the event of a business disruption**

Entities should consider the method they use to contact staff in the event of a business disruption event.

Many entities such as the Australian Taxation Office and the Department of Education, Employment and Workplace Relations have an entity-wide 1800 (free call) number, which all staff members can call to listen to a recorded announcement. This number is often printed on the staff member's facilities access card, or on the accompanying emergency procedures card which is carried with it. The entity may also have a public and/or secure-access link on their internet site where staff can access information.

Traditionally, entities have used a 'telephone tree' approach for contacting business continuity staff. In this approach each person is responsible for calling the next on the list. It is often accompanied by the use of 'wallet cards'.

More recently, entities have started adopting automated methods for contacting staff.

The National Library of Australia (NLA) has an arrangement with a service provider for 'broadcast SMS'. This allows the NLA to email a message to the service provider and have the service provider send an SMS (text message) to staff members' mobile phones. The NLA uses this to notify specific staff of incidents and their progress and call the emergency planning committee to meet. The system can also be tailored to different groups of staff. This is a low-cost solution that enables the NLA to quickly and efficiently broadcast tailored information to staff.

Another option is the use of an integrated business continuity database system. Some entities have developed their own in-house database, and there are also several commercially available products which some larger entities are using. These systems are capable of sending out the 'broadcast sms' as described above. In addition, they manage the suite of business continuity information, such as business impact analysis, plans, contact lists, testing and exercising schedules and results. By drawing on a database of information, they are able to populate and create documents such as plans, and they also have extensive reporting capabilities. This is a more costly solution, and each entity would need to asses these costs against the additional benefits received in the context of their entity.

Source: ANAO analysis.

**IMPORTANT UPDATE**

**Executive endorsement**

Upon completion, the business continuity plan must be reviewed and approved. A list for review and approval might include:

- Internal audit.
- Audit committee.
- Business continuity steering committee.
- Chief Executive Officer.
- Senior executives.

## *Quality assurance*

Reviews of the business continuity plan during its preparation and throughout its life are recommended to ensure its content remains relevant. It is recommended the business continuity custodian and management committee responsible for the business continuity plan ensure this is undertaken, in conjunction with routine testing.

## Implementing a business continuity management program - Checkpoint 4

| Checkpoint 4 | Generic characteristics of better practice business continuity management in public sector entities | Completed | Level of implementation |
|---|---|---|---|
| | Characteristic 5: Preparatory controls have been implemented. | Yes / No | Basic / Mature |
| | Characteristic 6: The entity has documented and the executive has endorsed its business continuity plans and framework. | Yes / No | Basic / Mature |

Table 1 on page 9 of this better practice guide provides detail on the implementation characteristics.

**Further references**

- *Commonwealth Procurement Guidelines,* Financial Management Guidance No. 1, Department of Finance and Deregulation, December 2008.
- *Developing and Managing Contracts Better Practice Guide,* 2007, Australian National Audit Office.
- *Developing and Managing Contracts Templates and Checklists,* 2007, Australian National Audit Office.
- *Fairness and Transparency in Purchasing Decisions. Probity in Australian Government Procurement Better Practice Guide,* 2007, Australian National Audit Office.

**IMPORTANT UPDATE**

# In the event of a disruption: Activating and deploying the plan

Declaring a business disruption event

Phases of a business disruption

Some examples of business continuity events

Returning to normal operations

Post incident review

Continuity event reporting

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# In the event of a disruption: Activating and deploying the plan

*You don't know what you've got 'til it's gone.*

*- Joni Mitchell.*

This section provides guidance for entities on the activation of a business continuity plan.

Some examples of recent incidents which have affected Australian Government entities, and have required the activation of business continuity plans, or have been used to exercise business continuity plans, include the:

- *concurrent firestorm in Victoria and floods in Queensland and New South Wales* (2009) – State and Federal emergency services and community recovery entities were stretched to the limit when disasters were concurrently declared in two states in February 2009. Hundreds of lives were lost, and there was extensive damage to homes, businesses, infrastructure and government property;
- *APEC and World Youth Day events in Sydney* (2007 and 2008) - these were planned events, however they disrupted business operations due to increased security requirements necessitating road closures in the central business district and eastern Sydney areas;
- *major storm in the Hunter Valley, Central Coast and Sydney* (2007) – this storm killed nine people, caused extensive damage to the Newcastle, Wyong and Gosford areas, and in the following days caused major floods in the Hunter region. Electricity supplies were also extensively reduced;
- *power supply failures in Victoria (2000 and 2007)* – a key power transmission line was cut by a bushfire; and industrial action, generator failure and high temperatures combined to trigger blackouts and restrictions. In both incidents, homes and businesses lost power for significant periods of time;
- *severe hailstorm in the ACT (February 2007)* – a SuperCell storm dumped nearly one metre of ice in Canberra. The ice was so heavy the roof collapsed in several buildings, including a newly built shopping centre, a university and a library;
- *Tropical Cyclone Larry in Queensland (March 2006)* – with wind gusts reaching 240 km/h, Cyclone Larry damaged buildings, caused major disruptions to power, water and telephone services, and resulted in one fatality. The cost of the cyclone was estimated at A$1 billion;
- *Boxing Day tsunami in the south pacific (December 2004)* – an earthquake triggered a series of tsunamis, killing more than 225 000 people in 11 countries, and inundating coastal communities with waves up to 30 meters high;
- *firestorm in NSW and the ACT (January 2003)* - after burning for a week around the edges of the ACT, fires entered the suburbs of Canberra. Four people died, more than 500 homes were destroyed or severely damaged and organisations such as the Canberra Hospital ran on back-up generators; and
- *terrorist activities worldwide* – while major terrorist activities such as the September 11 attack in 2001, the 2004 Madrid bombings, the Bali bombings in 2002 and 2005, and the 2005 London bombings account only for a small percentage of business disruptions, these are highly visible and traumatic events that impact communities and entities.

**IMPORTANT UPDATE**

## Declaring a business disruption event

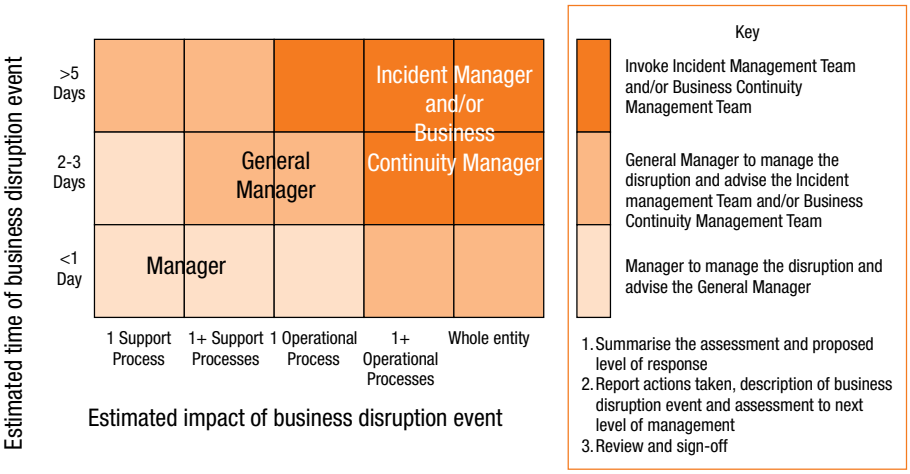
**The Workbook contains an example of activation levels, a checklist for considering issues when estimating the duration of a business disruption event, activation flow charts, a guide to sequence of response actions a template for an immediate response meeting agenda, and a template for area recovery steps.**
**See p. 127-134**

Declaring the business disruption and agreeing on the appropriate time to initiate operations under the business continuity plan can be difficult and requires advance planning.

There is a natural tendency for people to delay action until they are "certain" that a disaster is imminent or is serious enough to react. Therefore it is important to give clear guidelines on the declaration of a business disruption (business continuity event).

Figure 8 depicts an example of a declaration process.

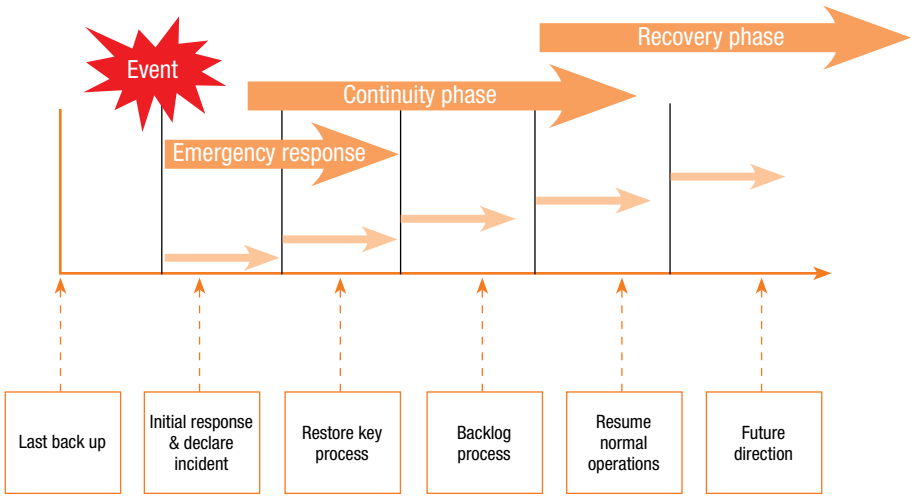
**Figure 8 - Example of a pictorial business disruption declaration procedure**




## Phases of a business disruption

It is useful to consider the likely phases an entity may experience during a business disruption event. Figure 9 depicts an example of the phases of a business disruption

**Figure 9 - Phases of a business disruption**




Source: *A practitioners Guide to Business Continuity Management, HB 292:2006, 2006, Standards Australia,* p.79.

**IMPORTANT UPDATE**

Each phase is described as follows:

- emergency response: this is the tactical response to the event. It occurs immediately after the event, and primary concern is the protection of life and safety. The transition from emergency response to continuity needs to be explicitly managed;
- continuity: this is the strategic and operational response to the business disruption. During this period the entity relies on alternative processes and resources, and aims to establish at least the minimum level of capability and performance required; and
- recovery: this is the strategic and operational response to the business disruption. During this period the entity returns to routine business processing, and aims to operate at the business-as-usual level of capability and performance.

## Some examples of business continuity events

A resilient entity uses the management of a business disruption as an opportunity for value creation or development.

*It's too late for plannin' when you're gettin' hit.*

*- Mohammed Ali.*

The following case studies provide examples of how small, medium and large public sector entities have handled business disruption events

### *Small entity: National Blood Authority – Hailstorm floods the office*

**Case study - Implementation of a Business Continuity Plan for the whole entity**

In 2007 the National Blood Authority (NBA) received a 'highly commended' award from Comcover, in the 'Risk Initiative' category, for its implementation of business continuity management. On the night of Tuesday 27 February 2007, a severe storm swept through Canberra. There was extensive damage to the city centre resulting in the closure of a number of buildings. The NBA's offices in Turner were flooded: computers were destroyed; carpets were ruined; furniture water logged and internal walls damaged. A building assessment identified the need to refit the entire office – a process which would take between three and four weeks. The NBA's Business Continuity Plan (BCP) was implemented.

**Business continuity planning proved effective** - Business continuity planning was guided by the NBA's risk management and crisis management plans. Key elements of the plan focussed on the need to restore information technology services as soon as possible to enable the NBA to operate with minimal disruption – the priority was to relocate the information technology infrastructure to temporary premises. The business continuity team worked quickly to salvage equipment, contact staff, and plan the next steps. The business continuity team moved the recovery operations to the General Manager's home where the business priorities were articulated and alternative plans for NBA operations were made.

**Stakeholder relationships maintained** - Paramount to the business continuity plan, and a high priority for the NBA, was effective management of stakeholder relationships during the crisis. By 8:30am the NBA was able to start contacting key stakeholders, including blood and corporate suppliers, to advise them that business processes would not be disrupted. A media release was issued and a communiqué placed on the NBA's and Department of Health and Ageing's websites.

## IMPORTANT UPDATE

**Operating at temporary offices** - The National Blood Authority relocated to temporary offices in Fyshwick whilst the Turner offices were refurbished. The NBA had moved and by lunchtime on Friday 2 March 2007, information technology services were operational – a mere two and a half days after the disaster. The plan demonstrated the NBA's organisational efficiency and ability to continue functioning effectively. During this period the NBA successfully negotiated a contract with a contingent supplier of a product – a major achievement under the circumstances!

**Staff response** - Staff members responded well to the significant change in their working environment and demonstrated cooperation and high spirit. Some were happy to hot-desk in the temporary offices while others were able to work from home - flexibility of staff was the key.

**Demonstrated achievement** - The benefits of the BCP are clear – where other premises in the city remained uninhabitable, the NBA was able to return to operational capacity within a very short period of time through the effective implementation of the BCP. This was done without major disruption to business requirements. The NBA calculates that a total of just 17.5 business hours were lost for most staff from the initial decision that staff could not enter the damaged premises on the morning of Wednesday 28 February 2007 to the move to temporary premises on Friday 2 March 2007, and then the return from the temporary site back to the restored premises (which was done overnight). The most significant achievement of this process was the ability of the NBA to demonstrate to stakeholders that it had planned for a business contingency and that it was capable of implementing that plan to a high standard. This has built credibility with stakeholders of the NBAs capacity to think strategically and act decisively when confronted with risks.

**Post incident review** – following the return to normal services, the NBA conducted a post incident review. This review identified a number of improvements to the BCP, including to the content of the crisis kits, the need to improve remote IT access, and the importance of pandemic planning. A number of business processes were also improved, such as incorporating flexible working arrangements into the Certified Agreement, and improved productive working relationships with suppliers.

Source: *NBA submission to Comcover's Awards for Excellence in Risk Management 2007.*

**IMPORTANT UPDATE**

## *Medium entity: Australian Electoral Commission – Election 2007's virtual tally room*

**Case study - Implementation of a Business Continuity Plan (IT Disaster Recovery component) for an event**

In delivering the 2004 federal election, the Australian Electoral Commission (AEC), experienced a number of disruptions to one of its critical business processes. As a consequence the AEC engaged an external party to conduct an independent review of business critical systems. The issues experienced by the AEC are detailed in its submission to the Joint Standing Committee on Electoral Matters' *Inquiry into the Conduct of the 2004 Federal Election.*

**Business continuity management reinvigoration** - Following the external review and parliamentary inquiry, the AEC decided to reinvigorate its business continuity management program, with the key outcome being preparation for the 2007 federal election. The AEC focused on selected business activities identified as being critical during the election period: the election call centre, the virtual tally room, the National Tally Room, the production of ballot papers, the payment of temporary staff, the production of certified lists and the issuing of postal votes. Several of these functions involved coordination through the national office with state and divisional office delivery. External assistance was used to tailor the existing business continuity plan template to fit election-critical activities. Workshops were held with national office and state and divisional office staff, to increase awareness and skills in business continuity planning and to develop the content of specific plans.

**Building resilience** – the AEC implemented a number of continuity measures in preparation for a possible disruption to the virtual tally room, building on the continuity strategies put in place in 2004. For example, the contract for the operation of the virtual tally room required the provider to demonstrate extensive continuity measures, including a fully redundant alternative hosting site. The AEC also conducted comprehensive testing and practice runs during the weeks prior to polling day. One of a number of contingency measures put in place was a complete manual processing alternative at the national tally room in Canberra.

**A critical election services** - the virtual tally room is a comprehensive results and information service accessible via the AEC website. For the 2007 election, the results of counting were made available to Australia and internationally, and were updated every 90 seconds on election night. The virtual tally room received over 43 million hits, an increase from 13.5 million in 2004, and handled in excess of 172 000 unique visitors (42 000 in 2004). The data from the virtually tally room is also fed to media organisations, to facilitate their coverage of the election.

**Continuity of a critical service** - A hardware failure within the primary hosting site occurred during election night. Processing of the election results was immediately transferred to the secondary site. The AEC estimates that the switchover process between sites was completed in under five minutes. While the AEC's election hosting support team was able to quickly restore the primary site, its incident management team chose not to switch back, due to the increased risk this posed – instead, the primary site became the 'back-up' for processing the results.

**Results achieved** - The AEC's business continuity preparations for 2007 prevented a disruption to one of its critical business process: the virtual tally room. On election night and during subsequent further counting, the virtual tally room represented a robust system that provided users with reliable, rapid access to results, reflecting up-to-date information.

Source: ANAO analysis.

**IMPORTANT UPDATE**

## *Large entity: Australian Taxation Office – Burst water pipes in head office*

**Case study - Implementation of a Business Continuity Plan for a single site**

The Australian Taxation Office (Tax Office) is the Government's principal revenue collection agency, and its role is to manage and shape tax, excise and superannuation systems that fund services for Australians. Audit Report No.16 of 2007-08, *Administration of Business Continuity Management in the Tax Office* details the business continuity arrangements in the Tax Office.

**Frequency of business continuity disruptions** - The majority of business continuity events experienced by the Tax Office, as recorded on its Business Continuity Planning database, relate to facilities, specifically buildings. In the past few years, a range of natural disasters as well as power failures and flooding due to burst water pipes have rendered all or part of at least one Tax Office building unusable each year. However with some 70 office locations across Australia, the Tax Office has been able to transfer the operation of critical processes to other buildings or locations. This has created a multi-dimensional capacity to perform critical processes despite the loss of a site.

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

**Emergency response** - A number of Tax officers reacted quickly and, in conjunction with emergency services, determined that the building was safe. The National BCM Director, who is based in Brisbane, was present in Canberra and coordinated the Tax Office response.

**Crisis management** - A number of crisis meetings were called and priority processes were allocated work space within the remaining National Office sites (including the recently redundant former National Office accommodation). Most staff were sent home and advised to call the 1800 emergency help line telephone number to be informed of updates.

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

Source: Adapted from a case study in Audit Report No.16 of 2007-08, *Administration of Business Continuity Management in the Tax Office.*

**IMPORTANT UPDATE**

## Returning to normal operations

During the earlier stages of their business continuity program, entities need to think through and document reconstitution procedures just as carefully as business continuity procedures. This will help ensure that the continuity approaches selected are supportive of a relatively seamless return to normal. A solution that gives an easy recovery, but makes it difficult to return to normal operations is not an effective continuity approach.

The return to normal services is the point that the business disruption is officially declared 'over'. At this point, entities will 'stand down' or deactivate their business continuity plan, and return to the business as usual management structure. It is important to document this decision.

Following the stand down of the business continuity plan and the return to normal operations, communications may be undertaken to bolster staff and stakeholder confidence.

## Post incident review

It is important to record and evaluate the business disruption. This facilitates the review of the business continuity response after the entity has returned to normal operations. By analysing successes and failures, lessons to be learned can be drawn out and actions can be taken to prevent future failures and to replicate and repeat successes.

A post incident review can be conducted the same way as a post exercise review. See *Post exercise review* in the section of the Guide on *Maintaining the program and plan: testing, exercising, updating and reviewing,* for an example list of questions to be answered in the post incident review. Alternatively, a route cause analysis, or other structured and systematic evaluation methodology may be used to review an incident or exercise.

**The Workbook contains a checklist for suggested post incident review questions. See p. 136**

## Continuity event reporting

The post incident review can be written up in a lessons learned report, with actions assigned to implement recommendations. This report needs to be provided to relevant parties, such as the business continuity committee.

***Finally, do not forget to thank staff for their efforts during the business disruption!***

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Maintaining the program and plan: Testing, exercising, updating and reviewing

Testing the plan

Exercising the plan

Updating the plan

Reviewing the program

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Maintaining the program and plan: Testing, exercising, updating and reviewing

This section of the guide provides guidance for entities on how to maintain the business continuity plan. This involves:

- testing the plan;
- exercising the plan; and
- updating the plan.

It also discusses assurance through reviewing the business continuity program.

*Fate favours the prepared.*

*- Translation adapted from Louis Pasteur.*

Maintaining the business continuity plan is essential to ensure it reflects the entity's objectives, critical processes and resources, and an agreed priority for recovery. Testing, exercising, and updating the recovery process documented in the business continuity plan will provide management assurance that the plan is effective - that is, it will ensure continuity of business if critical processes are lost.

**The Workbook contains a checklist for maintaining the business continuity program. See pp. 138-139**

Realistic and robust testing and exercising will often reveal areas requiring attention. If test results do not reveal opportunities for improvement, entities need to examine the adequacy and realism of their tests.

## Testing the plan

The terms 'test' and 'exercise' are sometimes used interchangeably in a business continuity context. However, the term 'test' can have negative connotations, as it implies a 'pass' or 'fail' aspect. Subsequently, the term 'testing' is often used when a technological feature is being trialled. For example, testing the rebuilding of a server from back-up tapes. Testing can be one outcome of an exercise.

**The Workbook contains a checklist for testing the plan, manual processing, and IT back-up procedures. See pp. 140-142**

## Exercising the plan

In better practice entities, an exercise program is developed so that over time, the entity gains assurance that the business continuity plan will operate effectively if and when required. This forward-looking exercise program is sometimes called a 'universe'. The major components of the business continuity plan should be exercised annually and updated based on the results of each exercise. It is important each component be individually exercised. Also, where an entity has critical interdependent processes or has outsourced any activity, the exercise needs to involve the relevant external party or outsourced provider. Exercising can be disruptive - it therefore requires commitment from management to allocate sufficient resources.

Caution must be applied if exercising the business continuity plan as a whole. This type of exercising is resource intensive and may itself cause a business disruption event. It is normally only conducted by entities with a mature business continuity approach that has been exercised and developed over time.

## IMPORTANT UPDATE

An approach is to start at the first hour, on the first day, at the point of the disruption. Each recovery team can then explain the process they would go through to recover their operations. The other teams can challenge the approach and identify any weaknesses detected in the plan. For example, asking:

- "Where would you obtain that information?"; or
- "Isn't that process dependent on the completion of another activity?".

Some approaches for exercising the business continuity plan are listed in Table 6.

**Table 6 - Approaches for exercising the business continuity plan**

| Exercise approach | Exercise purpose | Exercise description |
|---|---|---|
| Manual verification | Ensures the required recovery material is available as stated in the business continuity plan. May also ensure information and lists of the forms, supplies, equipment, inventories and associated vendor contact details are accurate. | This test requires checking that all required data, supplies and/or other hardcopy documents (as documented in the business continuity plan) are actually backed up and correctly stored off-site. It may also check that all information is accurate including phone number, address and key vendor contracts. It would verify whether the listed supplies, equipment or services are available for delivery or what the current lead time is. |
| Call out / Unannounced recovery team assembly | Ensures the lists for mobilising recovery teams are up to date and the teams can be mobilised in the required time. | The exercise is conducted as follows:<br>• the Recovery Coordinator contacts a number of team members on the notification contract list;<br>• on a rotating basis, the exercise is scheduled for: normal work hours; lunch time; after normal work hours on a weekday; and the weekend;<br>• the Recovery Coordinator notes the time the calling process starts and the time at which each team member was contacted; and<br>• the Recovery Coordinator reports on exercise results. |
| Desktop review | Ensures those individuals with responsibilities in the business continuity plan are aware of the plan and their responsibilities. | The recovery coordinator provides individuals with a presentation and discusses the content of the plan, and how it would be used in a disruption event. |

## IMPORTANT UPDATE

| Exercise approach | Exercise purpose | Exercise description |
|---|---|---|
| Desktop scenario / Structured walk-through / Simulation | Ensures the business continuity plan procedures are adequate. | The exercise requires the Recovery Coordinator to develop a disaster scenario and lead the service teams through a mock recovery (or engage a facilitator to run the scenario). The scenario chosen should be relevant and believable. The exercise is conducted as follows:<br>• all team leaders meet in a room to be given the scenario;<br>• they each work through their recovery team plans paying particular attention to the interaction with other teams; and<br>• issues identified should be immediately noted by the Recovery Coordinator to be discussed at the exercise debrief. |
| Partial live scenario | Ensures aspects of the business continuity plan can be effectively implemented if required. | The exercise requires a facilitator to develop and run a 'real time' mock scenario. The scenario chosen should be relevant and believable. The exercise is conducted as follows:<br>• the facilitator provides the Recovery Coordinator and recovery team members with mock information advising them on a disruptive event;<br>• the recovery team is responsible for assembling itself;<br>• the facilitator provides additional information to the recovery coordinator and members of the recovery team throughout the exercise (for example makes phone calls, emails them, presents them with mock media releases);<br>• the recovery coordinator and team members simulate undertaking actions as per their recovery team continuity plan; and<br>• issues identified should be noted by the facilitator or observers to be discussed at the exercise debrief. |
| Live scenario | Ensures the business continuity plan can be effectively implemented if required. | The exercise involves the closing down, or removal of access to a crucial activity or resource. This exercise is about the recovery of the lost elements, as well as the establishment of the alternative site.<br>Exercises of this nature are only recommended for entities with a mature business continuity solution. |

Note: These exercises are listed in order from lower cost and lower capability development, to higher-cost and higher capability development.

**The Workbook contains an exercise universe, and an exercise preparation template. See pp. 143-145**

**IMPORTANT UPDATE**

## *Post exercise review*

The debrief is often the most valuable aspect of an exercise for the entity. It is important to dedicate time to identify:

- whether the aims of the exercise were achieved;
- what worked well;
- what did not work well;
- lessons learned;
- improvements or revisions that need to be made to the business continuity plan; and
- areas for future tests and exercises.

**The Workbook contains a checklist for conducting a post incident review.**
**See p. 136**

Better practice entities provide a written report of the exercise to the business continuity committee. Better practice entities will also assign responsibility for implementing any recommendations and monitor progress.

The post exercise review can be conducted in the same way as a post incident review.

**Case study: Partial live scenario exercise**

The Australian Taxation Office (Tax Office) is the Government's principal revenue collection agency, and its role is to manage and shape tax, excise and superannuation systems that fund services for Australians. Audit Report No.16 of 2007-08, *Administration of Business Continuity Management in the Tax Office* details the business continuity arrangements in the Tax Office.

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

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

**Nature of the exercise** - The exercise principally involved bringing together the Northbridge business continuity team. This team exercised a real time scenario that involved Tax Office processes being threatened by a loss of staff due to multiple causes, such as a possible pandemic and sabotage. The Northbridge team came together quickly and notified relevant Tax Office staff locally and nationally. The team effectively managed the situation they were presented with and approached the exercise in a professional manner.

**Post exercise review** – Immediately following the exercise, a review of the scenario was conducted. This review involved all personnel involved in the incident. A number of lessons were learned and subsequently incorporated into a revised plan.

**Outcome** - As a result of the simulation nature of the exercise, Northbridge staff were exposed to practical experiences, and gained the skills required in relation to business continuity management.

Source: Adapted from a case study in Audit Report No.16 of 2007-08, *Administration of Business Continuity Management in the Tax Office.*

**IMPORTANT UPDATE**

## Updating the plan

Plans must be kept up-to-date to provide support for business continuity. Better practice entities have guidelines for periodic exercising, documentation maintenance, and ongoing training. Responsibilities for various aspects of business continuity plan updates are also established.

A business continuity plan is easily maintained if changes in the business and/or data processing environment initiate reviews and update the business continuity plan. When any component of the business continuity plan is affected, the following steps are taken:

- the effect of the change is evaluated using a business impact analysis focusing on the new component(s) and any new interrelationships which occur;
- the business continuity plans are modified to reflect the change; and
- the Recovery Coordinator determines exercising requirements and schedules an exercise, if necessary.

**The Workbook contains a template timetable for updating the business continuity plan.**
**See p. 147**

## Reviewing the program

Better practice entities schedule regular internal audit or external reviews and evaluations of their business continuity program.

Better practice entities also undertake self assessments against their objectives, considering relevant standards and guidance documents.

Reports of the audits, reviews and self assessments should be provided to the business continuity committee. Responsibility for implementing any recommendations made to improve performance needs to be assigned.

**Implementing a business continuity management program - Checkpoint 5**

| Checkpoint 5 | Generic characteristics of better practice business continuity management in public sector entities | Completed | Level of implementation |
|---|---|---|---|
| | Characteristic 7: Business continuity testing and exercises have been conducted. | Yes / No | Basic / Mature |
| | Characteristic 8: The entity monitors business continuity. | Yes / No | Basic / Mature |

Table 1 on page 9 of this better practice guide provides details on the implementation characteristics.

**Further references**

- *Public Sector Internal Audit Better Practice Guide, 2007,* Australian National Audit Office.
- *Public Sector Internal Audit Toolkit,* 2007, Australian National Audit Office.

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Appendices

# IMPORTANT UPDATE

**IMPORTANT UPDATE**

# Appendix 1: Terminology

Given the International focus of business continuity management, a variety of terms are used to describe the same concepts. As a number of terms have become interchangeable in recent years, the terms used in this guide are explained below.

**Table A 1 – Terminology used in this guide**

| Terminology used in this guide | May be referred to in other documents as | Meaning in this guide |
|---|---|---|
| Business continuity management | • Business continuity.<br>• Business continuity management lifecycle.<br>• Business continuity management program.<br>• Business continuity management system. | The development, implementation and maintenance of policies, frameworks and programs to assist an entity manage a business disruption event, as well as build entity resilience.<br>It is the capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a business disruption event. |
| Business continuity plan | | A collection of procedures and information that is developed, compiled and maintained in readiness for use in a business disruption event. |
| Business disruption event | • Business disruption.<br>• Business interruption.<br>• Outage.<br>• Major incident.<br>• Continuity event.<br>• Crisis. | An event that has an effect on the critical business processes of the entity, and inhibits the achievement of its objectives. It may be an acute, creeping, or sustained event. |
| Business impact analysis | • Business impact assessment. | A management level analysis, which evaluates the risks of disruption to critical business processes, including consideration of the impacts of capability loss over time and the need for, and interdependencies of, resources. |

**IMPORTANT UPDATE**

| Terminology used in this guide | May be referred to in other documents as | Meaning in this guide |
|---|---|---|
| Context | | The environment in which the entity seeks to achieve its objectives. It may include the:<br>• cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment;<br>• international, national, regional or local environment;<br>• key drivers and trends; and<br>• perceptions and values of stakeholders. |
| Critical business process | • Key business process. | Vital process without which an entity will either not survive, or will lose the capability to effectively achieve its objectives. |
| Emergency response management | • Emergency management.<br>• Emergency Control Organisation.<br>• Emergency Response Organisation. | Emergency response management addresses the immediate response to the incident and is primarily concerned with the protection and preservation of life and property.<br>It involves the entity managing the impact of an emergency on the entity. It is a different activity to community emergency response management, which involves the entity managing the impact of an emergency on the community. |
| Entity | • Agency.<br>• Organisation.<br>• Public sector entity.<br>• Australian Government. | An Agency, Commonwealth authority and subsidiary, and Commonwealth company and subsidiary, as defined in the *Auditor-General Act 1997.* |
| Incident management | • Event management.<br>• Crisis management.<br>• Strategic crisis management.<br>• Strategic event management. | The strategic management of the response to an emergency or business disruption event. |
| Interdependency | • Dependency.<br>• Partnership dependency. | The reciprocal relation, involving a reliance, directly or indirectly, of one process, activity or resource upon another. |

## IMPORTANT UPDATE

| Terminology used in this guide | May be referred to in other documents as | Meaning in this guide |
|---|---|---|
| Maximum tolerable period of disruption | • Maximum tolerable down time.<br>• Maximum down time.<br>• Maximum allowable outage.<br>• Maximum acceptable outage. | The maximum period of time that an entity can tolerate the disruption of a critical business process, before the achievement of objectives is adversely affected. |
| Recovery point objective | | The point in time (before the business disruption) to which electronic data must be recovered after a business disruption event.<br>For example, data must be recovered to the end of the previous day's processing. |
| Recovery time objective | | The target time set for:<br>• recovery of an activity, product, service, or critical business process after a business disruption event; or<br>• recovery of an IT system or application after a business disruption event. |
| Resilience | • The combination of Risk Management, Security Management, Emergency Management, and Business Continuity Management. | The adaptive capacity of an organisation to a changing and complex environment. |
| Risk management | | Coordinated activities to direct and control an entity with regard to risk. |

**Further references**

- *Australian Emergency Management Glossary,* Australian Emergency Manuals Series, Part I, The Fundamentals, Manual 3, Emergency Management Australia, 1998.
- *Risk Management: Vocabulary,* ISO/IEC Guide 73, 2002.
- *Glossary of Business Continuity Management Terms,* The Business Continuity Institute, 2002

**IMPORTANT UPDATE**

# Appendix 2: Emergency Response Management

## Link to business continuity management

*Emergency response management is the initial tactical reaction to an emergency. The emergency management team is primarily concerned with the preservation of life and property but also has a role in assessing the potential consequences of the disruption and determines whether the event needs to be escalated to the incident management team.*

*Once the incident management team assumes control of the incident, the emergency management team retains tactical responsibility for addressing issues that may occur on site.*

*In smaller entities, the emergency response management team and incident management teams may involve the same personnel, but the functional responsibilities of both teams remain unchanged.*

*An incident that requires emergency response does not necessarily require business continuity management, as the incident may not effect the critical business processes of the entity.*

Emergency response management could be as simple as the activation of a building evacuation plan, or as comprehensive as an emergency management strategy involving the immediate protection of people, property, and resources across multiple sites or communities.

For entities that are located in multiple sites, it may be appropriate to prepare emergency response plans for each location.

## IMPORTANT UPDATE

Typical activities that may be incorporated within an emergency response management plan include:

- building evacuation and role call;
- communication with Emergency Services;
- initial and on-going assessment of the consequences of the disruption on the entity;
- escalation to the incident management team as appropriate;
- addressing immediate people issues, which may include arranging transport, and providing funds, food and drink;
- securing of premises; and
- arranging for salvage of the site.

**Further references**


- *Australian Emergency Manual Series,* Various Years, Emergency Management Australia.
- Australian Emergency Manual Series, *Emergency Management in Australia Concepts and Principles,* Manual Number 1, 2004, Emergency Management Australia.
- *Audit Report No. 27 of 2007-08, Emergency Management Australia,* 2008, Australian National Audit Office.
- *Emergency control organization and procedures for buildings, structures and workplaces,* AS 3745—2002, 2002, Standards Australia.
- *Emergency management and business continuity programs,* Z1600, 2008, Canadian Standards Association.
- *Emergency Management Guide for Business and Industry,* FEMA 141, 1993, Federal Emergency Management Agency.
- *Societal security - Guideline for incident preparedness and operational continuity management,* ISO/PAS 22399:2007, 2007, International Standards Organisation.
- *The Australasian Inter-service Incident Management System,* AIIMS, 2004, Australasian Fire Authority Council.

**IMPORTANT UPDATE**

# Appendix 3: Incident Management

## Link to business continuity management

***Incident management provides for the overall control and strategic response to the situation. It is the incident management team that remotely monitors an event and makes the decision to escalate the incident into a business disruption event (for example a business continuity event).***

***Throughout the business disruption event, the incident management team monitors the situation and makes the strategic decisions required to recover the entity. It also manages conflicts that may occur over resource requirements for business processes and manages communications internally and externally.***

***Business continuity management requires incident management.***

Incident management defines how strategic issues will be managed and addressed by senior management during an emergency and/or business disruption event.

Once the initial emergency response has been performed, focus shifts to the management of the strategic impacts. This is called incident management.

For some events that are not physical, the first response may be incident management (for example IT failure, regulator notice, or fraud). Alternatively, it may be that the event being managed falls outside of the scope of business continuity and is not directly related to a business disruption (for example negative media exposure that has no business continuity implications). Because of this, the incident management team may be activated without any need for the emergency management plan or business continuity plan to be activated. However, emergency management and business continuity management require incident management.

By their nature, crises and incidents will vary and the incident management plan will include components and resources that are valuable in assisting the strategic decision making of management. To facilitate incident management, a plan identifies the resources necessary to undertake the strategic management of the incident that has occurred.

To facilitate the strategic decision making, incident management teams usually establish a command centre from which to direct operations. Typically, multiple command centres will be identified within a plan to address the situation where a primary site is unavailable.

## IMPORTANT UPDATE

It is likely that an incident management team will incorporate individuals that are skilled in:

- strategic thinking;
- internal and external communication;
- the operations of the entity;
- finance; and
- human resources.

Strategic decision making during an incident is key to a successful outcome and will include the decision to escalate from a strategic response into a full business continuity response.

Communications internally and externally and media responses are a key component of managing a strategic response, and need to be addressed by the incident management plan.

Other components of the plan may be developed to address such things as, liaison with the emergency response management team to understand the implications of the interruption and the progress in resolving the incident. In addition, liaison with business continuity teams to approve the activation of the business continuity plans, approving emergency expenditure, monitoring progress, addressing personnel issues, understanding and addressing the strategic implications of the incident on the entity are all likely to be required.

**Further references**

- *British Standard, Business Continuity Management – Part 1: Code of practice,* BS25999-1:2006, 2006, British Standards Institution. (see Section 8).
- *Business Continuity Management (authorised deposit-taking institution),* Prudential Standard APS 232, 2005, Australian Prudential Regulation Authority (see paragraph 30).
- *Connecting Government: Whole of government responses to Australia's priority challenges,* 2004, Management Advisory Committee (see Ch 7 Managing crises and their consequences).
- *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2007 Edition,* 2007, National Fire Protection Authority (see Section 5.9).
- *The Business Continuity Institute Good Practice Guidelines,* 2008, Business Continuity Institute (see Stage 3.1).

**IMPORTANT UPDATE**

# Appendix 4: Pandemics

## Link to business continuity management

*Smaller entities may choose to combine their business continuity and pandemic plans. If a combined plan is prepared, the entity needs to pay particular attention to the 'people' issues in the business continuity plan, including planning for reduced capacity and extended absences during a pandemic.*

*If separate plans are prepared, is not necessary to 'double-up' on activities or repeat information; the business continuity plan and pandemic plan should cross-reference each other. The business impact analysis from the business continuity plan can be re-used in the pandemic plan.*

*Many business continuity plans assume that some part of the entity is unaffected, and can provide the required capacity for the entity to provide services. They also assume the business disruption is short, and recovery can begin quickly. An influenza pandemic would be widespread and prolonged affecting not only the entity but many of its suppliers of goods and services; therefore a different continuity response is required.*

*A pandemic is a scenario that can be used to jointly exercise a pandemic plan and a business continuity plan.*

## Introduction

A pandemic is a global disease outbreak. A pandemic can start when a new virus or virus subtype emerges in humans that is capable of causing severe disease (and death) and transmits easily and rapidly between humans.[23]

Whilst Acquired Immunodeficiency Syndrome (AIDS) is an example of an ongoing pandemic, it is the emergence of a highly infectious and virulent disease for which there is little or no natural immunity in the human population that presents the worst case scenario. An example is Severe Acute Respiratory Syndrome (SARS) that emerged suddenly in 2002-2003, demonstrating that in the 21st century a pandemic virus could spread rapidly across borders with major health, social and economic impacts. Another example is an influenza pandemic.

[23] United Nation and World Health Organization influenza sites - http://www.un-influenza.org and http://www.who.int/csr/disease/avian_influenza/en [accessed 16/1/2009].

## IMPORTANT UPDATE

Influenza pandemics have occurred at irregular intervals throughout history. In the twentieth century, the world experienced three influenza pandemics:

- Spanish Influenza (1918-1919) – this pandemic caused the highest loss of human life. Worldwide, at least 50 million people are thought to have died, with over 10 000 Australians losing their lives. Most deaths occurred in young, previously healthy people, aged between 15 to 35;
- Asian Influenza (1957-1958) – this was milder than Spanish Influenza, with most deaths occurring in the young and the elderly; and
- Hong Kong Influenza (1968-1969) – this was the least severe of the three influenza pandemics of the twentieth century. Deaths were primarily in the over 65 age group.[24]

Since 2003, the World Health Organization (WHO) has reported outbreaks of H5N1 avian influenza (bird flu) affecting birds in countries in south and central Asia, Africa and Europe. Between December 2003 and December 2008, the WHO has confirmed there were 391 human cases of H5N1 influenza infection with 247 deaths.[25] While the virus has not yet developed the capacity to transmit efficiently from human-to-human, the widespread nature of H5N1 in birds has increased the risk of an influenza pandemic occurring in humans.

Further, in 2009 we are seeing the spread of swine influenza A (H1N1). At the time of publishing this guide, the WHO was coordinating a global response to human cases of swine influenza, and monitoring the corresponding threat of an influenza pandemic.

It is not possible to predict when pandemics will occur, how severe it will be, or how long it will last. The WHO reports that the world is moving closer to a pandemic, and history supports the fact that it is 'more likely than not' that a pandemic will occur. It is estimated an influenza pandemic could last from seven-to-ten months in Australia,[26] with impacts on the health system, the economy and society potentially lasting longer. At the peak of the pandemic, staff absences may be in the range of 30-50 per cent[27] due to illness, travel restrictions, or the need to care for family. Reduced staffing levels may coincide with a surge in the demand for services from agencies that are involved in the response to the pandemic and may also affect an agency's ability to service and maintain its physical infrastructure.

In addition, transport systems may be disrupted, communications systems may be overloaded, schools may be closed, and suppliers of goods and services may close. There is likely to be widespread uncertainty and panic in the community.

Therefore, it is important that entities at all levels of Australian government have appropriate management plans in place in advance of a pandemic to minimise the impact of a business disruption event caused by a pandemic, and to expedite recovery.

[24] *Australian Health Management Plan for Influenza Pandemic,* 2008, Department of Health and Ageing and *Business Continuity Guide for Australian Businesses,* Appendix C – Background on previous pandemics, 2006.

[25] World Health Organization, *Cumulative Number of Confirmed Human Cases of Avian Influenza A/(H5N1) Reported to WHO,* http://www.who.int/csr/disease/avian_influenza/country/cases_table_2008_09_10/en/index.html [accessed 14/10/2008].

[26] *National Action Plan for Human Influenza Pandemic - Working Draft,* Council of Australian Governments. Working Group on Australian Influenza Pandemic Prevention and Preparedness, 2008, p. 4.

[27] *Australian Health Management Plan for Influenza Pandemic,* 2008 Department of Health and Ageing, 2008 p. 16.

**IMPORTANT UPDATE**

## Pandemic preparedness

The National Action Plan for Human Influenza Pandemic outlines how Commonwealth, state, territory and local governments will work together to protect Australia against the threat of an influenza pandemic and support the Australian community should one occur. It asks entities at all levels of the Australian Government to have in place:[28]

- planning to ensure the continuity of the services they deliver to the Australian public. This means identifying the essential government services they are responsible for and how these services will continue to be delivered during an influenza pandemic; and
- planning to ensure the continuity of their business operations. This includes preparing for absences through illness, caring for infected family members and parenting responsibilities due to the closure of schools and childcare facilities. Plans also need to be developed to ensure the continuation of IT support, legal services, occupational health and safety requirements and staff welfare and counselling services.

The *Commonwealth Government Action Plan for Influenza Pandemic (2006)* outlines Australian Government responsibilities and high-level actions to prevent and manage an influenza pandemic and its consequences in Australia. It provides a resource for Australian Government agencies and their related bodies to continue to revise agency plans for managing the impacts of an influenza pandemic as part of their business continuity planning, taking into consideration issues such as:

- policies for conditions of service/people management;
- agency priority activities and critical business processes;
- continuity of income support and payment systems;
- knowledge management arrangements;
- legislative and contractual obligations;
- continuity of contracted Australian Government services, including not-for-profit organisations; and
- continuity of key suppliers where required (ICT, building security, property, cleaning and employee assistance programs).

## A planned response to a pandemic

To meet the challenge of a pandemic, it is essential to prepare in advance of the event. Pandemic preparation provides an opportunity for entities to develop robust procedures and improve administrative operations and processes. For example, the following elements of good administration and public sector governance will assist in pandemic preparation:

- up-to-date policies (for example pandemic policy, business continuity policy, sick, personal and carers leave policies, insurance policy and records management policy);
- effective knowledge management (for example standard operating procedures and records management);
- succession planning (for example identifying key personnel, rotating positions and cross-skilling);
- flexible work practices (for example remote access, working from interstate offices, working from home and engaging with relevant unions);

[28] *National Action Plan for Human Influenza Pandemic - Working Draft,* Council of Australian Governments. Working Group on Australian Influenza Pandemic Prevention and Preparedness, 2008, p. 26.

**IMPORTANT UPDATE**

- responsible sickness behaviour (for example not encouraging or allowing sick employees to come to work);
- understanding legislative requirements (for example Occupational Health and Safety and Duty of Care); and
- two-way communication with staff and stakeholders on key issues (for example ensuring relevant parties know the entity has a pandemic plan, and ensuring employees know their pay entitlements and responsibilities during a pandemic).

**The Workbook contains an example table of contents for a pandemic plan (or section on pandemics within a business continuity plan). See p. 124**

Introducing good hygiene practices in the workplace prior to a pandemic provides an opportunity to reduce absenteeism, improve the health of staff, and achieve a more productive workplace.

Entities that choose to prepare a separate Pandemic Plan may find it useful to structure their plan according to the activities they will undertake during each Australian 'phase' of a pandemic.[29]

Activities that entities might consider in their pandemic plan include:

- hygiene and cleaning practices (for example using alcohol-based sterilisers for hand cleaning in bathrooms and at desks, sterilising work surfaces, making face masks available to staff and training them in proper usage techniques);
- human resources (for example sick leave management, social distancing, staff rotation, engaging retirees and contractors to assist in the delivery of services);
- facilities (for example working from home and remote offices);
- transport (for example engaging private transport);
- communications (for example to staff and external stakeholders);
- interdependencies (for example which entities and organisations rely on your services and activities, which entities and organisations do you rely on, shortages in supply);
- continuity of services and activities (for example prioritisation, transfer, relocation); and
- revision of pandemic and continuity planning, based on emerging situational information.[30]

It is important that a pandemic plan is a living document. This requires it to be communicated to staff, exercised, and updated on a regular basis.

## Recovering from a pandemic

Recovery planning and actions commence at the earliest stages of planning for a pandemic. This will support the fastest possible return to normal operations.

Recovery issues to consider include the psychological consequences of a pandemic; permanent closure of suppliers who were unable to recover from the pandemic; staff and skills shortages; and the financial impact of a pandemic on staff and the entity.

[29] Leslie Whittet, *Continuity Forum Pandemic Planning Workshop,* 2008, Pandemic Plan Framework.

[30] Leslie Whittet, Continuity Forum Pandemic Planning Workshop, 2008, *Pandemic Plan Framework; National Action Plan for Human Influenza Pandemic,* 2006, COAG, Department of the Prime Minister and Cabinet, p. 25; *Business Continuity Guide for Australian Businesses,* 2006, Department of Industry, Tourism and Resources; and *Building Resilience Through Business Continuity and Pandemic Planning (for non-government organisations),* 2008, the Department of Families, Housing, Community Services and Indigenous Affairs.

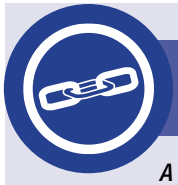
## IMPORTANT UPDATE

**Further references**

- *Australian Health Management Plan for Influenza Pandemic,* 2008 Department of Health and Ageing.
- *Audit Report No.6 2007-08, Australia's Preparedness for a Human Influenza Pandemic,* Australian National Audit Office.
- *Building Resilience Through Business Continuity and Pandemic Planning (for non-government organisations),* 2008, the Department of Families, Housing, Community Services and Indigenous Affairs.
- *Business Continuity Guide for Australian Businesses,* 2006, Department of Industry, Tourism and Resources.
- *Commonwealth Government Action Plan for Influenza Pandemic,* 2007, The Deputy Secretaries Interdepartmental Committee on Influenza Pandemic Prevention and Preparedness.
- *National Action Plan for Human Influenza Pandemic,* 2006, Council of Australian Governments Working Group on Australian Influenza Pandemic Prevention and Preparedness, Department of the Prime Minister and Cabinet. (An updated version is due for release in 2009).
- *Pandemic Planning and Risk Management,* PPG 223, 2006, Australian Prudential Regulation Authority.
- *Pandemic Planning in the Workplace,* 2009 (Draft), Council of Australian Governments Working Group on Australian Influenza Pandemic Prevention and Preparedness, Department of the Prime Minister and Cabinet.

**IMPORTANT UPDATE**

# Appendix 5: IT Disaster Recovery



## Link to business continuity management

*A key part of any business continuity response is to provide the resources necessary to enable an entity to continue to provide an acceptable level of service.*

*Information Technology (IT) systems are essential to most organisations and very few can operate for anything other than a short period of time without computer support.*

*IT disaster recovery planning is the mechanism by which technology systems are recovered in line with the needs of the entity. IT disaster recovery plans should be designed to meet the needs of the entity achieving no less than the required recovery time objective and recovery point objective defined within the business impact analysis.*

Information Technology disaster recovery is the process by which computer systems and associated infrastructure is recovered following a disruption to services. In some cases, IT disaster recovery plans may encompass other technical facilities such as telephony.

The recovery of IT systems should be based on the requirements of the entity that the systems support. However, the speed of recovery required will have a significant effect on the cost and complexity of the solution that is deployed.

The type of solution required to address IT disaster recovery needs is based on two main parameters. These being:

- recovery point objective, which is the point in time (before the business disruption) to which electronic data must be recovered after a business disruption event. For example, data must be recovered to the end of the previous day's processing; and
- recovery time objective, which is the target time set for recovery of an activity, product, service, or critical business process after a business disruption event, or recovery of an IT system or application after a business disruption event. Note: The recovery time objective must be less than the maximum tolerable period of disruption. If it is greater, manual processing must be developed for interim processing.

Entities may wish to explore the option of shared arrangements for IT recovery with other entities.

## IMPORTANT UPDATE

For an entity that requires a very fast recovery time objective and no data loss (zero recovery time objective), it may be necessary to duplicate the entire technology environment at an alternative site. Clearly, this is a very expensive and complex solution that would require the real time update of data at both sites.

Conversely, for an entity that can accept a recovery time objective of 48 hours and also accepts the loss of data accumulated over the last 24 hours, a traditional lower cost recovery from off-site tape based data backups may be appropriate.

It is the requirements of the entity that are crucial and determine the level of sophistication required by the IT disaster recovery plan. Recovery time objective and recovery point objective for each software application are determined as part of the business impact analysis. The point in time of the business cycle can also effect the maximum tolerable period of disruption.

IT disaster recovery plans contain the tasks and processes that need to be undertaken to effect the recovery in line with the required recovery time objective and recovery point objective. In most cases, successful IT disaster recovery plans will need to identify a second site at which systems can be recovered. They may also identify how the infrastructure, hardware, specialist equipment, application software, infrastructure and associated data will be accessed and/or recovered.

**Further references**


- *Australian Government ICT Security Manual (ISM),* ACSI 33, 2008, Department of Defence, Defence Signals Directorate.
- *Code of Practice for Information and Communications Technology Continuity,* BS25777 / PAS 77, 2008, British Standards Institute.
- *Contingency Planning Guide for Information Technology Systems,* NIST Special Publication 800-34, 2002, National Institute of Standards and Technology.
- *Control objectives for information and related technology,* COBIT 4.1, 2007, ISACA.
- *Information Security Management,* ISO 27001, 2005, International Standards Organisation.
- *Information technology - Security techniques - Code of practice for information security management,* ISO/IEC 17799:2005, 2005, International Standards Organisation.
- *Information technology – Security techniques – Guidelines for Information and communications technology disaster recovery services,* ISO/IEC 24762:2008, 2008, International Standards Organisation.
- *Information Technology Service Management,* ISO 20000 – 1, 2005, International Standards Organisation.
- *Information Technology Service Management* – Code of Practice ISO 20000 – 2, 2005, International Standards Organisation.
- *Protective Security Manual,* 2005, Attorney-General's Department.

**IMPORTANT UPDATE**

# Appendix 6: Risk Management

## Link to business continuity management

*In a business continuity management context, the entity starts from the assumption that the preventative controls were ineffective, or there were no preventative controls in place, and a business disruption event occurs. The entity responds to such events in proportion to their significance - matters of cause and likelihood are no longer relevant.*

*Risk management considers both likelihood and consequences, but does not focus on low likelihood-high consequence events. This is the role of business continuity management. However, it is important that there is coordination between the two approaches.*

*It will also have to determine what needs to be done in advance of any disruption event so that its negative consequences can be mitigated. For example, most entities institute back-up and recovery procedures for the information stored on their computer systems. In the event that there is a loss of data, the consequences are reduced to the extent of the gap between the data set that was lost and the last saved version of that data set.*

*The entity will need to determine what must be done, by whom, and at what time after an event that would otherwise lead to the entity's resources or processes being adversely affected for a period in excess of the maximum tolerable down time.*

Risk is the effect of uncertainty on objectives. All activities of an entity involve risks. Risk management aids decision making by taking account of uncertainty and its effect on achieving objectives, and assessing the need for any actions.

Risk management is an essential pillar of good public sector governance.[31] Public sector governance arrangements must be tailored to the circumstances of individual entities. They should be based on a risk management approach that considers potential benefits and costs associated with activities that contribute to meeting specified objectives. These risks could either prevent the entity from achieving its business objectives, or provide the opportunity for extra benefits to be realised.

To be effective, the risk management process needs to be rigorous, structured and systematic. It is important that the emphasis is on real actions and outcomes so that it does not become a procedures-based exercise. Effective risk management requires an entity to have a risk-assessment culture whereby all major decisions are considered in terms of risk management principles.

[31] See the ANAO's 'House of Public Sector Governance', in various publications such as *Public Sector Governance,* Better Practice Guide, Volume 1 2003.

## IMPORTANT UPDATE

In June 2008, the Department of Finance and Deregulation's Comcover branch published a Better Practice Guide on *Risk Management.* Comcover's guide provides a summary of the key principles and concepts of risk management as well as some practical tips to be considered when implementing or reviewing an entity's framework for managing risk. It also emphasises the importance of developing the right culture for managing risk.

The risk management process generally used in Australia today is modelled on Standards Australia's *Risk Management: AS/NZS 4360:2004.*

To effectively implement risk management within an entity, AS/NZS 4360:2004 requires the entity to develop a framework for risk management that is a set of components that provides the foundations and organisational arrangements for designing, implementing, monitoring and reviewing and continually improving risk management throughout the entity. This includes the development of risk management policy and a risk management plan.

AS/NZS 4360:2004 proposes a logical and systematic methodology for establishing the context, identifying, analysing, evaluating, treating and monitoring and reviewing risks. It also emphasises embedding risk management into the entity's culture through communication and consultation, and the appropriate recording of risks.

In 2009 a new International Standards Organisation standard, ISO 31000, that builds upon AS/NZS 4360:2004, is expected to be released.

**Further references**

- *Enterprise-Wide Risk Management: Better Practice Guide for the Public Sector,* 2002, CPA Australia.
- *Public Sector Audit Committees,* Better Practice Guide, 2005, Australian National Audit Office.
- *Public Sector Governance,* Better Practice Guide, Volume 1 and 2, 2003, Australian National Audit Office.
- *Risk Management,* AS/NZS 4360:2004, 2004, Standards Australia.
- *Risk Management,* Better Practice Guide, June 2008, Department of Finance and Deregulation, Comcover.
- *Risk Management Guidelines,* Handbook 436:2004, 2004, Standards Australia.
- *Risk Management: Principles and guidelines on implementation,* ISO 31000, Forthcoming International Standard.

**IMPORTANT UPDATE**

# Appendix 7: Australian and International References

## Australian resources

### Business Continuity

*Australian Government resources*

| | |
|---|---|
| Attorney-General's Department | http://www.ag.gov.au |
| *See also* | |
| Emergency Management Australia | http://www.ema.gov.au |
| Australian National Audit Office | http://www.anao.gov.au |
| Australian Prudential Regulation Authority | http://www.apra.gov.au |
| Australian Public Service Commission | http://www.apsc.gov.au |
| *See also* | |
| Management Advisory Committee | http://www.apsc.gov.au/mac |
| Department of the Prime Minister and Cabinet | http://www.pmc.gov.au |

*Other resources*

| | |
|---|---|
| Business Continuity Forum | http://www.continuity.net.au |
| Business Continuity Institute | http://www.thebci.org.au |
| The Disaster Recovery Institute | http://www.dri-australia.org |
| Standards Australia | http://www.standards.org.au |

### Risk Management

*Australian Government resources*

| | |
|---|---|
| Australian Prudential Regulation Authority | http://www.apra.gov.au |
| Department of Finance and Deregulation | http://www.finance.gov.au |
| *see also* | |
| Comcover | http://www.finance.gov.au/Comcover |

**IMPORTANT UPDATE**

*Other resources*

| | |
|---|---|
| CPA Australia | http://www.cpaaustralia.com.au |
| Standards Australia | http://www.standards.org.au |

## Emergency Management

*Australian Government resources*

| | |
|---|---|
| Australian National Audit Office | http://www.anao.gov.au |
| Emergency Management Australia | http://www.ema.gov.au |

*Other resources*

| | |
|---|---|
| Australasian Fire Authority Council | http://www.afac.com.au/home |
| Standards Australia | http://www.standards.org.au |

## Pandemics

*Australian Government resources*

| | |
|---|---|
| Attorney-General's Department | http://www.ag.gov.au |
| Australian Prudential Regulation Authority | http://www.apra.gov.au |
| Department of Agriculture, Fisheries and Forestry | http://www.daff.gov.au |
| Department of Families, Housing, Community Services and Indigenous Affairs | http://www.fahcsia.gov.au |
| Department of Foreign Affairs and Trade | http://www.smartraveller.gov.au |
| Department of Health and Ageing | http://www.health.gov.au |
| Department of the Prime Minister and Cabinet | http://www.pmc.gov.au |

## IT Disaster Recovery

*Australian Government resources*

| | |
|---|---|
| Attorney-General's Department | http://www.ag.gov.au |
| Department of Defence – Defence Signals Directorate | http://www.dsd.gov.au |
| NSW Office of Information Technology | http://www.gcio.nsw.gov.au |

**IMPORTANT UPDATE**

## International resources

*Business Continuity*

These references are current at the time of publication.

**Further references**

Canada

- *Emergency management and business continuity programs,* Z1600, 2008, Canadian Standards Association.

Israel

- *Security and Continuity Management Systems,* SI 24001, 2007, Standards Institution of Israel.

Singapore

- *Singapore Standard for Business Continuity Management (BCM),* SS540, 2008, Singapore. (formerly TR:19)

United Kingdom

- *British Standard, Business Continuity Management – Part 1: Code of practice,* BS25999-1:2006, 2006, British Standards Institution. (Formerly PAS 56)
- *British Standard, Business Continuity Management – Part 2: Specification,* BS25999-2:2006, 2006, British Standards Institution.
- *Disaster Recovery: Business tips for survival,* 2003, London Chamber of Commerce and Industry.
- *Expecting the Unexpected,* 2003, The National Counter Terrorism Security Office.
- *The Business Continuity Institute Good Practice Guidelines,* 2008, Business Continuity Institute.

United States of America

- *ASIS Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery,* 2005, ASIS International.
- *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2007 Edition,* 2007, National Fire Protection Authority.
- *Standard Checklist Criteria for Business Recovery,* 2006, US Federal Emergency Management Authority.

**IMPORTANT UPDATE**

| | |
|---|---|
| Federal Emergency Management Agency | http://www.fema.gov |
| British Standards Institute | http://www.bsi-global.com |
| Business Continuity Institute | http://www.thebci.org |
| Canadian Standards Association | http://www.csa.ca |
| Continuity Central | http://www.continuitycentral.com |
| Disaster Recovery Institute International | https://www.drii.org/index.php |
| National Fire Protection Association | http://www.nfpa.org |
| Singapore Standards e-shop | http://www.singaporestandardseshop.sg |

## Risk Management

| | |
|---|---|
| International Standards Organisation | http://www.iso.org/iso/home.htm |

## Emergency Management

| | |
|---|---|
| Federal Emergency Management Agency | http://www.fema.gov |
| Australasian Fire Authority Council | http://www.afac.com.au/home |
| Canadian Standards Association | http://www.csa.ca |
| National Fire Protection Association | http://www.nfpa.org |

## Pandemics

| | |
|---|---|
| World Health Organisation | http://www.who.int |

## IT Disaster Recovery

| | |
|---|---|
| British Standards Institute | http://www.bsi-global.com |
| Disaster Recovery Institute International | https://www.drii.org |
| International Standards Organisation | http://www.iso.org/iso |
| ISACA and IT Governance Institute | http://www.isaca.org |

**IMPORTANT UPDATE**

# Appendix 8: Acknowledgements

The better practice guide was developed by drawing from:

- aspects of key Australian and international business continuity references and standards (listed on page 7 and in *Appendix 7: Australian and International References*);
- findings from ANAO assurance audits (listed in Table 1);
- findings from ANAO performance audits of business continuity;[32] and
- interviews with a range of small, medium and large Australian Government and State Government entities, private sector organisations, and business continuity subject matter experts.

The ANAO records its appreciation of the valuable assistance and insights provided by the following Australian Government entities and private sector organisations:

Australia and New Zealand Banking Group Limited (ANZ).

Attorney-General's Department.
- Emergency Management Australia.

Australian Electoral Commission.

Australian Institute of Aboriginal and Torres Strait Islander Studies.

Australian Maritime Safety Authority.

Australian Securities and Investments Commission.

Australian Taxation Office.

Business Continuity Forum:
- Australian Capital Territory Chapter.

Business Continuity Institute:
- Australian Capital Territory Forum.
- Victoria Forum.

Department of Agriculture, Fisheries and Forestry.

Department of Education, Employment and Workplace Relations.

Department of Families, Housing, Community Services and Indigenous Affairs.

Department of Finance and Deregulation:
- Australian Government Information Management Office.
- Comcover.

Department of Health and Ageing.

Department of the Prime Minister and Cabinet.

Ernst and Young.

IBM Australia Ltd – Recovery Centre.

National Blood Authority.

National Library of Australia.

Qantas Airways Limited.

Reserve Bank of Australia.

State Library of Victoria.

The Treasury.

VicForests.

[32] Audit Report No.53 of 2002-03 *Business Continuity Management Follow-on Audit*, Audit Report No.9 of 2003-04 *Business Continuity Management and Emergency Management in Centrelink*, and Audit Report No.16 of 2007-08, *Administration of Business Continuity Management in the Tax Office.*

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Workbook

**IMPORTANT UPDATE**

**IMPORTANT UPDATE**

# Workbook overview

## Introduction

This workbook provides examples, templates and checklists, for each element of the business continuity management program identified in the 2009 version of the ANAO's *Better Practice Guide Business Continuity Management: Building resilience in public sector entities.*

This workbook should be read in conjunction with the better practice guide - explanatory material for each element of the business continuity management program is provided in the better practice guide.

There is no 'one size fits all' approach to the development of a business continuity program. While this workbook provides entities with examples, templates and checklists for each step in the business continuity program, it is important that entities analyse and assess, in turn, their specific needs, as well as the extent to which the templates are relevant to their entity's objectives, critical business processes and business continuity strategy.

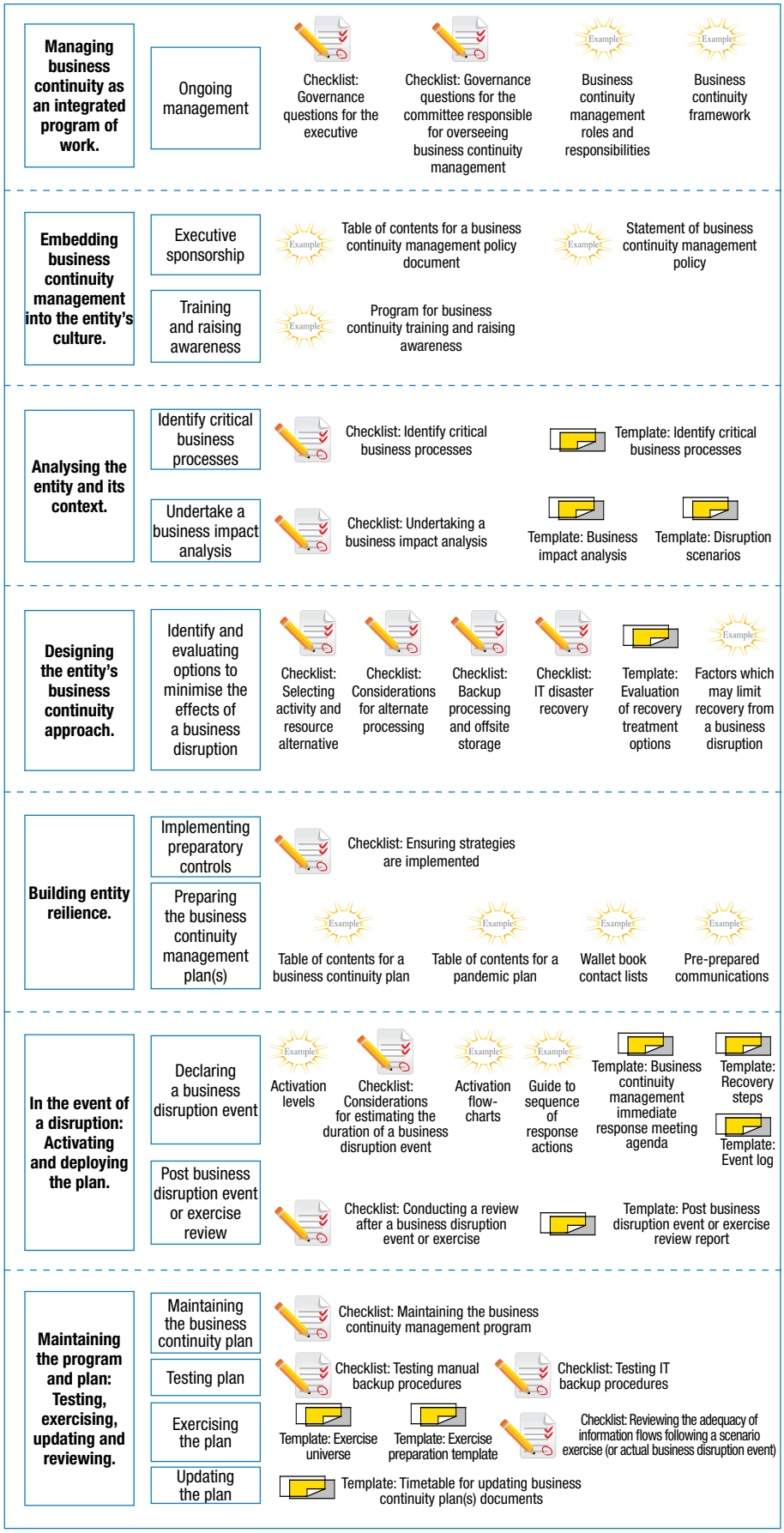
It may not be necessary for an entity to complete all of the templates included, nor does the workbook consist of an exhaustive listing of templates and checklists that may be applicable to some entities. Entities are encouraged to be pro-active in selecting templates to use that will be beneficial for their business continuity management program. Entities are also encouraged to alter the templates so that they are relevant to organisational objectives, the nature and function of the business, the size of the entity, and the locations and distribution of their people, assets and clients.

Note: Some examples sourced from public sector entities use entity specific terminology, which may be inconsistent with the terminology used in other areas of the better practice guide and workbook.

Figure A depicts the structure of the workbook.

**IMPORTANT UPDATE**

Figure A - Structure of this workbook



**IMPORTANT UPDATE**

## Generic characteristics of better practice business continuity management in public sector entities

The ANAO's analysis of public sector business continuity implementation has identified some generic characteristics associated with better practice business continuity management programs.[1] These are depicted in the following checklist. This is not a prescriptive 'black and white checklist' for a business continuity management program – as noted throughout this better practice guide, the development and implementation of a business continuity program needs to be relevant to the entity's operating context.

The following checklist may assist entities in developing and implementing a business continuity management program.

**Details for each characteristic are provided on page 9-12 of the better practice guide.**

**Checklist: Implementation of a business continuity management program**

| Characteristics of better practice business continuity management in public sector entities | Completed Yes/No | Level of implementation (Basic/Mature) |
|---|---|---|
| Characteristic 1: A business continuity management framework is in place. | | |
| Characteristic 2: Training and awareness of business continuity has been conducted. | | |
| Characteristic 3: A risk assessment has been conducted. | | |
| Characteristic 4: A business impact analysis has been conducted. | | |
| Characteristic 5: Preparatory controls have been implemented. | | |
| Characteristic 6: The entity has documented and the executive has endorsed its business continuity plans and framework. | | |
| Characteristic 7: Business continuity testing and exercises have been conducted. | | |
| Characteristic 8: The entity monitors business continuity. | | |

[1] There are several models in the marketplace (for example the Capability Maturity Model Integration and the Control Objectives for Information and Related Technology) which also provide assessment criteria for business continuity implementation, and the impact on business objectives of IT weaknesses.

**IMPORTANT UPDATE**

# Managing business continuity as an integrated program of work

Business continuity management does not have a discrete start and end; it is a continuous and iterative process. Better practice entities manage business continuity on an ongoing basis, integrated with other corporate management processes.

**Explanatory material about ongoing management of an entity's business continuity program can be found on page 14 of the better practice guide.**

## Ongoing management

The cornerstone of effective ongoing management of business continuity in an entity is developing and implementing a robust governance framework. Entities that have done this well have integrated business continuity management into their existing governance framework.

## Business continuity governance checklists

The following checklists will assist entities in identifying governance questions for those responsible for the oversight of a business continuity management program.

## IMPORTANT UPDATE

**Checklist: Governance questions for the executive**

| Governance questions for the executive | Completed Yes/No |
|---|---|
| Have management and staff adopted an attitude to continuity management planning that ensures a positive control environment is maintained? | |
| Does the entity regularly communicate its vision, goals and objectives to staff? | |
| Does management carefully analyse and assessing risks and opportunities before authorising new ventures or significant changes? | |
| Does the business continuity plan complement the entity's corporate governance and risk management framework? | |
| Is the entity responsible for providing a time-critical service to the public or the Government? | |
| If yes, have the implications been considered if the service were unavailable for a period of time? | |
| Does the business impact analysis identify internal and external interdependencies? | |
| Are business continuity practices and procedures in place to ensure timely decision making during a disaster and to assign accountability to designated staff? | |
| Does a business impact analysis exist that identifies the recovery timeframes of the critical business processes? | |
| Does the entity have a person identified who has overall responsibility and accountability for business continuity? | |
| If so, has the person been provided with adequate training and resources to perform the role? | |
| Has the entity's business continuity program been subject to independent review (for example by internal audit)? | |
| Is the business continuity plan(s) linked to the emergency management and incident management plans for the entity? | |
| Is there a process in place for the business continuity plan to be periodically reviewed? | |
| Has the business continuity plan been formally evaluated as part of the entity's overall corporate governance arrangements? | |
| If the entity has undergone changes in focus and direction, or changes to business resources (personnel, facilities, information technology, and communication), has the business continuity plan been amended to reflect these changes? | |
| Are the continuity plans updated on a regular basis (at least annually)? | |
| Are the continuity plans regularly subject to testing and exercises? | |
| Were the results of the tests and exercises reviewed? | |
| Were recommendations for improvement taken up and subject to exercising? | |

## IMPORTANT UPDATE

**Checklist: Governance questions for the committee responsible for overseeing business continuity management**

| Governance questions for the committee responsible for overseeing business continuity management | Completed Yes/No |
|---|---|
| Is the scope of the business continuity process appropriate given the entity's circumstances and risk management strategy? | |
| Is an appropriate governance framework in place and has responsibility been assigned at the correct level of management? | |
| Is the business continuity plan properly coordinated to take into consideration other risk management initiatives? | |
| Are synergies between other risk management initiatives and business continuity fully used? | |
| Have all internal and external audit recommendations regarding business continuity management been followed up? | |
| Are the maximum tolerable period of disruption, recovery time objectives, and recovery point objectives determined as part of the business impact analysis in line with the committee's understanding of the business? | |
| Are recommended recovery strategies appropriate given other business initiatives? | |
| As part of the review of the internal audit strategic and annual work plans is business continuity and more specifically, business continuity exercising and maintenance properly addressed? | |
| Are business continuity initiatives properly communicated to all levels of management and across the entity? | |

**IMPORTANT UPDATE**

## Business continuity management roles and responsibilities

Roles and responsibilities of people involved in business continuity management should be clearly documented.

The following example of a roles and responsibility statement assumes the Recovery Coordinator is also the custodian of the business continuity management plan. It also assumes there is a separate emergency response management team and incident management team.

**Example: Business continuity management roles and responsibilities**

| Role | Managing the business continuity program | In the event of a business disruption |
|---|---|---|
| Committee responsible for overseeing business continuity management | • Ensure governance framework supports business continuity.<br>• Ensure approach to risk management supports strategic goals of the entity.<br>• Provide overall direction and drive for the business continuity program.<br>• Monitor performance and compliance of business continuity program.<br>• Establish milestones and performance reporting requirements.<br>• Authorise new versions of the business continuity plan.<br>• Approve the test and exercise schedule and scenarios.<br>• Approve budget to support business continuity activities.<br>• Provide resources to ensure business continuity management is an ongoing program, integrated with other corporate management processes. | • Review post incident /exercise review reports, and impact of any proposed revisions of the business continuity plan. |

IMPORTANT UPDATE

| Role | Managing the business continuity program | In the event of a business disruption |
|---|---|---|
| Chief Executive Officer | • Sponsor the business continuity program.<br>• Maintain awareness of business continuity management, and receive business continuity management training.<br>• Contribute to business continuity awareness raising in the entity.<br>• Participate in business continuity testing and exercising.<br>• Appropriately resource the business continuity function.<br>• Endorse a business continuity management policy.<br>• Endorse key business continuity documents such as the business impact analysis and business continuity plan. | • Brief Minister and board on the disruption, expected consequences and recovery timeframe.<br>• Provide a focal point for the entity to ensure the public and media receive correct non-contradictory, information.<br>• Ensure staff and stakeholders are made aware of the problems.<br>• Ensure the Recovery Coordinator and Recovery Teams have the resources and support necessary to do their job. |
| Incident Manager | • Contribute to the development and review of the business impact analysis.<br>• Contribute to the development and update of the business continuity plan – particularly for contact details.<br>• Participate in tests and exercises of the business continuity plan.<br>• Receive training on their specific role, as well as good practice in business continuity management generally. | • Decision to declare a business disruption event.<br>• Decision to activate the incident management plan.<br>• Decision to activate the business continuity plan.<br>• Activate the command centre.<br>• Lead and project manage the incident management team.<br>• Determine the recovery strategy for the given situation. |
| Emergency Response Manager | • Contribute to the development and review of the business impact analysis.<br>• Contribute to the development and update of the business continuity plan – particularly for contact details.<br>• Participate in tests and exercises of the business continuity plan.<br>• Receive training on their specific role, as well as good practice in business continuity management generally. | • Assess the extent of damage to building, facilities and equipment<br>• Report to the Incident Manager (and Chief Executive Officer and/or board if necessary).<br>• Decision to activate the emergency response management plan.<br>• Lead and project manage the emergency response management team. |

| Role | Managing the business continuity program | In the event of a business disruption |
|---|---|---|
| Recovery Coordinator / Business Continuity Custodian. | • Day-to-day implementation and coordination of business continuity management tasks.<br>• Contribute to the development and review of the business impact analysis.<br>• Prepare and update the business continuity plan.<br>• Maintain the business continuity kit.<br>• Schedule and conduct tests and exercises of the business continuity plan.<br>• Promote an awareness of business continuity management, and schedule business continuity management training.<br>• Receive training on their specific role, as well as good practice in business continuity management generally.<br>• Update the business continuity plan for lessons learned from all disruption events. | • Decision to declare a business disruption event.<br>• Lead and project manage the recovery team.<br>• Assess the extent of damage to building, facilities and equipment and report to the Incident Manager (and Chief Executive Officer and/or board if necessary).<br>• Contact necessary staff required for the recovery.<br>• Assist in establishing the recovery site, if applicable.<br>• Direct, coordinate and monitor all recovery operations.<br>• Convene recovery status meetings with the executive.<br>• Schedule subsequent recovery status meetings.<br>• Liaise with real estate agent, if applicable.<br>• Contact insurance assessors to determine their requirements and coordinate their on-going liaison with all recovery teams.<br>• Minimise further losses and salvage recoverable resources.<br>• Provide assurance and information updates to staff not involved in the recovery effort.<br>• Prepare the recovery site.<br>• Coordinate the post incident review. |

IMPORTANT UPDATE

| Role | Managing the business continuity program | In the event of a business disruption |
|---|---|---|
| Support area and business unit recovery teams | • Contribute to the business impact analysis.<br>• Contribute to the development and update of the business continuity plan – particularly for contact details.<br>• Prepare the recovery plan for their support area or business unit.<br>• Participate in tests and exercises of the business continuity plan.<br>• Maintain an awareness of business continuity management, and participate in business continuity management training. | • Contact the staff required for the recovery team.<br>• Convene status meeting with team members.<br>• Assist with disaster assessment as required.<br>• Continually assess and address the entity's needs (for the support area or business units' area of expertise).<br>• Determine requirements and coordinate acquisition of equipment, furniture, stationery and communications resources necessary for recovery.<br>• Provide regular updates to the Recovery Coordinator.<br>• Liaise with other recovery teams. |

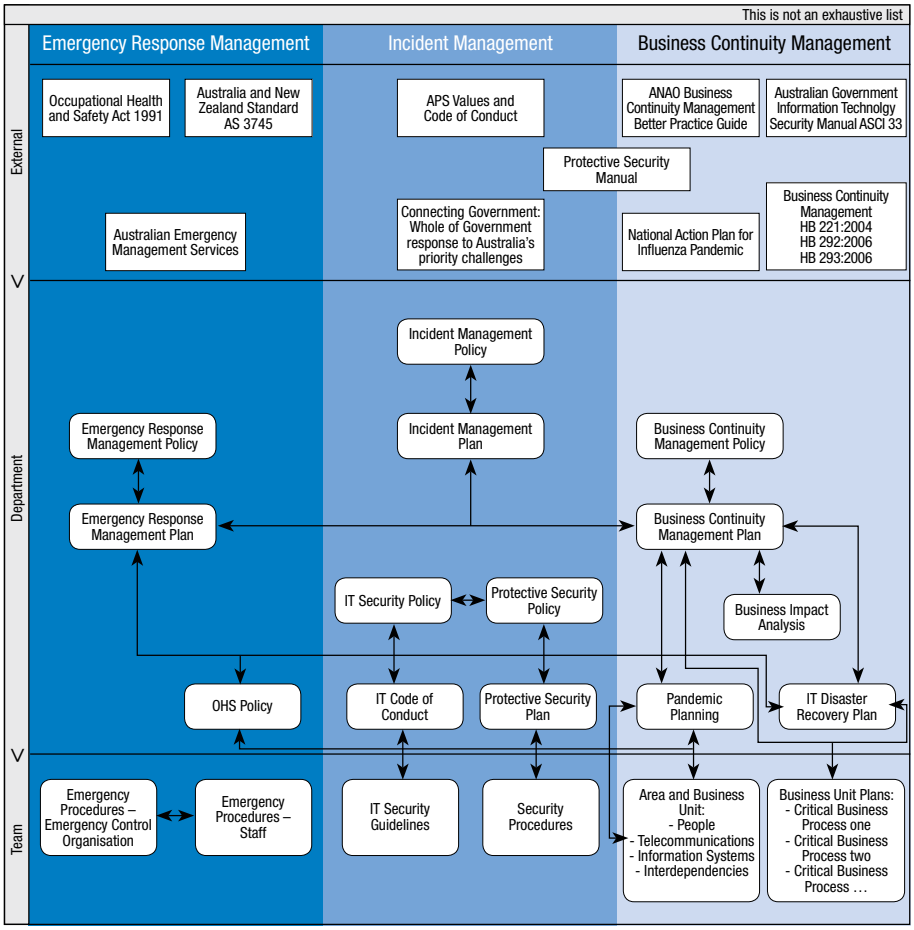
IMPORTANT UPDATE

**IMPORTANT UPDATE**

## Example business continuity framework

The following is an example of how a business continuity framework could be established, and represented in a diagram.

**Example: Business continuity framework**



**IMPORTANT UPDATE**

# Embedding business continuity management into the entity's culture

**Explanatory material on executive sponsorship, as well as a case study on embedding business continuity management into an entity's culture can be found on page 17 and 18 of the better practice guide.**

Throughout the business continuity management process there are opportunities to embed business continuity management into the entity's culture, to ensure it becomes part of the entity's core values and business-as-usual management.

## Executive sponsorship

One way the executive can promote business continuity within the entity is through an endorsed business continuity management policy. This policy sets out the entity's agreed priorities, the business continuity management framework, and responsibilities for the program. **The policy needs to be appropriate to the entity's scale, complexity, and the nature of its operations.**

**IMPORTANT UPDATE**

## Business continuity management policy

The following is an example table of contents for a business continuity management policy document.

**Example: Table of contents for a business continuity management policy document**

| Section | Contents of a business continuity management policy |
|---|---|
| Introduction | • Background.<br>• Objective.<br>• Scope.<br>• Policy Ownership. |
| Business continuity management policy | • Statement of Entity Policy.<br>• Listing of Entity-Level Critical Business Processes, Assets and Sites.<br>• Business Continuity Priorities. |
| Business continuity management framework | • Governance Structure.<br>• Standards, Regulations, and Policies (to be adhered to, or benchmarked against).<br>• Roles and Responsibilities.<br>• Key Internal and External Interdependencies.<br>• Risk Evaluation and Business Impact Analysis.<br>• Annual Review and Maintenance of Business Continuity Management Documentation.<br>• Awareness and Training.<br>• Independent Review. |

## IMPORTANT UPDATE

The following are example statements of business continuity management policy.

**Example 1: Statement of business continuity management policy**

### Business continuity management policy

<Entity name>is required to identify, evaluate, mitigate, monitor and report business continuity risks to ensure it is able to continue operations in the event of a material business disruption and to continue to meet financial and service obligations to stakeholders.

Direct responsibility and final accountability for business continuity management rests with the management and requires that:

- appropriate plans be implemented to ensure the continuity of critical activities;
- plans address internal and external dependencies;
- plans are tested on a regular basis;
- staff are trained in the operation of the plans; and
- an appropriate governance structure that ensures the long-term adequacy of business continuity plans is implemented.

**Example 2: Statement of business continuity management policy**

### Business continuity management policy

The objective of <entity name> business continuity management is to maintain the continuity of identified business critical processes in order to minimise the impact on major stakeholders.

The critical business processes that are supported by <entity's> business continuity management are, in priority order:

- <critical business process priority 1>;
- <critical business process priority 2>; and
- <critical business process priority ….>.

The <entity's> broader business continuity objectives are to:

- protect human life;
- minimise business disruptions;
- ensure a timely resumption of operations following a business disruption event;
- protect <entity> from legal ramifications and law suits; and
- preserve stakeholder confidence, entity credibility and goodwill.

**IMPORTANT UPDATE**

## Training and raising awareness

Training and raising awareness activities are important components of managing a business continuity program. Such activities assist in providing an understanding of, as well as developing skills and competencies in, business continuity management.

The following is an example program for business continuity training and raising awareness.

**Example: Program for business continuity training and raising awareness**

| Audience | Program for business continuity training and raising awareness subjects |
|---|---|
| Executive / board | Business continuity program management.<br>Business continuity standards, guidelines and legislation.<br>Incident management.<br>Key features of the entity's business continuity management program. |
| Business continuity custodians | Business continuity program management.<br>Business continuity standards, guidelines and legislation.<br>Conducting a business impact analysis.<br>Developing and maintaining a business continuity plan.<br>Running tests and exercises.<br>Key features of the entity's business continuity management program. |
| Staff with a business continuity role | Skills necessary to undertake their business continuity role. For example:<br>• communications training;<br>• managing teams;<br>• operating in stressful situations; and<br>• negotiation skills.<br>Key features of the entity's business continuity management program. |
| Staff | Introduction to business continuity management.<br>Key features of the entity's business continuity management program. |
| Stakeholders | Key features of the entity's business continuity management program. |
| Interdependent entities | Key features of the entity's business continuity management program. |

**Explanatory material about training and raising awareness, business continuity training references, and a case study on business continuity awareness can be found on pages 19-21 of the better practice guide.**

**IMPORTANT UPDATE**

# Analysing the entity and its context

The following tasks are targeted at the development of a whole-of-entity business impact analysis. They may be customised to assist with the completion of business unit/service area business impact analysis. Also, the way in which the tasks and templates are completed will depend on the size and complexity of the entity, and the nature of the functions performed by the entity. For example, a large entity may use a questionnaire accompanied by interviews and workshops, while a smaller, non-complex entity (or a single business unit or support area) may conduct a brainstorming workshop with key personnel. Regardless of the approach, it is important to document the results, and obtain executive endorsement.

**Explanatory material about identifying critical business processes, as well as case studies can be found on page 23 of the better practice guide.**

## Identify critical business processes

It is important in preparation for the business impact analysis to have a clear and agreed understanding of the entity's business objectives, and the critical business processes which ensure these objectives are met.

## IMPORTANT UPDATE

The following checklist may assist entities to identify critical business processes.

**Checklist: Identify critical business processes**

| Identify critical business processes tasks | Completed Yes/No |
|---|---|
| Document and confirm entity objectives and performance criteria. | |
| List all critical business processes which underpin achievement of objectives. | |
| Rank the processes in order of importance to the entity's objectives and exclude those processes not considered critical to achieving the objectives. | |
| Review the functional organisation chart to identify general areas of operational responsibility. | |
| Obtain any supporting documentation that is available which would provide a summary of critical business processes. | |
| Interview managers responsible for critical business processes to confirm understanding. | |
| Consider process interdependencies that exist:<br>• between internal areas; and<br>• with external entities or organisations. | |
| Determine the minimum requirements necessary to perform each critical process. Consider:<br>• activities;<br>• resources;<br>o people;<br>o facilities (including building and equipment);<br>o technology (including IT systems/applications);<br>o telecommunications;<br>o vital records;<br>• interdependencies; and<br>• other. | |
| Obtain executive endorsement of the prioritised list of critical business processes. | |

**IMPORTANT UPDATE**

The following template may assist entities in identifying their critical business processes.

Note: An 'Identify critical business processes' template should be completed for each of the entity's business units and service areas. In mature, large, complex or geographically dispersed a template should also be completed for the entity as a whole. This moderating process will prioritise the critical business processes at the entity level, and identify commonalities and interdependencies across business units and service areas.

A 'Business impact analysis' template (such as the template on page 110 of this workbook) should then be completed for each of the critical business processes identified.

**Template: Identify critical business processes**

## Document control

| Identify critical business processes document details | |
|---|---|
| Version number | |
| Authorisation date | |
| Authorised by | |
| Expiry date | |
| To be revised on | |

## Entity/business unit/service area details

| Entity/business unit/services area details | |
|---|---|
| Entity/business unit/service area name | |
| Contact name | |
| Title | |
| Phone number | |
| Location | |
| Email | |

## Entity/business unit/service area objectives and performance indicators

| Objectives (in priority order) | Performance indicators |
|---|---|
| | |
| | |

**IMPORTANT UPDATE**

## Entity/business unit/service area critical business processes

| Critical business processes (in priority order) | Section/Team Key contact |
|---|---|
| | |
| | |

## Requirements necessary to perform each critical process

| Critical Business Process 1: <insert process name> | |
|---|---|
| Activities | |
| Resources | |
| • People | |
| • Facilities (including buildings and equipment) | |
| • Technology (including IT systems/ applications) | |
| • Telecommunications | |
| • Vital records (including paper and electronic). | |
| Interdependent processes (including internal and external) | |
| Other | |

| Critical Business Process 2: <insert process name> | |
|---|---|
| Activities | |
| Resources | |
| • People | |
| • Facilities (including buildings and equipment) | |
| • Technology (including IT systems/ applications) | |
| • Telecommunications | |
| • Vital records (including paper and electronic). | |
| Interdependent processes (including internal and external) | |
| Other | |

*<Repeat the* 'Requirements necessary to perform each critical process' *table for each critical process>*

**IMPORTANT UPDATE**

**Explanatory material about undertaking a business impact analysis can be found on page 30 of the better practice guide.**

## Undertake a business impact analysis

A business impact analysis determines and documents the impact of a business disruption event to each critical business process. It considers disruptions to the activities and resources that support critical business processes.

The following checklist may assist entities in undertaking a business impact analysis.

**Checklist: Undertaking a business impact analysis**

| Undertaking a business impact analysis tasks | Completed Yes/No |
|---|---|
| Gather relevant existing information, such as:<br>• disruption scenarios;<br>• emergency response management plan;<br>• incident management plan;<br>• pandemic plan; and<br>• IT disaster recovery plan. | |
| Consult key personnel and business units. Consider:<br>• internal audit;<br>• business areas;<br>• emergency response management;<br>• finance (and insurance);<br>• external entities and organisations (for example, service providers, interdependencies, and unions).<br>• Information technology;<br>• risk management;<br>• building and facilities;<br>• occupational health and safety; and | |
| Evaluate the impacts of a loss of each critical process from the perspective of the entity's objectives. Consider:<br>• financial;<br>• reputation;<br>• regulatory;<br>• health and safety;<br>• third party relationships and interdependencies; and<br>• other categories (determined by the entity).<br>• customer service;<br>• legal/contractual;<br>• work backlog;<br>• environmental; | |
| Identify interim processing procedures (alternative or manual processing) techniques to be adopted during the recovery phase. | |
| Determine the maximum tolerable period of disruption for each critical process. | |
| Determine internal and external critical interdependencies. | |
| Identify vital records. | |
| Determine the recovery time objective for each critical business process and IT system/application. | |
| Determine the recovery point objective electronic data. | |
| Estimate the time to overcome the backlog of work accumulated during a business disruption event. | |
| Obtain executive endorsement of the business impact analysis. | |

**IMPORTANT UPDATE**

## Business impact analysis template notes

The entity's critical business processes and the requirements necessary to undertake each critical business process (as identified using a templates such as the template on page 106 of this workbook) are required for the business impact analysis.

For mature, large, complex or geographically dispersed entities the business impact analysis should be completed following consideration of the whole-of-entity view. This moderating process will prioritise the critical business processes at the entity level, and identify commonalities and interdependencies across business units and service areas.

An objective and consistent basis on which to assess the impact of a business disruption event needs to be established. This will help ensure business units and support areas consider the same factors when determining their maximum tolerable period of disruption.[2]

The level of impact can be assessed using a scale, such as the one presented in the table below.

| Impact | Assessment | Score |
|---|---|---|
| Extreme | Threatens achievement of objectives. | 5 |
| Major | Significant impact on business drivers. | 4 |
| Moderate | Impact on short term business operations. | 3 |
| Minor | Inconvenient, but no real ongoing business impact. | 2 |
| Nil | Reconsider the inclusion of this as a critical response. | 1 |

The maximum tolerable period of disruption should be determined for the critical activities and resources. That is, how long can the critical business process survive without the critical activity and/or resource before it will substantially impact on the achievement of objectives.

The maximum tolerable period of disruption is set at or above the point where there would be a significant impact on business drivers (Score 4). In effect, the entity can do without the business process for any time under that point, as it will not prevent the entity from achieving its objectives.

The maximum tolerable period of disruption may be expressed in terms of hours, days or weeks depending on the process being assessed. For example:

– <6 hours
– 12 hours
– 1 day
– 2-3 days
– 5 days
– > 5 days

The impact of a sustained disruption due to a pandemic should also be considered.

The recovery time objective may be expressed using the terms above.[3] The recovery point objective may be expressed slightly differently, using terms such as point of failure, intra-day, start of day, start of week, or start of month.[4]

The following template may assist entities undertake a business impact analysis.

Note: A business impact analysis is completed for each critical business process.

[2] The maximum period of time that an entity can tolerate the disruption of a critical business process, before the achievement of objectives is adversely affected.

[3] The recovery time objective is the target time set for recovery of an activity, product, service, or critical business process after a business disruption event, or recovery of an IT system or application after a business disruption event.

[4] The recovery point objective is the point in time (before the business disruption) to which electronic data must be recovered after a business disruption event. For example, data must be recovered to the end of the previous day's processing.

**IMPORTANT UPDATE**

**Template: Business impact analysis**

## Document control

| Business impact analysis document details | |
|---|---|
| Version number | |
| Authorisation date | |
| Authorised by | |
| Expiry date | |
| To be revised on | |

## Entity/business unit/service area details

| Entity/business unit/services area details | |
|---|---|
| Entity/business unit/service area | |
| Contact name | |
| Title | |
| Phone number | |
| Location | |
| Email | |

## Critical business process <insert process name>- details

| Critical Business Process: <insert process name> | |
|---|---|
| Process description | |
| Process frequency | |
| Critical periods | |
| Key contacts | |
| Maximum tolerable period of disruption | |
| Manual workarounds description | |

## Critical business processes <insert process name>- assumptions

| Assumptions | |
|---|---|
| | |
| | |

## Critical business process <insert process name>– impact analysis

| Impact type | <6 hrs | 12 hrs | 1 day | 2-3 days | 5 days | > 5 days | Sustained period (Pandemic) | Comments |
|---|---|---|---|---|---|---|---|---|
| Financial | | | | | | | | |
| Reputation | | | | | | | | |
| Customer Service<br>• Internal; and<br>• External. | | | | | | | | |
| Legal/contractual | | | | | | | | |
| Regulatory | | | | | | | | |
| Work Backlog | | | | | | | | |
| Health & Safety | | | | | | | | |
| Environmental | | | | | | | | |
| Third party relationships and interdependencies | | | | | | | | |
| Other<br>• stakeholder confidence and goodwill;<br>• employee morale and wellbeing;<br>• management control and capability; and<br>• other. | | | | | | | | |

IMPORTANT UPDATE

IMPORTANT UPDATE

## Critical business process <insert process name>– people analysis

| Role | Description of capability / skill set | Numbers |
|---|---|---|
| | | |
| | | |

## Critical business process <insert process name> – facilities (including buildings and equipment) analysis

| Facilities/sites used | Description of usage | Numbers |
|---|---|---|
| | | |
| | | |

## Critical business process <insert process name> – technology (including IT systems/applications) analysis

| IT systems/applications used | Description of usage | Recovery Point Objective | Recovery Time Objective |
|---|---|---|---|
| | | | |
| | | | |

IMPORTANT UPDATE

## Critical business process <insert process name> – telecommunications analysis

| Telecommunications used | Description of usage | Recovery Time Objective |
|---|---|---|
| | | |
| | | |

## Critical business process <insert process name> – vital records analysis

| Electronic and paper vital records | Description of usage | Primary Location | Secondary Location |
|---|---|---|---|
| | | | |
| | | | |

## Critical business process <insert process name> –interdependency analysis

| Internal and external interdependent processes | Name of client, business partner, vendor or service provider etc | Key contacts including out of hours contact details | Alternative supplier details |
|---|---|---|---|
| | | | |
| | | | |

*<Repeat business impact analysis template for each critical business process>*

**IMPORTANT UPDATE**

## Disruption Scenarios

When an entity undertakes a risk management process it is important to identify those events, which if they were to occur, might affect the entity achieving its objectives. Often scenario analysis is used as part of risk identification.

These scenarios may be based on the previous experiences of the entity or of similar entities. While it is noted that business continuity management is concerned with taking action after the event (for example it assumes that a business disruption event has occurred and it is not primarily aimed at preventing the disruption), it is still beneficial to the entity to consider some generic scenarios that may occur as these may require specific continuity preparations and responses.

**Explanatory material about disruption scenarios can be found on page 33 of the better practice guide.**

Realistic disruption scenarios may include frequently occurring events such as IT system failure, electrical supply failure, industrial action, transport system failures and bad weather.

The following template may assist entities when determining business disruption scenarios. A rating scale can be used to complete the template.

**Template: Disruption scenarios**

| Scenario | Likelihood | Consequence | Impact |
|---|---|---|---|
| Natural hazards. For example:<br>• Fire;<br>• Flood; and<br>• Pandemic. | | | |
| Generic scenarios. For example:<br>• Loss of building;<br>• Loss of people;<br>• Loss of IT systems;<br>• Loss of telecommunications; and<br>• Loss of water, electricity, gas, sewage. | | | |
| Other hazards:<br>• <list possible hazards> | | | |

**IMPORTANT UPDATE**

# Designing the entity's business continuity approach

The entity's business continuity approach should minimise the effects of disruptions to each critical business process for which a maximum tolerable period of disruption and recovery time objective has been established.

## Identifying and evaluating options to minimise the effects of a business disruption

Evaluating options available to continue critical business processes in the face of a business disruption requires entities to consider the alternative activities and resources to be used.

The following checklist may assist entities to select alternative activities and resources.

**Explanatory material about identifying and evaluating options to minimise the effects of a business disruption event, as well as case studies on human resources and facilities considerations can be found on page 35 of the better practice guide.**

## IMPORTANT UPDATE

**Checklist: Selecting activity and resource alternatives, where services are provided by an external supplier**

| Considerations for selecting activity and resource alternatives | Considered Yes/No |
|---|---|
| In selecting alternative activities and/or resources, the following areas are addressed:<br>• people;<br>• facilities (including building and equipment);<br>• technology (including IT systems/applications);<br>• telecommunications;<br>• vital records;<br>• interdependencies; and<br>• other. | |
| Document a brief description of each option to minimise the effects of a business disruption event (example treatment options are provided in the better practice guide). | |
| Determine other resources required and the costs for each option (this may require information from vendors). | |
| Compare recovery options, including cost, in light of recovery priorities and the maximum tolerable period of disruption. Consider:<br>• does the option meet recovery needs?<br>• does the option exceed our needs? | |

## IMPORTANT UPDATE

The following checklist may assist entities when considering alternative processing, where services are provided by an external supplier.

**Checklist: Considerations for alternative processing, where services are provided by an external supplier**

| Considerations for alternative processing, where services are provided by an external supplier | Considered Yes/No |
|---|---|
| The characteristics of the alternative processing facilities indicate adequate physical security and appropriate environmental controls. | |
| The risk profile of the alternative vendor site is different to that of the entity's own site so that both locations are unlikely to be affected by the same disruption. For example, there is sufficient distance from the entity's primary site, different power grid and different flood plain exposure. | |
| Contracts clearly specify the availability of alternative vendor sites and the rights of individual subscribers in the event of multiple disaster declarations. | |
| Amount and nature of support services the vendor will provide is defined relative to:<br>• implementation assistance;<br>• support for testing;<br>• logistical support; and<br>• after hours support. | |
| The vendor has limits concerning the total number of clients for any given facility. | |
| The vendor cannot renew (except by automatic renewal clause) or renegotiate the contract while the subscriber is experiencing a disaster or in recovery phase. | |
| The amount and scheduling of test time is defined. | |
| The entity can periodically audit the installation to ensure that the specified configuration is maintained. | |
| An escape clause allow the entity to terminate the contract without penalty for any of the following reasons:<br>• failure to maintain technical compatibility;<br>• failure to provide agreed support services;<br>• failure to maintain suitable environmental support;<br>• change to subscriber limits;<br>• change of location for the provided services; and<br>• any breach of contract. | |
| Fees should not be subject to change without the written consent of the subscriber. | |
| The contract should not be assignable without written consent. | |
| The vendor should be subject to appropriate non-disclosure conditions. | |

## IMPORTANT UPDATE

The following checklist may assist entities in backup processing and off-site storage considerations.

**Checklist: Backup processing and off-site storage, where services are provided by an external supplier**

| Considerations for backup processing and off site storage, where services are provided by an external supplier | Considered Yes/No |
|---|---|
| Ensure all resources required for the selected strategies are stored off-site. | |
| Review documented off-site backup processing standards and procedures, if they exist. If standards and procedures do not exist, ensure they are developed. | |
| Interview personnel responsible for implementation of backup procedures to see if procedures are being adhered to. | |
| Document critical elements of the off-site backup procedures for inclusion in the appropriate sections of the contingency plan. | |
| Analyse off-site backup processing procedures and document concerns. | |
| Schedule review of off-site storage facility. | |
| Partial recovery from off-site facilities has been tested. | |

The following checklist may assist entities manage IT disaster recovery.

**Checklist: IT disaster recovery, where services are provided by an external supplier**

| Considerations for IT disaster recovery, where services are provided by an external supplier | Considered Yes/No |
|---|---|
| Definition of the backup capability of the vendor site is clear and consistent throughout the contract. | |
| Occupation of the hot site for a minimum of {entity to determine number of weeks}. | |
| Conditions under which the subscriber can continue to occupy hot site facilities after the number of weeks determined is defined. | |
| The number and description/type of locally attached terminals and/or other devices available while on-site is defined (this is important for data entry requirements). | |
| Continuing technical compatibility is assured throughout the life of the contract. | |
| The contract specifies a guarantee of access to the hot site (including after hours access) during period of disaster and recovery. | |

## IMPORTANT UPDATE

| Considerations for IT disaster recovery, where services are provided by an external supplier | Considered Yes/No |
|---|---|
| The nature and extent of IT support services to be provided by the vendor has been defined relative to:<br>• network diagnostic capabilities and implementation assistance;<br>• support for testing activities;<br>• assistance in configuring facilities (for example equipment acquisition, transportation, storage, removal and return);<br>• access to and use of vendor software, documentation, ancillary facilities (for example photocopying, and food services), and<br>• logistical support. | |
| Realism of assumptions by business areas regarding the availability of appropriately skilled IT personnel, and sourcing of specialist equipment in the event of a business disruption. | |

The following template is a worksheet for evaluation of recovery treatment options.

**Template: Evaluation of recovery treatment options**

| Options | Implementation time | Within MTPD | | Full cost (list components) | Cost effective | |
|---|---|---|---|---|---|---|
| | | Yes | No | | Yes | No |
| Initial response | | | | | | |
| Interim processing | | | | | | |
| Restoration | | | | | | |
| Other issues | | | | | | |

Note: MTPD is the maximum tolerable period of disruption.

**IMPORTANT UPDATE**

## Business continuity management limitations

It will assist entities to recognise and document the factors that may limit recovery from a business disruption event, to bring them to the attention of management. The following is an example of limiting factors.

**Example: Factors which may limit recovery from a business disruption**

| Resource | Factors which may limit recovery from a business disruption |
|---|---|
| People | • There is an insufficient number of personnel possessing the appropriate skills available to implement business continuity operations.<br>• An insufficient number of qualified personnel are available to perform user tasks during the recovery phase.<br>• Personnel who play a role in recovery are unaware of their responsibilities and may not have been adequately trained to perform the recovery tasks.<br>• Staff support areas are not be prepared to support the recovery operation.<br>• No alternative contacts have been identified.<br>• Periodic testing and exercising of the business continuity plan is not conducted resulting in lack of staff knowledge/understanding when necessary. |
| Facilities (including buildings and equipment) | • The Recovery Plan will NOT cover any event which simultaneously renders both the primary and all alternative data centre facilities inoperable.<br>• The Recovery Plan will NOT cover any event which simultaneously renders the data centre inoperable and the essential off-site storage inaccessible.<br>• A disaster that renders the data centre inoperable affects large geographic areas, public utilities, the transportation infrastructure or other facilities and/or services ordinarily available (Note that this excludes an electrical distribution failure).<br>• Transactions lost between the point of the most recent backup and the disaster event cannot be reconstructed and re-entered to computer systems within the maximum acceptable outage (or maximum tolerable period of disruption) period.<br>• Periodic testing and exercising of the business continuity plan is not conducted.<br>• Critical systems are not periodically evaluated and their minimum essential features can not be provided for in a disaster.<br>• A complete listing of production files and their location on backup tapes is not rotated off-site with adequate frequency.<br>• The entity experiences voluntary or involuntary separations of employment or relationships with any employees, suppliers, or other vendors between the occurrence of the disaster event and complete recovery.<br>• Off-site storage locations are not intact and accessible.<br>• Off-site information backup and rotation procedures are inadequate to implement full recovery within maximum acceptable outage (or maximum tolerable period of disruption) time frames.<br>• Daily transactions needed to reconstruct critical data are not rotated off-site with adequate frequency. |

## IMPORTANT UPDATE

| Resource | Factors which may limit recovery from a business disruption |
|---|---|
| Technology (including IT systems/ applications) | • Lack of alternative processing facilities available as and when required.<br>• Critical operations and systems documentation for each platform are not stored off-site.<br>• The organisation lacks access to a fully configured second processing site sufficient in capacity to support data processing for critical business processes with critical application support needs.<br>• Critical users do not have the ability to reconstruct any lost work in-progress.<br>• Critical users do not have recovery plans developed to be able to process at the alternative processing facility.<br>• Lack of capacity to adequately implement a possible solution, such as remote access.<br>• Periodic testing and exercising of the business continuity plan is not conducted.<br>• Replacement equipment is not readily available.<br>• Appropriately skilled IT personnel, or specialist equipment are not available. |
| Telecommunications | • Ready access to public network following a disruption is not available.<br>• Delayed access to replacement mobile phones.<br>• Delays in re-routing critical phone numbers to new location.<br>• Lack of access to communications hardware (for example pager, fax, email).<br>• Periodic testing and exercising of the business continuity plan is not conducted. |
| Vital records | • Vital records are stored in a single location.<br>• Electronic data replies on IT systems/applications – see limiting factors above.<br>• Periodic testing and exercising of the business continuity plan is not conducted. |
| Interdependencies | • Contact details for interdependent entities are not regularly maintained.<br>• Testing and exercising does not involve interdependent entities.<br>• Periodic testing and exercising of the business continuity plan is not conducted. |
| Business continuity management capability | • The entity has inadequate financial resources to implement the business continuity plan according to the time frames established by the business impact analysis.<br>• There is inadequate maintenance of business continuity procedures.<br>• No ongoing effort to minimise exposures to disasters will continue and operations/ systems vulnerabilities.<br>• Designated user representatives are not promptly notified if a business disruption occurs.<br>• Periodic testing and exercising of the business continuity plan is not conducted. |

**IMPORTANT UPDATE**

# Building entity resilience

Resilient entities implement preparatory and reactive procedures to minimise business disruptions and support recovery.

**Explanatory material about implementing preparatory controls can be found on page 43 of the better practice guide.**

## Implementing preparatory controls

Preparing for a business disruption event involves establishing controls that will mitigate the consequences of the disruption to a level acceptable to the entity.

The following checklist may assist entities in ensuring business continuity strategies are implemented.

**Checklist: Ensuring strategies are implemented**

| Considerations | Considered Yes/No |
|---|---|
| For each strategy selected, the likely costs are the most commercially viable and represent value for money (that is, investigate other vendors in the marketplace). | |
| The requirement of a potential alternative vendor to gain an understanding of the operating environment within the entity. | |
| Other requirements or changes that need to be made in order for the strategies to be effective. | |
| Changes to off-site storage procedures should be made as they are identified. | |
| Contracts demonstrate better practice for contract management, as well as comply with internal guidelines for contract management. | |
| Contracts are finalised. | |

**IMPORTANT UPDATE**

## Preparing the business continuity plan(s)

Better practice business continuity plans are concise, easy to follow documents. The business continuity plan identifies action-oriented procedures to be undertaken during an outage.

The following is an example table of contents for a business continuity plan.

**Example: Table of contents for a business continuity plan**

| Section | Information contained |
|---|---|
| Cover page | Title and version.<br>Concise statement of objective of plan.<br>Executive endorsement |
| Table of contents | Contents of document. |
| Activation | Steps to be taken immediately after an incident occurs (emergency response management).<br>Escalation process flow.<br>Incident management activation.<br>Criteria for business continuity plan activation. |
| Roles and responsibilities | Recovery organisation chart.<br>Roles and responsibilities of teams. |
| Recovery plan | Team assembly arrangements.<br>Recovery steps (action-oriented procedures, tasks and action lists). |
| Resource requirements | People.<br>Facilities (including buildings and equipment).<br>Technology (including IT systems/applications).<br>Telecommunications.<br>Vital records.<br>Interdependent entities.<br>Other (for example cross reference other plans and their locations). |
| Communication | Communication protocol.<br>Sample communications (for example team activation message, press release, and staff broadcasts). |
| Event log | Event log template. |
| Contact lists | Emergency services contact list (for example plumber, glazier, carpet cleaners, and alternative processing sites).<br>Internal team contact list.<br>Dependent organisations contact list.<br>External/stakeholder contact lists.<br>Staff contact lists. |

**Explanatory material about preparing the business continuity plan, as well as a case study about contacting business continuity and other staff during a business disruption event can be found on page 48 of the better practice guide.**

## IMPORTANT UPDATE

The following is an example table of contents for a separate pandemic plan, or for a pandemic section within a business continuity plan.

**Example: Table of contents for a pandemic plan**

| Section | Contents |
|---|---|
| Preliminaries | Background, scope, roles and responsibilities, relationship to other plans, document control etc. |
| Pre-pandemic preparation | Details of activities to be undertaken in preparation for a pandemic. |
| Pandemic response | Details of activities to be undertaken during ALERT phase. |
| | Details of activities to be undertaken during DELAY phase. |
| | Details of activities to be undertaken during CONTAIN phase. |
| | Details of activities to be undertaken during SUSTAIN phase. |
| | Details of activities to be undertaken during CONTROL phase. |
| Recovery | Details of activities to be undertaken after the pandemic. |
| Appendices | Contact details, checklists etc. |

## IMPORTANT UPDATE

The following is an example wallet book/contact list for business continuity staff. This contact list would be printed to business card size (it may fold out). It may also include the activation diagram or written escalation procedures on the reverse.

**Example: Wallet book/contact list**

| Role | Name | Contact Details | Alternates' Name and Contact Details |
|---|---|---|---|
| Emergency response manager | | | |
| Incident manager | | | |
| Business continuity manager | | | |
| Business continuity support staff | | | |
| • | | | |
| • | | | |
| IT disaster recovery manager | | | |
| General update Info line | | | |
| BCM command centre primary (onsite) address:<br>BCM command centre alternative (offsite) address: | | | |

Note: Entities may choose not to include names for security reasons.

Entities must comply with privacy requirements, such as obtaining consent from individuals to use personal contact details.

Entities may create contact lists specific to each team. Some teams may include contact details of externals, for which the entity has interdependencies, or which will be relied on in an emergency or business continuity disruption event.

## IMPORTANT UPDATE

The following are examples of pre-prepared communications.

**Example: Pre-prepared communications**

### Recorded telephone message for staff

This is a recorded message from <entity> business continuity management team. A <situation> occurred at the premises of <entity name, entity location>. The <emergency service> attended the <situation>.The <entity>has activated its business continuity plan. At this stage, staff are requested to <remain at home/return to work>. This message will be updated at <time, date>.

### Print media advertisement for staff

<entity logo>

ATTENTION <insert entity name>

A staff meeting has been organised to discuss the recent events. All personnel are directed to attend, the details are as follows:

Date: <insert date>

Time: <insert time>

Venue: <insert venue>

Staff are requested to bring their ID / building passes for identification.

If you are unable to attend please contact <insert name and number>.

### Press release

<time> <date>

A <situation> occurred at the premises of <entity name, entity location>.

There <were/were not> staff injuries. Staff <were/were not> taken to hospital.

The <emergency service> attended the <situation>.

The <entity>has activated its business continuity plan. Critical business functions will continue with limited interruption.

A media briefing shall be conducted at the site <time, date>.

An <entity> representative will provide more information and answer questions.

Media enquiries: <insert name and number>.

**IMPORTANT UPDATE**

# In the event of a disruption: Activating and deploying the plan

This section provides examples, templates and checklists which may be used during a business disruption event.

## Declaring a business disruption event

Declaring the outage and agreeing on the appropriate time to initiate operations under the business continuity plan can be difficult and requires advance planning. It is therefore important to give clear guidelines on the declaration of a business disruption (business continuity event).

The following provides an example of activation levels during a business disruption event.

**Example: Activation levels**

| Level | Description |
|---|---|
| Critical | Incident management team and/or the business continuity management team convene (in person or via teleconference) to manage the situation. |
| Major | Response and/or recovery situation monitored by emergency response manager or delegate, with the incident management team and/or the business continuity management team alerted and on standby.<br>Hourly situation reports are provided to the incident management team and/or the business continuity management team. |
| Minor | Response and/or recovery situation monitored by administrative support staff, with the incident management team and/or the business continuity management team alerted and on standby.<br>Daily situation reports are provided to the incident management team and/or the business continuity management team. |

Note: Activation of any critical business process or support area recovery action plan will be under the direction of the incident manager and/or the business continuity manager to ensure resources are allocated in accordance with entity-wide priorities.

**Explanatory material about declaring a business disruption event, as well as case studies about implementing the business continuity plan for the whole entity can be found on page 54 of the better practice guide.**

## IMPORTANT UPDATE

The following checklist may assist entities in considering issues when estimating the duration of a business disruption event.

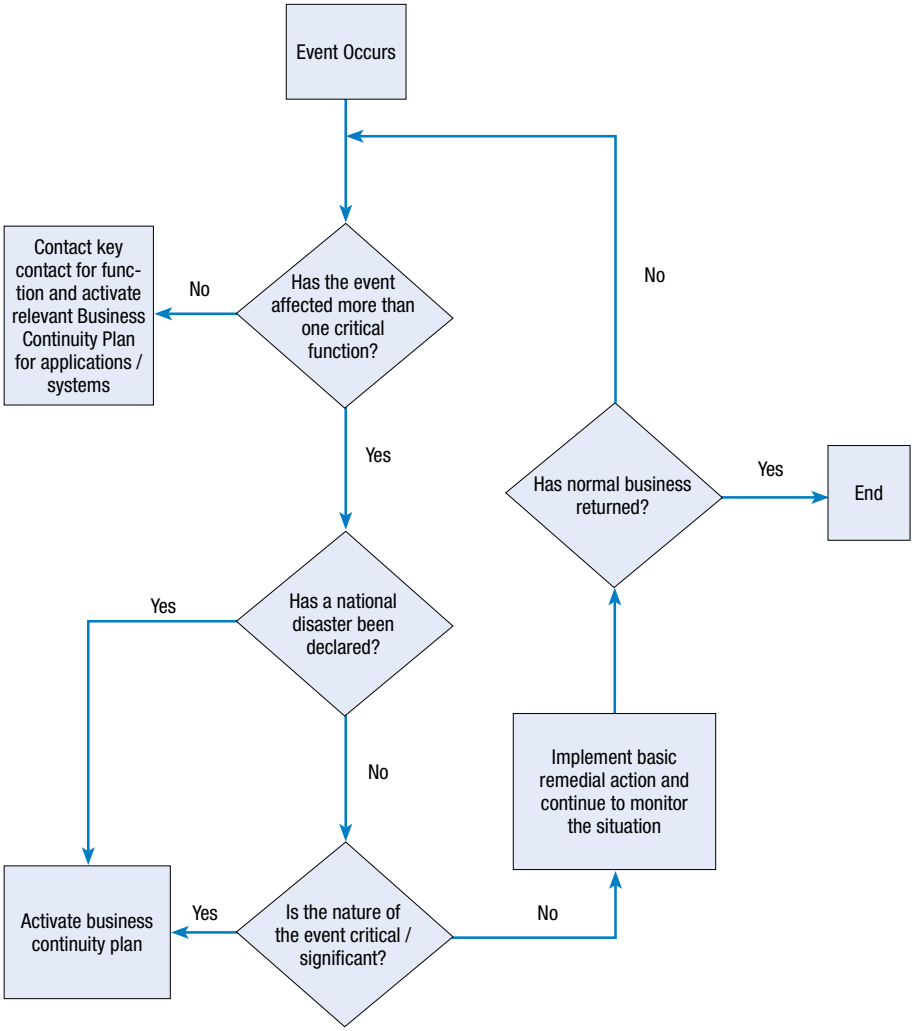
**Checklist: Considerations for estimating the duration of a business disruption event**

| Considerations for estimating the duration of a business disruption event | Completed Yes/No |
|---|---|
| Has input from emergency services, contractors been gathered to use in the evaluation of likely repair time? | |
| Are critical business processes affected? | |
| If so, have the impacts on the critical business processes been considered? | |
| Are the people involved in the estimation process clearly identified? | |
| Are notification procedures for those involved in the estimation process clearly identified? | |
| Are timeframes for the assessment clearly identified? | |
| Are safety procedures for assessment identified in line with Occupational Health and Safety Standards? | |
| Do outside parties need to be part of the assessment? | |
| If yes, are they all identified? | |
| Are all relevant insurance companies appropriately informed of the incident before assessment takes place (some insurance is void if certain disaster assessments are carried out without the insurance company present or without their knowledge)? | |

## IMPORTANT UPDATE

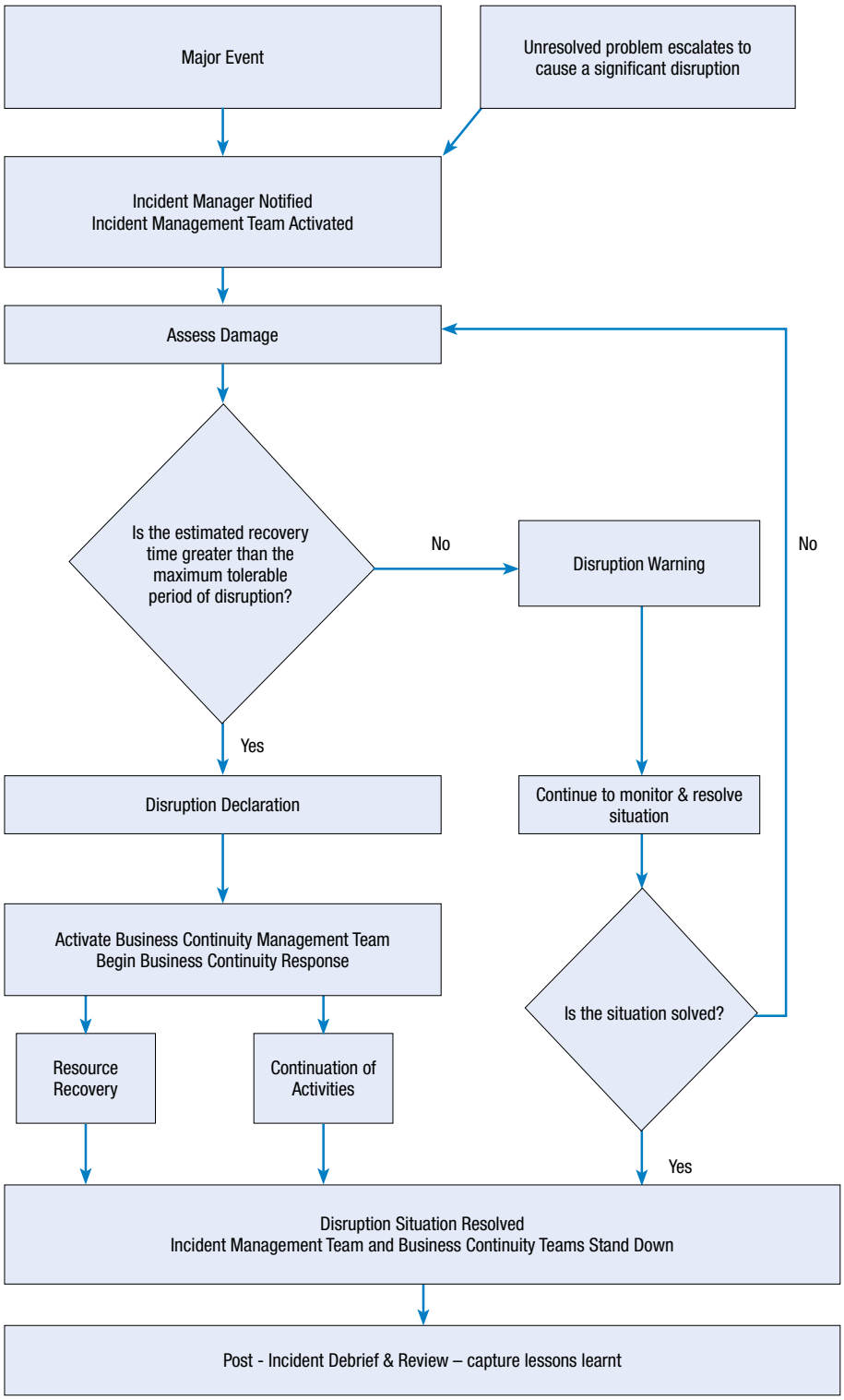
The following may assist entities by providing examples of an activation flowchart.

**Example 1: Activation flow-chart**



**IMPORTANT UPDATE**

Example 2: Activation flow-chart



## IMPORTANT UPDATE

The following is an example of a guide to sequence of response actions.

**Example: Guide to sequence of response actions**

| Sequence number | Action | Contact name or number |
|---|---|---|
| **1. ALERT PHASE** | | |
| 1.1 | The entity becomes aware of a business disruption event. | |
| 1.2 | Call Emergency Services (if required). | Ph. 000 |
| 1.3 | Attend to casualties (if required). | |
| 1.4 | The incident management team and/or business continuity management team is notified. | |
| 1.5 | The Chief Executive Officer is notified. | Mr/Ms X |
| **2. ACTIVATION PHASE** | | |
| 2.1 | The incident management team and/or business continuity management team takes charge and assesses the situation. | |
| 2.2 | A safety assessment of the entity's premises is undertaken (if required). | |
| 2.3 | Facilities Manager turns power on/off as required. | Mr/Ms X |
| 2.4 | The entity's building is secured and a security presence is established if necessary. | |
| 2.5 | Tasks are delegated by the incident management team and/or business continuity management team. | |
| 2.6 | The Command Centre is established. | |
| 2.7 | Incident management team and/or business continuity management team convenes at Command Centre. | |
| 2.8 | Voice and telephone services are redirected if necessary. | |
| 2.9 | Site managers are selected if required. | |
| 2.10 | Delegation of tasks to site managers (if multiple sites) and area recovery teams is confirmed. | |
| 2.11 | Area recovery teams are advised of the situation and how to respond to any queries, and whom enquires should be directed. | |
| 2.12 | Entity staff are notified of the situation. | |
| 2.13 | Comcare is notified if required (death within 2 hours, serious personal injury/incapacity/dangerous occurrence within 24 hours). | Ph (xx) xxxx xxxx |
| 2.14 | Appropriate people, interdependencies and organisations are contacted. | |
| 2.15 | A media liaison point is established (if required), a media centre is established, and a media conference convened (if required). | |

**IMPORTANT UPDATE**

| Sequence number | Action | Contact name or number |
|---|---|---|
| 2.16 | A recorded telephone message for staff, a print media advertisement or a press release is prepared and released. | |
| 2.17 | Incident management team and/or business continuity management team holds regular area recovery team meetings for updating and planning. | |
| 2.18 | Appropriate people, interdependencies and organisations are advised of the business disruption event (initial advice). | |
| **3. OPERATIONAL PHASE** | | |
| 3.1 | Incident management team and/or business continuity management team holds regular area recovery team meetings for updating and planning. | |
| 3.2 | Appropriate people, interdependencies and organisations are kept regularly informed. | |
| 3.3 | Regular Media Conferences are convened (if required). | |
| **4. STAND DOWN PHASE** | | |
| 4.1 | Incident management team and/or business continuity management team, and area recovery teams stand down. | |
| 4.2 | Appropriate people, interdependencies and organisations are advised when the situation is stabilised or finalised. | |
| 4.3 | Prepare and release a media statement/release when the situation is stabilised or finalised. | |
| 4.4 | Entity returns to normal operations. | |
| 4.5 | Entity undertakes post incident review. | |

## IMPORTANT UPDATE

The following template is for the development of a business continuity management immediate response meeting agenda.

**Template: Business continuity management immediate response meeting agenda**

| Agenda Item |
|---|
| Time: Date: Attendance: |
| **Status Reports**<br>Business continuity manager to brief team members<br>Team leaders to provide briefings |
| **Resources**<br>People<br>• Are staff to be sent home or relocated to a different site?<br>• Do staff need immediate counselling?<br>• Has Comcare been notified of deaths or injuries?<br>Facilities<br>• Is the building secure?<br>• Are sensitive/classified areas secure?<br>• Has preliminary damage assessment for facilities been arranged?<br>• Has subsequent salvage been arranged?.<br>Technology<br>• Has preliminary damage assessment for technology been arranged?<br>• Has the IT disaster recovery plan been activated?<br>Telecommunications<br>• Has preliminary damage assessment for telecommunications been arranged?<br>• Activate phone diversions.<br>Vital records<br>• Has preliminary damage assessment for vital records been arranged?<br>• Are sensitive/classified documents secure? |
| **Communications**<br>• Answering machine— Message to be left on <entity> Staff Enquiry Telephone Line;<br>• Staff briefing/ Chief Executive Officer/Secretary to address staff; and<br>• Stakeholders/Media. |
| **Information gathering requirements**<br>Resumption cost options; and<br>Staff relocation options. |
| Date, time and purpose of next business continuity team meeting. |

## IMPORTANT UPDATE

The following are templates for business unit or support area recovery steps. The template should be completed in advance of a business disruption event.

**Template 1: Recovery steps**

| No | Action | Responsibility | Timing |
|---|---|---|---|
| | <Action title><br><br><Short description of action including references> | <Team member name> | <Due date><br><br><Resource estimate> |
| | | | |

**Template 2: Recovery steps**

| | |
|---|---|
| Business unit/Support Area objective: | |
| Resource requirements: | |

| Critical Process | Responsibility | Minimum timescale for restoration | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | <6 hrs | 12 hrs | 1 day | 2-3 days | 5 days | >5 days | Sustained period |
| | | | | | | | | |
| | | | | | | | | |

| Task | Responsibility | Liaise with | Time due | Completed? |
|---|---|---|---|---|
| | | | | |
| | | | | |

## IMPORTANT UPDATE

The following templates may assist entities in the development of an event log.

**Template 1: Event log**

| Event Log | | | |
|---|---|---|---|
| INITIAL NOTIFICATION: | | Briefly describe the event: | |
| **Action required:** | **Yes / No** | | |
| Disaster declared: | | | |
| Standby requested from service provider: | | | |
| Date: | | Time: | |
| **Notified by:** | | **Estimated time to resolve the event:** | |
| | | Days: | Hours: |
| DISASTER DECLARED: | | | |
| Date: | | Time: | |
| Recovery site address: | | | |
| Authorised by: | | | |

**Template 2: Event log**

| Event Log | | | | |
|---|---|---|---|---|
| Event description: | | | | |
| Location: | | | | |
| **Date** | **Time** | **Actioned by** | **Contact** | **Task** |
| | | | | |
| | | | | |

**Template 3: Event log**

| Decision / Action | Date/Time | By who |
|---|---|---|
| | | |
| | | |

**IMPORTANT UPDATE**

**Explanatory material about post incident review can be found on page 59 of the better practice guide.**

## Post business disruption event or exercise review

It is important to record and evaluate the business disruption. This facilitates the review of the business continuity response after the entity has returned to normal operations.

The following checklist may assist entities in conducting a review after an exercise or business disruption event.

**Checklist: Conducting a review after a business disruption event or exercise**

| Task | Completed Yes/No |
|---|---|
| Determine whether the aims of the exercise were achieved/whether the aims of the business continuity plan were achieved. | |
| Determine what worked well. | |
| Determine what did not work well. | |
| Identify lessons learned. | |
| Identify potential improvements or revisions to be made to the business continuity plan. | |
| Identify areas for future tests and exercises. | |
| Draft report of the exercise. | |
| Assign responsibility for implementing any recommendations made to improve performance. | |
| Monitor implementation of recommendations. | |

## IMPORTANT UPDATE

The following template may assist entities in developing a post business disruption event or exercise review report.

**Template: Post business disruption event or exercise review report**

| Post business disruption event or exercise review |
|---|
| Division/Office:<br><br>Critical business process:<br><br>Specific functionalities:<br><br>Team leader:<br><br>Team members:<br><br>Type of disruption/exercise:<br><br>Business Continuity Plan/Exercise objectives:<br><br>Were the objectives met? (If no, explain):<br><br>Brief summary of findings:<br><br>Corrective action recommendations:<br><br>Schedule to implement plan changes:<br><br>Assigned to:<br>Sign-off (Division/Office Head):<br>Date: |

**IMPORTANT UPDATE**

# Maintaining the program and plan: Testing, exercising, updating and reviewing

Better practice entities maintain the business continuity plan to reflect the entity's objectives, its critical business functions, the corresponding processes and resources and agreed priority for recovery.

The following checklist may assist entities in maintaining their business continuity plans.

**Checklist: Maintaining the business continuity management program**

| Element | Issue | Activity Status | | | | Comments |
|---|---|---|---|---|---|---|
| | | Not started | Delayed | On track | Completed | |
| Entity/business unit/service area name: | | | | | | |
| Year: | | | | | | |
| Training and Awareness | Staff have received information explaining the business continuity program. | | | | | |
| | Staff have received information explaining the structure and content of plans. | | | | | |
| | Nominated staff have received relevant specialist/technical training (for example in the conduct of the business impact analysis). | | | | | |
| | Nominated staff have taken part in training through the exercising of plans. | | | | | |
| Testing and Exercising | A program of testing and exercising has been developed. | | | | | |
| | Testing and exercising has been implemented. | | | | | |
| Updating | The business continuity plan has been updated. | | | | | |
| | The business impact analysis has been revalidated. | | | | | |

## IMPORTANT UPDATE

| Element | Issue | Activity Status | | | | Comments |
|---|---|---|---|---|---|---|
| | | Not started | Delayed | On track | Completed | |
| Reviewing | The business continuity management program is subjected to regular monitoring and review of its effectiveness. | | | | | |
| | Plans are subject to regular performance monitoring and review of their effectiveness. | | | | | |
| | Criteria have been identified and are monitored for triggering the review of plans. | | | | | |
| | A program or framework of assurance activities is in place to help ensure conformance to entity needs. | | | | | |

**IMPORTANT UPDATE**

**Explanatory material about testing the business continuity plan can be found on page 61 of the better practice guide.**

## Testing the plan

Testing the recovery processes documented in the business continuity plan will provide management assurance that these processes will be effective in the case of a business disruption.

The following checklist may assist entities in testing manual backup procedures.

**Checklist: Testing manual backup procedures**

| Testing manual backup procedures tasks | Completed Yes/No |
|---|---|
| Identify all categories of off-site backup addressed by the procedures. Consider:<br>• hard copy documentation;<br>• forms (application forms, manual receipts; blank cheques) ;<br>• supplies, and<br>• equipment. | |
| For each of the categories of items identified as being backed up, identify the triggers for adding/replacing/deleting off-site backup items. | |
| Identify people responsible for determining what is to be backed up. | |
| Identify people responsible for review and approval of changes/terminations of off-site backup items. | |
| Determine if an inventory of items is available and how the inventory is maintained. | |
| Determine whether a hardcopy of the off-site backup inventory is stored off-site. | |

## IMPORTANT UPDATE

The following checklist may assist entities in testing IT backup procedures.

**Checklist: Testing IT backup procedures**

| Testing IT backup procedures tasks | Completed Yes/No |
|---|---|
| Identify all types of files being backed up off site. Consider:<br>• system software:<br>- operating systems;<br>- support software;<br>- utility packages;<br>- communications software, and<br>- job control language.<br>• application software:<br>- source libraries;<br>- production libraries (Executable Code);<br>- data dictionary files; and<br>- production data disk files and databases.<br>• user files:<br>- on-line documentation;<br>- production scheduling;<br>- computer operations documentation (for example recovery/restart), and<br>- application system/program documentation.<br>• archival files. | |
| For each of the categories of items identified as being backed up, identify the method(s) of backup. Consider:<br>• on-line replicated data backup at alternative site;<br>• full saves (entire file or database backed up);<br>• incremental saves;<br>• production job stream;<br>• on request by user;<br>• application nightly backup batch run; and<br>• special job stream. | |
| Determine the backup frequency and number of cycles retained off-site for each category of backup. | |
| Identify persons responsible for determining what is to be backed up. | |
| Identify persons responsible for review and approval of changes/terminations of off-site backup cycling. | |
| Note the reason(s) why any types of files are not being backed up off-site. | |
| Determine if backup procedures are applied application by application, or to an entire category of applications such as those designated critical. | |

**IMPORTANT UPDATE**

| Testing IT backup procedures tasks | Completed Yes/No |
|---|---|
| Identify the tool(s) used for identifying and recording off-site backups. Consider:<br>• logs of on-line file replication;<br>• tape library management software packages;<br>• manual logs;<br>• special program/system with manual input; and<br>• special program/system with automated input. | |
| Determine if vendor provided software products are used to perform backups. | |
| Regular recovery from backup media to confirm the integrity of the data | |
| If a third party provides off-site storage, does the existing contract for retrieval and recovery of storage media match the requirements of the business continuity plan? | |

Note: When the term application(s) is used in the above checklist, it refers to operating system software, support software, utilities, and communication software in addition to end user business applications.

**IMPORTANT UPDATE**

## Exercising the plan

An exercise program should be developed so that over time the entity gains assurance that the business continuity plan will operate if and when required. This forward-looking exercise program is sometimes called an exercise universe.

The following template is an exercise universe.

**Template: Exercise universe**

| Exercise | Year A | | | | Year B | | | | Year C | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| Business continuity | | | | | | | | | | | | |
| Whole of entity plan | | | | | | | | | | | | |
| Business area/service unit plans | | | | | | | | | | | | |
| Resources:<br>• People<br>• Facilities<br>• Technology<br>• Telecommunications<br>• Vital records | | | | | | | | | | | | |
| Interdependencies | | | | | | | | | | | | |
| Other | | | | | | | | | | | | |
| Related exercises | | | | | | | | | | | | |
| Incident management | | | | | | | | | | | | |
| Emergency response management | | | | | | | | | | | | |
| Pandemics | | | | | | | | | | | | |
| IT disaster recovery<br>• System/Application<br>• Infrastructure | | | | | | | | | | | | |

**Explanatory material about exercising the business continuity plan, as well as a case study about a partial live exercise scenario can be found on pages 63-64 of the better practice guide.**

## IMPORTANT UPDATE

The following templates are for business continuity exercise preparation.

**Template 1: Exercise preparation template**

| Exercise development worksheet | | | |
|---|---|---|---|
| **Title of exercise:** | *(What type & method of exercise will be used)* | | |
| **Business Unit/Department/Organisation involved in exercise:** | | | |
| **Location of exercise:** | | | |
| **Date/Time of exercise:** | | | |
| **Length of exercise:** | | | |
| **Objective(s) of exercise:** | | | |
| **Critical resources to be trained or exercised:** | **Resources** | **Yes** | **No** |
| | People | | |
| | Facilities (including buildings and equipment) | | |
| | Technology (including IT systems/ applications) | | |
| | Telecommunication | | |
| | Vital records | | |
| | Interdependency | | |
| **Exclusions from exercise:** *(what will not be in the exercise)* | | | |
| | | | |
| **Support requirements:** *(what equipment, staffing, facilities, scripts will be needed)* | | | |
| | | | |
| **Approved by:** *(name and position)* | | | |

**IMPORTANT UPDATE**

**Template 2: Exercise preparation template**

| Business continuity exercise preparation | | | | | | |
|---|---|---|---|---|---|---|
| Business Unit: | | | | | | |
| Location: | | | | | | |
| Contact name and title: | | | | | | |
| Telephone: | | | | | | |
| Email: | | | | | | |
| Exercise title: | | | | | | |
| Plans to be exercised: | | | | | | |
| Critical business functions/organisational units involved: | | | | | | |
| Exercise locations: | Date 1 | | Start | | End | |
| | Date 2 | | Start | | End | |
| | Date 3 | | Start | | End | |
| | Date 4 | | Start | | End | |
| Exercise objectives: | | | | | | |
| Resources involved/required: | | | | | | |
| Exercise exclusions: | | | | | | |
| Support requirements: | | | | | | |
| Exercise facilitator: | | | | | | |
| Exercise approved by: | | | | | | |

## IMPORTANT UPDATE

The following checklist may assist entities in reviewing the adequacy of information flows following a scenario exercise (or actual business disruption event).

**Checklist: Reviewing the adequacy of information flows following a scenario exercise (or actual business disruption event)**

| Reviewing the adequacy of information flows following a scenario exercise (or actual business disruption event) tasks | Completed Yes/No |
|---|---|
| The business continuity plan has communication flows which enabled the Recovery Coordinator to be kept adequately informed by the business unit and service area recovery teams throughout the recovery process. | |
| The business continuity plan communication flows keep underlying service area recovery teams informed throughout the process. | |
| The business continuity plan ensures service area recovery team members are kept adequately informed of where the agency is in the recovery process. | |
| Business unit and service area recovery teams working to recover interrelated business processes are kept properly informed of the recovery process and keep other teams informed of their progress. | |
| Business unit and service areas keep appropriate external parties and stakeholders informed (not including parties/stakeholders that would be kept informed as part of the management plan) of the recovery process. | |
| External and internal parties included in the business continuity plan are informed immediately that their assistance may be called upon. | |
| Ensure all human resource needs are properly addressed. Consider: OHS, counselling and other support lines of communication. | |
| Was part of the recovery process the re-implementation of controls (physical, logical and environmental)? | |
| The incident management team and/or executive are kept properly informed throughout the process. | |
| There are specific protocols for media liaison and management. | |

**IMPORTANT UPDATE**

## Updating the plan

Plans must be kept up-to-date to provide support for business continuity. Administrative procedures and guidelines should be developed to provide for periodic exercising, documented maintenance of the plans as well as ongoing training.

The following template is a timetable for updating business continuity plan(s) documents.

**Template: Timetable for updating business continuity plan(s) documents**

| Part | Name of plan | To be updated | | | | |
|---|---|---|---|---|---|---|
| | | Q1 | Q2 | Q3 | Q4 | Triggers for non scheduled updates |
| Year: | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Explanatory material about updating the business continuity plan can be found on page 65 of the better practice guide.**

**IMPORTANT UPDATE**

## References

The examples, templates and checklists contained in this better practice guide and workbook have been developed by the ANAO, using information from:


- ANAO audits of the *Financial Statements of General Government Sector Agencies,* various years.
- ANAO Better Practice Guide *Business Continuity Management: Keeping the wheels in motion 2000.*
- ANAO *Business Continuity Plan 2008.*
- *Attorney-General's Department Business Continuity Plan 2008.*
- Australian Maritime Safety Authority, various documents.
- Australian Taxation Office, various documents.
- Comcover *BCP Template.*
- Comcover: *Business Continuity Management Participant Manual 2007.*
- *Department of Education, Employment and Workplace Relations Business Continuity Framework 2008.*
- Department of Families, Housing, Community Services and Indigenous Affairs, various documents.
- Ernst and Young, *Business Continuity Test Universe.*
- Ernst and Young, *Generic Business Continuity Management Policy.*
- *HB 221:2004 Business Continuity Management.*
- *HB 292:2006 A Practitioners Guide to Business Continuity Management.*
- National Blood Authority, various documents.
- *The Treasury Business Continuity Plan 2008.*
- Whittet, Continuity Forum Pandemic Planning Workshop, *Pandemic Plan Framework,* 2008.

**Business Continuity Management**

The *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act 1997* were replaced by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and supporting rules on 1 July 2014. The PGPA Act provides a common legislative framework for the governance, performance and accountability of all Commonwealth entities.

The ANAO proposes to update this Guide in 2015-2016 to reflect national and international developments in standards and practices for business continuity management.

Further information on the PGPA Act is available at:

www.pmra.finance.gov.au

**< BACK**