Business Continuity Management

Keeping the wheels in motion

Better Practice

Australian National Audit Office

A Guide to Effective Control—January 2000

ISBN 0 644 39018 2

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Information on Australian National Audit Office publications and activities is available on the following Internet address: http://www.anao.gov.au

Disclaimer

The Auditor-General, the ANAO, its officers and employees are not liable, without limitation, for any consequences incurred, or any loss or damage suffered by an organisation or by any other person as a result of their reliance on the information contained in this Guide or resulting from their implementation or use of the accompanying Workbook, and to the maximum extent permitted by law, exclude all liability (including in negligence) in respect of the Guide and the accompanying Workbook.

Designed by Art Attack Pty Ltd Canberra
Printed by Pirie Printers Canberra

Business Continuity Management

Keeping the wheels in motion

Guide to Effective Control—January 2000

Better practice

The Australian National Audit Office produces better practice guides as part of its integrated audit approach which includes information services to audit clients.

A Better Practice series has been established to deal with key aspects of the control structures of entities—an integral part of good corporate governance.

This Guide forms part of that series. It deals with business continuity management within a risk management framework. The accompanying Workbook is designed to assist organisations in the development of a comprehensive business continuity plan.

Acknowledgments

The Guide has been prepared with the valuable assistance and insights from a number of Commonwealth organisations, primarily:

- Air Services Australia;
- Australian Nuclear Science and Technology Organisation;
- Australian Maritime Safety Authority; and
- Therapeutic Goods Administration.

Input from Standards Australia and Emergency Management Australia has also been invaluable in refining the approach developed for this Guide so that it fully integrates into the risk management framework within an organisation. Finally, the valuable assistance of Deloitte Touche Tohmatsu in developing the business continuity plan (BCP) project steps discussed in Part Two is also recognised. The ANAO records its appreciation of this assistance.

Auditor-General's foreword

Continuity of public sector business is a critical issue to be considered by Boards, chief executives and senior management in Australian public sector organisations and for business activities. Many services delivered by government organisations are critical to the economic and social well-being of our society—a failure to deliver these could have very significant consequences for those concerned.

The uninterrupted availability of all key resources to support essential business processes or simply, *business continuity,* has been taking a considerable amount of managers' time and attention recently. Much of the impetus to review business continuity resulted from a need to treat business continuity risks associated with any systems failures at the change to the year 2000 or, as it is more commonly known, the Y2K bug. Considerable resources were expended to ensure minimal disruption from the anticipated problems.

The current focus of business continuity efforts on Y2K remedies and contingency planning was acceptable in the circumstances. However, beyond this, organisations should address and regularly review **all** aspects of their business continuity management.

This Guide presents a structured approach to business continuity management. The approach involves identifying preventative treatments for continuity risks that can be routinely managed, and developing an organisation-wide business continuity plan—to deal with the consequences should the preventative treatments fail. The approach should be tailored to meet organisational needs while satisfying the major steps identified for business continuity management in the context of overall risk management.

Managers should have an ongoing focus on business continuity as an element of the overall risk management framework in their organisation. While the profile of business continuity is still high, it would be opportune to build on the work and analyses done in relation to the risks associated with Y2K, to ensure business continuity risks are identified, assessed, analysed and treated, as well as being monitored and reviewed.

The Guide further develops the approach promoted by Emergency Management Australia in its publication: *Non-stop Service*.

The increasing level of devolved authority and management in the public sector, a greater use of contracted service delivery and the pursuit of improved efficiencies and performance, means that the need to manage proactively an organisation's overall risk has never been greater. It would be ill-advised to ignore risks to business continuity because their likelihood is too

remote—in the medium to longer term this could well prove costly for both the organisations and the clients (citizens). There are sufficient examples in the public sector to demonstrate the unlikely can, and does, happen ... usually when we least expect it. Often these events are outside the direct control of the organisation, but this does not mean you should not plan for their impact. The following incidents provide compelling reasons for business continuity to be taken seriously:

- *severe hailstorms in Sydney, NSW, (1999)* – damage to many government and business buildings and meant emergency measures had to be taken to relocate operations while continuing to provide a service to their clients;
- *the Victorian gas crisis (1999)* – following an explosion at a gas production facility, the entire State faced weeks without gas supplies and the costs to business and government was estimated in the billions of dollars;
- *Brisbane, Queensland and Auckland, New Zealand, power outages (1998)* – following generator and grid failures, the cities were without electricity—government and business alike has to operate in a city without reliable power supplies for an extended period;
- *fires at the Bankstown Council, NSW, (1997) and Knox Council, VIC, (1994)* – in which the council chambers were burnt down and vital records as well as IT were lost; and
- *Jolimont Centre incident, Canberra, ACT (1993)* – following a siege and fire, the then Commonwealth Department of Industrial Relations was forced to relocate about 400 staff and the supporting infrastructure.

The range, source and impact of risk to which an organisation is exposed in today's business world demand that business continuity has to rank highly for ongoing management attention. Indeed, it should be an integral element of the organisation's risk planning strategy.

P.J. Barrett
Auditor-General

January 2000

Contents

Overview of this Guide

Business continuity management is an integral part of the risk management framework within an organisation. All organisations face a variety of risks. These may be sourced externally, and therefore largely out of the immediate control of the organisation, or internally. Internal risks arise both at the strategic (organisation-wide) level and at the operational (business process) level.

This Guide has been prepared primarily for the people involved in a business continuity project—from individual team members through to the Chief Executive and Board. Each participant plays an important role and has an array of responsibilities in ensuring the success of the project and continuing validity of the plan.

Successful business continuity management relies on the expertise from within the organisation—it is the people that understand the organisation—its business, processes and business risks. However, the Guide does not assume everyone is an expert in the field of risk management so describes each phase of business continuity against an accepted, generic risk management framework.

Each risk, depending on its nature, will have a greater or lesser chance of occurrence (likelihood) and a greater or lesser business impact on the organisation (consequence). The business impact of each risk will also vary according to its nature—for any particular risk event there may be, for example, a financial consequence, a legal consequence, a staff safety consequence, and a business interruption consequence.

Organisations, through a structured, systematic process attempt to manage all significant business risks pro-actively, by implementing appropriate preventative controls and other risk treatments. This risk management process is designed to reduce the residual risk of an event—in terms of its likelihood of occurrence and/or its consequences, to an acceptable level.

However, preventative controls and other pro-active treatments are no guarantee that risk events will not occur, that is, they cannot entirely eliminate their likelihood of occurrence. Therefore, for effective risk management it is equally important that organisations design controls that are implemented once a risk event has occurred.

The design (and therefore cost) of such corrective controls and treatments will need to take into account assessments of the pro-active controls and the residual risk levels. The key question is how much time, effort and resources need to be invested in corrective controls—in preparing for an eventuality that may never occur.

This Guide has been designed to assist organisations answer this question for those risk events that have a business interruption consequence of a nature and impact that warrants effective management action.

The underlying approach adopted in this Guide is to start from the point that a risk event has occurred which has interrupted business operations—that is, assuming a *worst case* scenario where all processes and resources are not available. In this context the cause or nature of the actual risk events are not considered to be the drivers for management action. It is the business interruption **consequence** that mainly determines the process.

This *bottom-up* approach complements the 'top down' approach inherent in the over-arching risk management process. It ensures completeness of consideration of all consequences arising from a business interruption risk event. It also ensures pro-active and corrective controls are complementary and should allow organisations, for example, to achieve a cost-effective compromise between preparedness for the *worst case* scenario and the likelihood of such a scenario ever arising.

The Guide is divided into two major parts—the first part deals with business continuity management concepts in a risk management context; the second part identifies the processes and procedures required to be undertaken to produce a business continuity plan.

A number of supporting pro-forma schedules, working papers and questionnaires have been prepared to facilitate the overall process described in the Guide. These are contained in the Business Continuity Workbook that accompanies this Guide.

Part One

Continuity and risk concepts

Introduction

Business continuity management

- Objective
- Outputs
- Underlying approach
- Terminology

Risk management

- Overview of the risk management process
- Step one: establish context
- Step two: identify and assess risks
    - risk indentification
    - risk analysis
    - risk treatment design
- Step three: implement treatments
- Step four: monitor and review

Introduction

Business continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities.

An organisation's business strategies and decisions are based on an assumption of the business continuing. An event that violates this assumption is a significant occurrence in the life of any organisation, impinging directly on its ability to fulfil its business objectives and the livelihood of those involved.

Among other things, risk management is about putting in place treatments that seek to prevent business interruption events (outages) from occurring in the first place. It also encompasses establishing appropriate responses (treatments) should such an event occur.

Business continuity management is therefore that part of risk management that establishes cost-effective treatments should an outage occur. As such, it deals with actual events—a risk event which has occurred—and the action required to respond to the event. To this extent, it complements the overall risk management process which deals foremost with possibility of occurrence of risks events (including outages) that may occur, and the analysis and pro-active treatment of such events.

This section of the Guide outlines the risk management process and discusses how business continuity management fits within this process. It is not intended to cover all aspects of risk management. Instead, the Guide will focus on those parts of the process where business continuity risks should be specifically addressed.

However, before dealing with the risk management process, the Guide introduces a number of key business continuity concepts. It is important that readers of the Guide familiarise themselves with these concepts and in particular, the terminology used, before embarking on the business continuity management process.

Part Two of this Guide takes the reader through the detailed steps for the business continuity management process.

Business continuity management

The difference between business continuity and disaster recovery is not a 'what' but a 'whose'. Business continuity now appears on the boardroom agenda, but there was a time when disaster recovery was relegated to one corner of the computer room. Planning for business continuity should be a top-level concern for enterprises, considering the potentially devastating financial and organizational impact of a disaster.
An Introduction to Business Continuity Planning, InSide GartnerGroup This Week (IGG),
C. Gooding, January 8, 1997

In the business continuity management process it is important to consider what plans are already in place, so effort is not wasted.

Objective

The objective of business continuity management is to **ensure the uninterrupted availability of all key business resources required to support essential (or critical) business activities**.

This holistic view of business continuity management differs from what many managers traditionally term *Disaster Recovery Planning* which has been closely, if not solely, associated with information technology. By changing the focus, the emphasis is placed on the whole business, not just on technology issues alone. This reinforces the concept of continuity of **all key processes**, extending beyond information technology systems, important though they are in modern business.

Outputs

The primary output from the business continuity management process is a **Business Continuity Plan (BCP)**. The BCP comprises many elements which, collectively, define the approach to dealing with a break in business continuity, and which prescribes the steps an organisation should take to recover lost business functions.

Amongst other matters, the BCP will bring together the:

- service area Contingency Plans;
- Disaster Recovery Plan (DRP); and
- Business Resumption Plan (BRP).

The business continuity management process and the BCP need to bring together all such elements to ensure they adequately address the organisation's business interruption risks.

There are probably already some parts of the BCP the organisation has in place as part of its normal business operations. They include:

- IT disaster recovery plans;
- emergency response procedures;
- off-site of recods;
- backup and recovery procedures;
- evacuation plans;
- communications strategies; and
- media liaison strategies.

Alone these do not constitute a complete BCP, but are important elements of a robust continuity plan.

Underlying approach

The BCP is initiated when a risk event occurs that has a **business interruption** consequence. The business interruptions that are of concern from a continuity viewpoint are referred to as **outages**. These events will cause a significant disruption to, or loss of, key business processes. It follows that such events will have a high impact on, and severe consequences for, the organisation.

Outages 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 off a communications link which needs to be re-established with a service provider.

The concept of an outage has a time dimension as well as a business process dimension. The business continuity management process includes establishing the maximum periods for which each function can be disrupted or lost altogether, before it threatens the achievement of organisational objectives.

What is the maximum time the business can survive without key business functions before the BCP must be initiated and recovery procedures must commence?

The analysis of the impact of an outage focuses on consequences. It is not concerned with the likelihood or cause of occurrence, as they are not elements of the BCP. Matters of likelihood and cause should already have been addressed as part of the *top down* risk management process and preventative controls should already have been established to reduce the likelihood and consequences of all risk events (including business interruption events) to levels that are acceptable to management.

The *bottom-up* approach to business continuity management complements the *top down* approach adopted for overall risk management by asking "what happens if the controls fail"? It puts in place planned, coordinated responses which escalate according to the nature of the outage. This extends to a complete loss of all business processes and resources, referred to as a *disaster*. While *disasters* thankfully are an extremely rare occurrence in the life of most organisations, the consequence (or business impact) analysis assumes that a disaster can occur. This *worst case* scenario modelling will ensure that all impacts arising from an outage are considered regardless of the likelihood of occurrence.

As discussed above, consideration of causes and sources of threats is not part of the BCP. It is important that continuity plans are not developed solely from this perspective as it is unlikely organisations will be able to identify all possible causes of outages or the source of all threats. In the past, many plans have failed as they have confined themselves to one type of outage based on a limited threat analysis—usually a physical disruption.

Terminology

The above discussion introduced a number of key terms and concepts. The following table summarises these terms and their meanings for ease of reference and understanding.

Concept	Description	Examples/Comments
Outage • extraordinary event • loss of key business processes • high impact	An outage is an extraordinary event, causing a disruption to, or loss of, key business processes, which has a high impact on the organisation. This is distinct from downtime or systems failures that may occur as a part of normal operations where the impact simply reduces the effective utility of processes in the short term.	*During an outage parts of the Business Continuity Plan (BCP) may be activated in order to deal with the situation. The full activation of a plan (ie. for a total disaster) must be defined for each plan during the plan development phase.*
Maximum Acceptable Outage (MAO) • threat to achieving business objectives	The MAO is the time it will take before an outage threatens an organisation achieving its business objectives. The MAO defines the maximum time an organisation can survive without key business functions before business continuity plans and recovery procedures must commence.	*A 'disaster' is used in this Guide to mean an event that leads to a business interruption that will extend beyond the period specified for an MAO.*
Business Impact Analysis (BIA) • key business processes • recovery priority	The BIA is undertaken for all key business processes and establishes the recovery priorities, should those processes be disrupted or lost.	*Key business processes should have been identified as part of other business planning or risk management processes. If this has not been done, the BIA will need to do so.*
Key business processes • business activities and resources	Key business processes are those processes essential to delivery of outputs and achievement of business objectives. Business activities and resources are the essential elements that combine to make up each key business process. Loss of a key business process in excess of the MAO is a business interruption event	*In a self-funding organisation, a key business process would be a billing system as the organisation depends on cash flow for its survival. In a budget-funded organisation that pays benefits, a key business process may be a benefits payments system that is essential to servicing client needs.*

Concept	Description	Examples/Comments
Business activities	A business activity is a series of actions combining to produce an identifiable output and/or result.	*The billing process may require customer sales information, a system to record information and calculate and print invoices, and registry or mail system to send invoices and receive remittances. A benefits payments process may rely on staff to interview clients and fill in forms; entering that information on a computer system; periodic payments to bank accounts; and include an an inquiry facility to follow-up on discrepancies.*
Resources	Resources are the means that support delivery of an identifiable output and/or result. Resources may be money, physical assets or, most importantly, people. Without resources, activities (and therefore business processes) would simply not occur.	*The customer billing system relies on people to undertake procedures; operate computer systems; produce information; office supplies for preparing and mailing the invoices; buildings and power to house the people; and computers. A benefits payments system relies on people, computers, office supplies, building and power and also on having sufficient funds available to make payments when due.*
Procedures	Procedures are the steps undertaken by an individual to achieve a result. Identification of these procedures is important in continuity planning as it is these steps which will need to be recreated or redesigned to be used during an outage.	*Customer billing and benefits payments may rely on a series of steps to ensure information is correct prior to bills being issued or benefits paid. If an outage causes the loss of the computer system supporting these validations, alternate processes may need to be developed to ensure continuity of that business function.*
Risk event	Any non-trivial event that affects the ability of an organisation to achieve its business objectives.	*Risk events may be considered in terms of their causes, likelihood and impacts.*
Business interruption event	A risk event that has a business interruption consequence.	*Business interruption events are 'outages' and other operational events that do not affect business continuity.*

Risk management

Overview of the risk management process

The risk management process generally used in Australia today and as espoused in the MAB/MIAC *Guidelines for Managing Risk in the Australian Public Sector*[1], is modelled on the Australian/New Zealand Standard AS/NZS 4360:1999 '*Risk Management*'.

The Standard proposes a logical and systematic methodology for identifying, analysing, assessing, treating and monitoring risks. In this context, risks may be considered as events that will, should they occur, impact on the achievement of organisational objectives.

While risk is generally considered in a negative light, that is, as having an adverse impact, the Standard contemplates not only events that may lead to loss or harm, but also those that may lead to gain or advantage.

A business continuity event (described as an 'outage' in this Guide) is an **adverse** risk event. The primary objective of managing such events is to prevent them from occurring in the first place, where it is both within the control of the organisation and where it is cost-effective to do so. Treatments designed to prevent risk events occurring are commonly referred to as preventative controls. However, even the best-designed controls can breakdown in operation and an outage may occur.

In addition, certain risk events may be outside the control of the organisation (referred to as *external risks*). This is particularly the case in relation to natural (eg. fire, flood); political (eg. change of government policy, changes to legislation), and economic (eg. financial market collapses, economic downturn) events.

The primary objective, when **any** risk event (including an outage) becomes a reality, is to have in place treatments that will mitigate the business impact of the event. In the case of an outage, the preferred outcome is to maintain the continuity of service.

A comprehensive approach to risk management will therefore consider risk treatments both proactively—by designing and implementing controls to prevent risk events occurring—and reactively—by mitigating the consequences of such events, should they actually occur.

This philosophy can be best summed up as **plan for the best but be prepared for the worst**. In practice, this requires risk managers to undertake an analysis of risks and risk treatments from the *top down*—starting with possible risk events and designing controls—and from the *bottom up*—assuming a risk event has occurred and preparing appropriate contingency

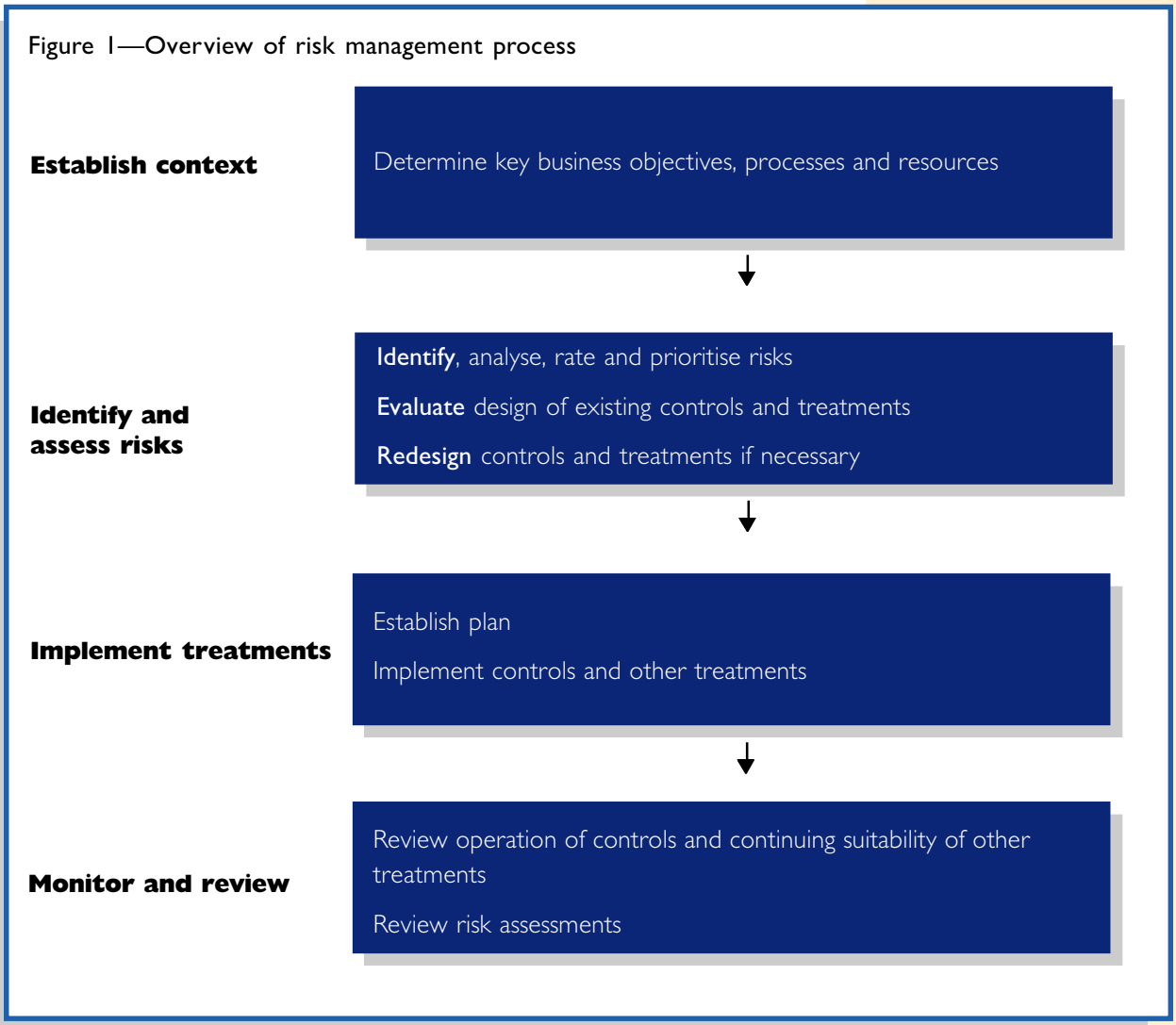
1 MAB/MIAC Report No. 22 *Guidelines for Managing Risk in the Australian Public Service*, October 1996.

plans. These approaches are complementary and should be undertaken in parallel, using the process described in the Risk Management Standard.

Figure 1 outlines a risk management process developed from the Standard which is relevant to business continuity management. There are four major steps in this process:

- establish the organisational context;
- identify and assess risks and design treatments;
- implement risk treatments; and
- monitor and review risks and treatments.

Figure 1—Overview of risk management process



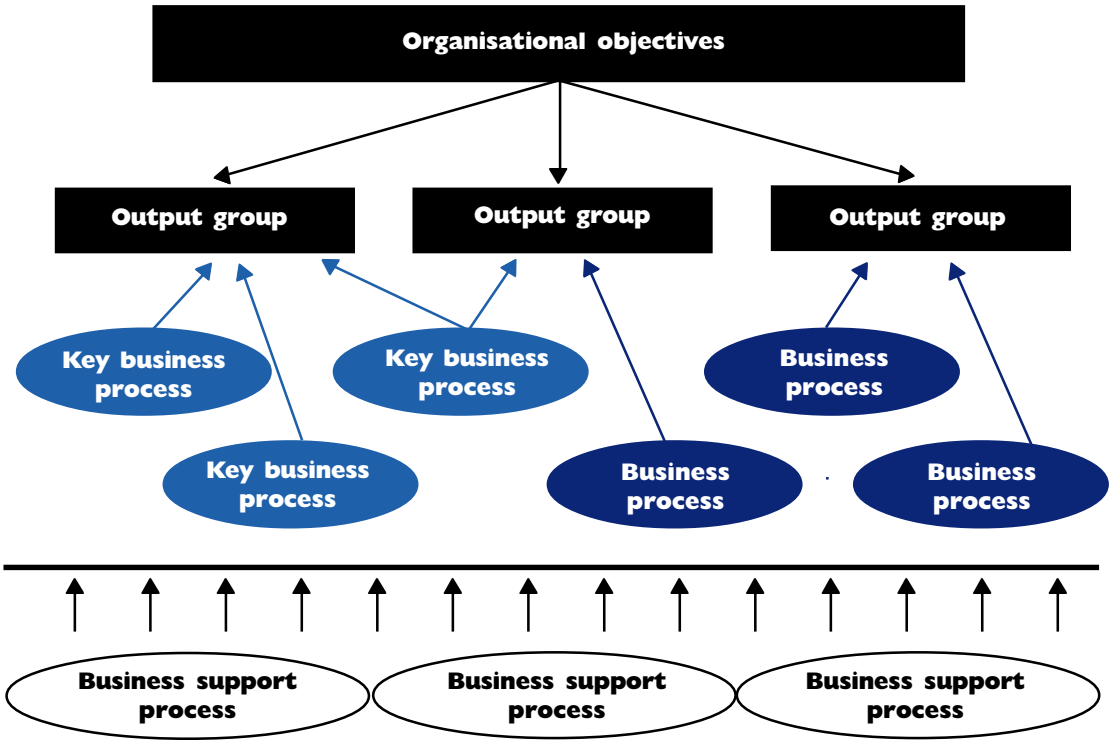
Business continuity management is an integral part of this process. The remainder of this section deals with those aspects of the risk management process that relate directly to business continuity. Each step is examined in turn.

Step one: establish context

Risk management is undertaken at both the strategic (organisation–wide) and operational (business process) levels of an organisation. The Risk Management Standard discusses the need to first establish the organisational and risk management context (Figure 2) in order to create a framework within which the process is carried out.

In particular, the organisational objectives must be clearly defined, as well as the functions, activities and related resources that are to be subject to risk assessment. This step enables organisations to determine which are the key business processes so that they may focus and prioritise their risk management efforts.

Figure 2—Establishing the organisational context



Organisations should identify their key business processes and business support processes by relating them to their overall objectives, outcomes and outputs. The activities and resources attributable to these critical processes should be afforded the highest priority in undertaking risk assessments.

Link with business continuity management

The first step toward developing a business continuity plan is to undertake a **business impact analysis**. This analysis defines the **maximum acceptable outage** for each key business process and sets the recovery priorities for the activities and resources underpinning them.

Key business processes may have been identified earlier during an overall risk management project. These become an input to the business impact analysis.

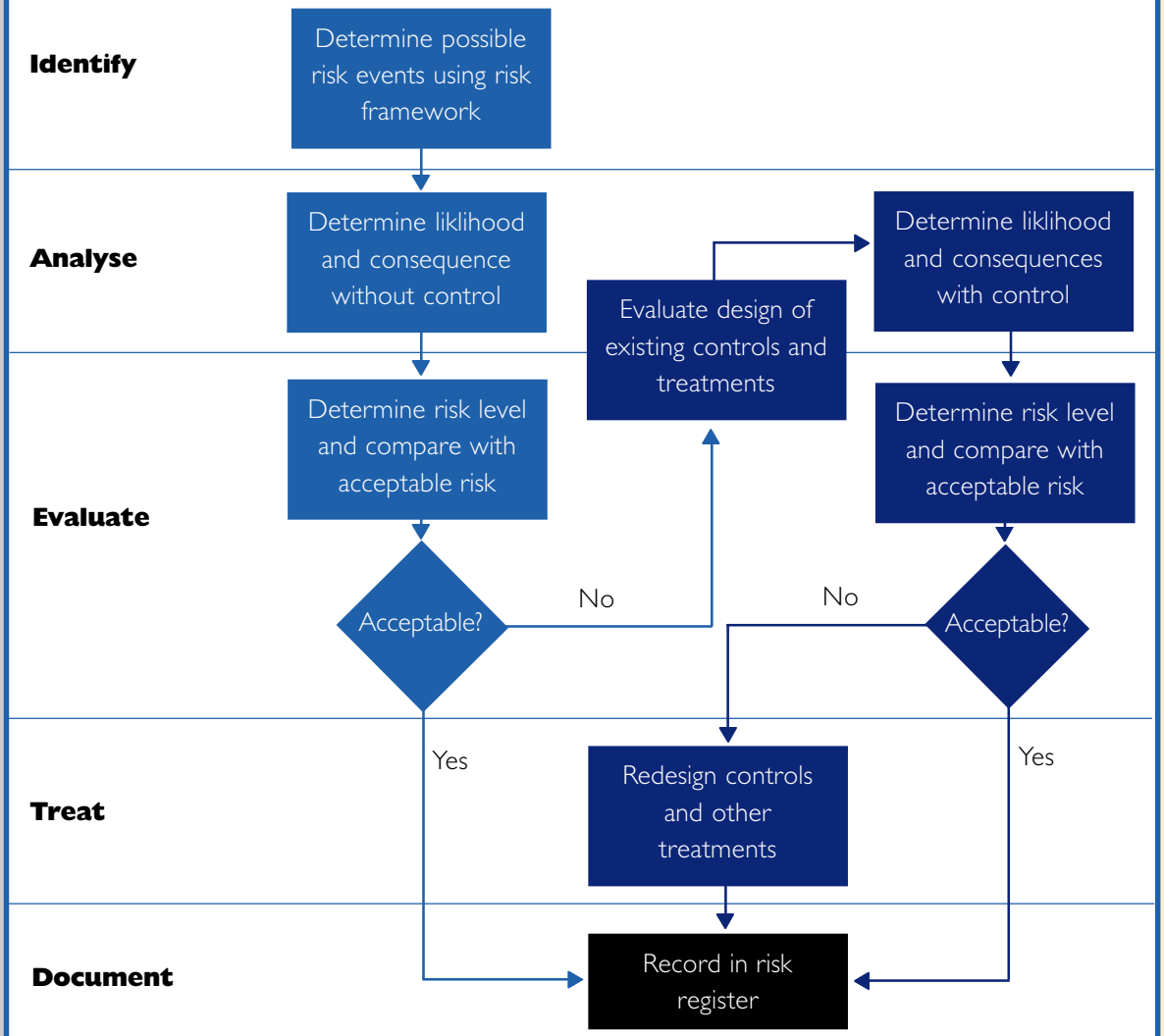
Step two: identify and assess risks

This phase of the risk management process requires organisations to:

- identify all non-trivial business risks;
- assess those risks; and
- design treatments that reduce the risks to an acceptable level.

These aspects of the overall risk management process are highlighted in Figure 3.

Figure 3—Outline of the risk assessment phase of the risk management process

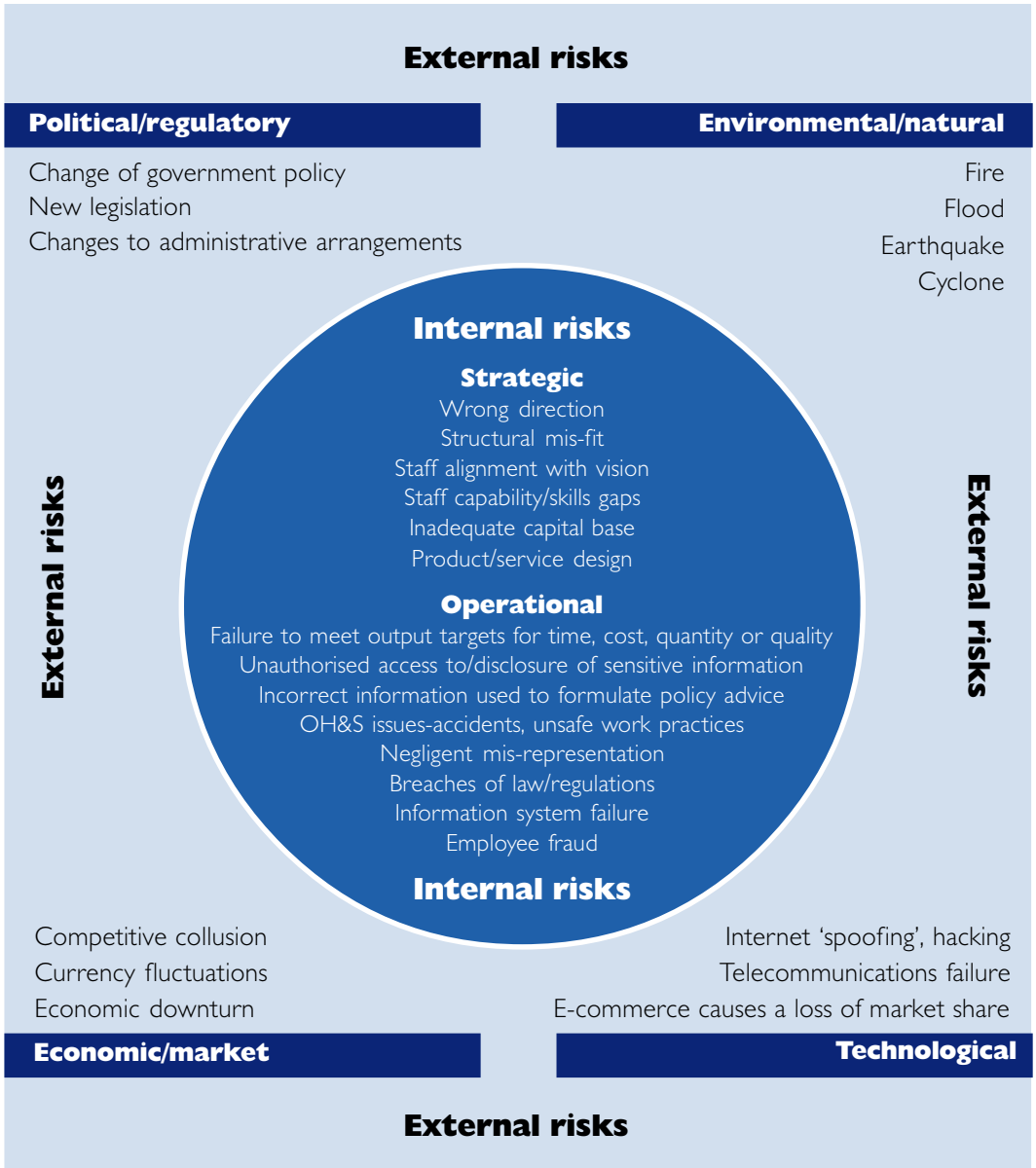


Once risks have been identified, they are analysed in terms of their likelihood and consequences. The diagram illustrates a two-step approach which analyses risk before and after consideration of controls.

Risk identification

Typically, organisations use a risk classification framework to ensure that all likely risks are identified. An example of such a framework is illustrated in Figure 4.

Figure 4—Risk classification framework



Risks may arise both from external sources and internally—emanating from within the organisation and arising from its strategic and operational processes.

Each risk event may have a number of consequences that will impinge on an organisation's ability to achieve its business objectives. The next step in the risk assessment phase is to analyse these impacts and determine the likelihood of occurrence so that a **risk level** can be established for each risk.

Risk analysis

The objective of this analysis is to separate the risks identified in the previous step into minor (acceptable) risks and major (unacceptable) risks. This is achieved by comparing the risk level to pre-determined criteria of acceptability.

There are number of approaches to risk analysis that may involve quantitative, qualitative or semi-quantitative evaluation. For whatever approach is adopted, the likelihood and consequences of each risk event are determined and the combination of these two evaluations provides the risk level.

It is common practice in this step to undertake a *first pass* review of all risks prior to considering existing controls and other risk treatments, to eliminate trivial and minor risks from further, detailed consideration.

Links with business continuity management

The consequences (business impacts) in a business continuity management context relate to business interruption (outage). In analysing identified risk events, management should consider whether each event could interrupt the normal course of business operations. Events which have a direct, detrimental effect on an organisation's resources (staff, facilities, telecommunications information systems) such as fire, power supply failure and fraud, are likely to have some business interruption consequences.

The analysis of consequences involves establishing evaluation criteria to guide management in forming a view on how significant a particular event is to the business. This is usually undertaken by establishing criteria on an escalating scale against impact areas. To aid in completeness of the analysis, these impact areas may be categorised as outputs, resources, reputation, compliance and business interruption.

For a risk event that has a business interruption consequence, the relevant evaluation criterion is the duration of the business interruption.

In the business continuity management process, a **maximum acceptable outage** is established for each key business process and resource. Where a risk event is likely to cause a business interruption that will exceed the time limits defined in the maximum acceptable outage, this is an *extreme* consequence and accordingly would receive the highest rating. Figure 5 illustrates the risk analysis process for risk events that have a business interruption consequence.

Whereas the likelihood of a risk event occurring is not part of the Business Continuity Plan, it is relevant at this stage when determining pro-active treatments and controls. The more likely an event is to occur, which will also have a major or severe impact, the more cost-effective preventative controls will need to be.

Figure 5—Consequence analysis of events with business interruption impacts

As part of the risk assessment process, a benefits payment service organisation identifies the unintentional deletion by its employees of client information as a risk event. Without this information it is unable to process new client applications, variations to client details, or pay its clients. It has a fortnightly payment cycle.

This event is recorded on an analysis sheet (extract below) and the various business impacts noted.

Benefits Payment Business Process (extract)

Business objective: pay benefits to bona fide clients only, on time and for the correct amount.

Analyse consequence of risk events (without considering controls)

	Business impact of event occurring						
Risk events	Outputs	Resources	Reputation	**Business Interruption**	Clients/ stakeholders	Compliance	Rating
Internal Risks							
Operational processes							
Incorrect classification of client benefit type				No impact			
Unintentional deletion of Client Master File records by staff	Does not achieve timeliness KPI of 99% payments on time	Extra staff and consultants costs to recover lost data estimated to be $500,000	Will require Ministerial explanation and likely to lead to questions in the Parliament	Minimum four weeks to reconstruct file from paper records	Unable to process client payments	No impact	5 - Extreme
Intentional deletion of Client Master File records				As above			
Employee fraud – bogus client created				No impact			

The risk event highlighted above forms a part of the internal risks to the organisation and relates to its operational processes. A number of other business impacts have been identified for this event in addition to the business interruption impact. The overall impact has been rated as *extreme* for this event. The consequence rating was determined by reference to the following evaluation criteria.

	Consequence evaluation criteria by impact area					
Rating	Outputs	Resources)	Reputation	**Business Interruption**	Clients/ stakeholders	Compliance
5 – Extreme	>10 per cent variance from KPI targets	Death of employee >$10 million 'loss'	Royal Commission	>2 weeks (ie. > MAO)	Death of client	Breach of Constitution
4 – Major				1 – 2 weeks		
3 – Moderate				< 1 week		
2 – Minor				< 1 day		
1 – Negligible				None		

The Maximum Acceptable Outage (MAO) for this information resource and business process was set at two weeks (Part Two of the Guide discusses how an MAO is set). The estimated time to reconstruct client records exceeds this duration- accordingly for this criterion an *Extreme* rating applies. Note that while other impacts from the event may achieve a lower rating, the highest rating overall should be used in the risk assessment process.

Risk treatment design

The final part of risk assessment is to design appropriate risk treatments. The treatment options available to an organisation range from accepting the risk (where it cannot otherwise be cost-effectively managed) to controlling the risk, and to transferring the risk.

In a two-stage approach to risk analysis, the risk level is first determined for all risks—which are then categorised between minor and major—before considering existing controls and treatments. The major risks are then evaluated in the context of existing controls and other risk treatments. Where the risk level remains unacceptable, notwithstanding existing controls and treatments, it is incumbent on management to design new controls or to consider other treatment options.

Links with business continuity management

Controls established by management to treat risks can be defined either as preventative (stop the risk event from occurring in the first place) or corrective (detect the risk event when it occurs and respond accordingly). Preventative controls operate primarily to reduce the likelihood of occurrence of a risk event, whereas corrective controls operate primarily to minimise the consequences once a risk event has occurred.

An example of a preventative control is the use of passwords to gain access to the information systems of an organisation. If correctly implemented, this control will prevent unauthorised access. An example of a corrective control is the review of a computer log of access attempts. If correctly implemented, this should detect any unauthorised access and highlight what information, if any, was altered.

In a business continuity management context, the organisation starts from the assumption that the preventative controls have failed, or there were no preventative controls in place, and a business interruption occurs. The organisation needs to respond to such events in proportion to their significance—matters of likelihood and root cause are therefore no longer relevant.

The organisation will need to determine what must be done, by whom, and at what time **after** a risk event has occurred that would otherwise lead to the organisation's resources or processes being adversely affected for a period in excess of the maximum acceptable outage.

It will also have to determine what needs to be done in advance of any outage so that its consequences can be mitigated. For example, most organisations 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.

Step three: implement treatments

This step of the risk management process requires organisations to establish a plan for implementing any new treatments, additional controls or modifications to existing controls arising from the risk assessment phase. It must then ensure that the implementation plan is executed by establishing responsibility and timeframes for any actions required and accountability for outcomes.

The Risk Management Standard recommends the following minimum documentation[2]:

- who has overall responsibility for the implementation of the plan;
- what resources are to be utilised;
- budget allocation;
- timetable for implementation; and
- details of mechanism and frequency of review of compliance with treatment plan.

Links with business continuity management

The Business Continuity Plan is a **risk treatment**. It **is not** the implementation plan referred to above. The implementation plan should include the need to establish a BCP if one does not already exist.

If the risk assessment process has functioned effectively, it will have identified controls and treatments that reduce the likelihood and consequences of all risk events, including business interruptions events, to an acceptable level.

The BCP is a corrective control that is activated only after a business interruption has occurred.

2 AS/NZ 4360:1999 Risk Management, see Appendix H

Step four: monitor and review

The objective of the final step in the risk management process is to monitor risks and the effectiveness of controls over time to ensure changing circumstances do not alter risk priorities or weaken the operation of controls.

Many organisations integrate risk assessment into their corporate and annual business planning processes. This ensures regular, periodic review of both strategic and operational risks.

Review of controls, to ensure they operate as management intended, has traditionally been the major role of the internal audit function. However, the major drawback is that it may lead operational managers to conclude that internal audit, not the operational manager, is responsible for the system of control.

To counteract this view, many organisations have implemented Corporate Governance programs that highlight manager's responsibilities for controls[3]. The use of control 'sign-offs' and the introduction of control self-assessment are two useful initiatives in this area.

Links with business continuity management

As with any other control, the BCP needs to be monitored and reviewed for effectiveness. This requires that it be tested regularly. It also requires that the impact of organisational changes or any other changes to circumstances be considered to ensure the plan maintains its currency.

3 The ANAO has published two Better Practice Guides discussing corporate governance and control relevant to this issue: *Better Practice Guide to Effective Control—Controlling Performance and Outcomes*, 1977 and *Corporate Governance in Commonwealth Authorities and Companies*, 1999.

Part Two

The business continuity process

Overview of the business continuity process

Step one: **Project initiation**

Step two: **Key business processes identification**
Establish key business processes
Rank key business processes
Determine activities that constitute each process
Match resources to activities

Step three: **Business impact analysis (BIA)**
Analysis of operational and financial impacts

Step four: **Design continuity treatments**
Identify and evaluate treatment options
Select alternate activities and resources

Step five: **Implement continuity treatments**
Implement preparatory controls
Prepare the Business Continuity Plan (BCP)

Step six: **Test and maintain the plan**
Test the plan
Maintain the plan

Overview of the business continuity process

As discussed in Part One of this Guide, business continuity management is an integral part of total risk management. The *top down* approach to risk management—which starts with business objectives and identifies risks; is complemented by the *bottom up* approach to business continuity—which starts with identification of resources and processes being affected by an outage.

Given their close inter-relationship, it is recommended that a BCP be developed in conjunction with the Risk Management Plan for the organisation.

This Part of the Guide deals with the steps required to produce the BCP and what needs to be done to ensure that it is properly maintained. There is a high degree of commonality between the steps described herein and those discussed in Part One—further reinforcing the need to undertake these steps as part of an overall risk management process. The similarity in steps also serves to highlight that it is not the process so much that differs in constructing a BCP but the underlying approach.

The steps in the business continuity management process are:

- initiate the project;
- identify key business processes;
- undertake a business impact analysis;
- design treatments;
- formulate a BCP; and
- test and maintain the BCP.

These steps are illustrated in Figure 6 and each step is discussed in detail in the remainder of this Part.

Figure 6—Overview of the business continuity management process

1. Project initiation ■ Document objectives, scope, boundaries ■ Establish management committee ■ Establish budget and timetable	**Project plan**	**Executive management involvement required**
2. Identify key business processes ■ Identify key business objectives ■ Identify key business outputs ■ Align business processes with key outputs ■ Understand key activities, resources and inter-dependencies	**Key activity and resource schedule**	**For key business processes only** ■ **Activities** ■ **Resources**
3. Undertake business impact analysis ■ Identify key personnel ■ Schedule and conduct interviews ■ Document concerns, priorities and expectations ■ Determine Maximum Acceptable Outage for each process	**'Maximum acceptable outage' schedule**	**Treatments designed to:** Prevent ■ Reduce liklihood ■ Reduce consequence Recover ■ Respond ■ Interim ■ Restore
4. Design continuity treatments ■ Review existing controls ■ Identify and evaluate options ■ Select alternative activities and resources ■ Implement treatments	**Risk treatment plan**	**Contents** ■ Cover page ■ Table of contents ■ Event log ■ Management plan ■ Service area plans ■ References ■ Technical items ■ Contact lists ■ Inventory ■ Limitations
5. Implement continuity treatments ■ Establish recovery teams ■ Document service area action steps ■ Establish event escalation process ■ Obtain contact and inventory lists ■ Document recovery management process	**Contracts with vendors, suppliers.** **Updates to policy and procedure manuals** **Business continuity plan**	
6. Test and maintain plan ■ Paper test ■ Manual verification ■ Supply validation ■ Supply, service & equipment availability ■ Stuctured walkthrough ■ Unannounced team assembly	**Test plan**	**Timing** ■ Annually

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

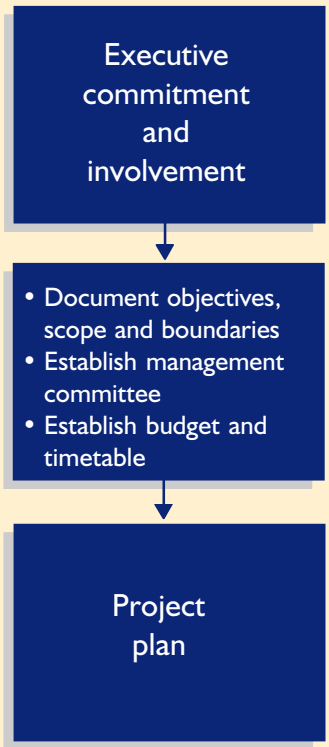
Step one: project initiation

A plan should be prepared documenting the objectives, scope, and boundaries of the business continuity planning project. The manager, or management committee, responsible for the project should approve the plan, including a budget. The plan need not be overly large or detailed, but needs to reflect the size and complexity of business continuity issues in the organisation.

Team roles and responsibilities should also be established, and relevant reference material or existing documentation collected at this stage.

Like most plans, the business continuity project plan should:

- continue to develop during the life of the project as more about the organisation and its risks is learned;
- be prepared by managers who understand the business and be approved prior to the commencement of work; and
- reflect the organisation's approach to risk management.



Checklist for the development of a business continuity project plan	
• Document the project's objectives	✔
• Define and document the project's scope and any limitations	✔
• Explain any assumptions made	✔
• Assign responsibility for project tasks	✔
• Present the budget, including staff resources, required for the project	✔
• Set project timeframes and deliverables for tasks	✔
• Plan is formally approved by Chief Executive and/or appropriate management committee	✔

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Case study

Ensuring the business continuity planning project was well-focussed and understood by all participants, a public statutory body developed a requirement specification document to outline the scope, tasks, deliverables and assistance for the project.

An example of this plan is in the Workbook at Step one (p. 6).

Step two: key business processes identification

The primary input to the Business Impact Analysis (BIA) in step three is a list which ranks the key business processes of the organisation—that is, those processes essential to the delivery of outputs and achieving business objectives.

Each key process is defined in terms of the activities undertaken and the resources consumed by those activities. A structured approach to this step requires organisations to:

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

Establish key business processes

It is important, in preparation for the BIA, that management has a clear and agreed understanding of the organisation's business objectives and outputs, and the key business processes which ensure these objectives are met and outputs are achieved.

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

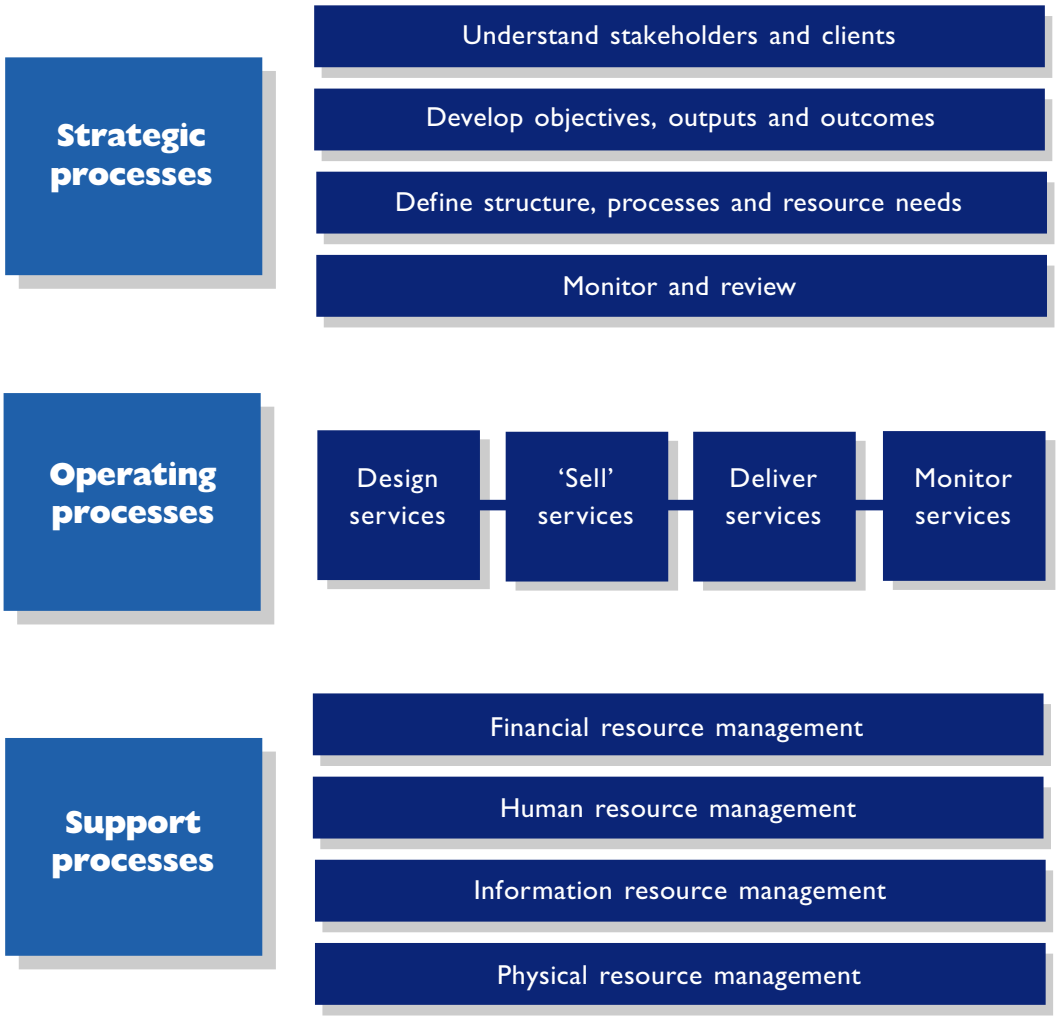
To assist in achieving consistency in terminology and common agreement in process definition, organisations may wish to utilise a business process classification scheme. Such schemes provide generic categorisations of business processes common to most organisations.

An example of such a scheme, applied to the public sector, is provided in Figure 7. This diagram outlines the 'mega' business processes categorised between strategic, operational and support processes. Within each *mega* process are a number of *major* business processes.

For example:

- ***Strategic processes***—*Monitor and review* would include internal audit, control and risk self-assessment, quality management programs, and program evaluation processes;
- ***Operational processes***—*Develop services* could include designing application forms for grants or establishing a call centre; *Sell services* could include processing client applications or claims; *Deliver services* could include formulation and provision of policy advice; and *Monitor services* could include grant acquittal processing; and
- ***Support processes***—*Financial resource management* includes purchasing and payments, payroll, costing, and budgeting and forecasting.

Figure 7—Example of a process classification scheme for Government organisations



This scheme is based on the 'Universal Process Classification Scheme' for the private sector developed by the American Productivity and Quality Centre in conjunction with Arthur Andersen, IBM, DEC and Xerox.

Rank key business processes

The key business processes need to be ranked in order of their importance to the organisation. This ranking should reflect the importance of the business process to achieving business objectives and delivering outputs. The ranking of key 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; and
- degree of dependency on business processes by internal business units or clients.

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

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

In a large organisation 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.

Determine activities that constitute each process

The business activities supporting key business processes then need to be identified. These are the activities that produce an output from the key business process.

These may be the activities of a single operational area in the organisation, or may be the activities of a number of operational areas, which combine to produce the output.

A thorough understanding of activities is essential to identify such inter-dependencies. Some activities may rely on the outputs from other activities from within the organisation (commonly referred to as *enabling* outputs), or even from outside the organisation. 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 inter-dependencies, 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.

Match resources to activities

The resources necessary for delivery of the key business processes also need to be identified. These are the resources required by the operational areas to support the activities that deliver the outputs or results. Without these resources, the business processes would not achieve their goals. Some resources to consider are:

- **people**—both the organisation's staff and people external to the organisation which may be critical to the success of the activity;
- **infrastructure**—buildings and other property used by the organisation to deliver its services and produce its outputs;
- **assets and supplies**—equipment and consumables which are used by the people and the processes as part of the activity; and
- **finance**—some activities require money to be available to make payments on time.

Checklist to ensure all key business processes, activities and resources are identified	
• Document and confirm organisational objectives and outputs	✔
• List key business processes that underpin achievement of objectives and delivery of outputs	✔
• Review the functional organisation chart to identify general areas of operational responsibility	✔
• Interview managers responsible for key business processes to confirm understanding of activities (complex organisation only)	✔
• Document the activities and resources essential to each key business process	✔
• Formally communicate the list of key business processes and supporting activities and resources to the project steering committee	✔

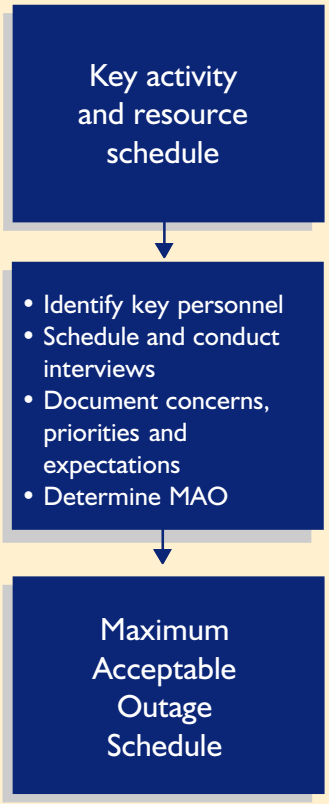
Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Example: interdependent activities and resources

A customer fault repair activity of a utility had a high business priority, given its impact on public image. The activity was dependent on a call centre as a customer interface and on the stores area for equipment. These areas were in turn dependent on the information technology infrastructure for customer detail, information transfer, progress tracking and stock level information.

Due to these interdependencies, the recovery timeframe for the call centre, stores and information technology were directly influenced by the recovery requirements of the fault repair activities.

Investigation of the stores turnover determined that the level of stock retained in the central and satellite stores was sufficient to continue activities for up to a week. This information resulted in a lower recovery priority for the stores activities and associated information technology processes.



Step three: business impact analysis (BIA)

By this step the information collated includes:

- documentation of key business processes;
- identification of the activities and resources critical to the key business processes;
- interdependencies within and between activities and resources; and
- a priority ranking of the processes, activities and resources which represents the organisation's agreed view.

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

From this, the maximum acceptable outage can be determined for the critical processes and resources. That is, how long can the key business process survive without the critical activity and/or resource before it will have a detrimental effect?

Analysis of operational and financial impacts

A series of *business impact analysis interviews* with the managers responsible for critical activities and resources will be the quickest way to undertake the analysis.

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

An approach founded on risk likelihood will fail to propose a treatment for highly unlikely events, despite their impact. For example, not to have a plan in place to relocate operations or recover from the loss of a building because *...that will never happen...* will leave the organisation floundering, possibly leading to its demise, should the *impossible* happen.

This aspect of risk management is about coping with events that are less likely, and have a major impact. Most effort in risk management, and justifiably so, is put into addressing risks with high likelihood and high impact—risk management models and methodologies devise and implement controls (or treatments) to eliminate or reduce the effect of these risks.

Where an event is unlikely, yet its impact is significant, it may not be feasible to treat the risk, but it is folly to ignore the risk. Treatments for each event need to be determined.

The real purpose of a business impact analysis is to identify those systems that when absent would create a danger to the enterprise's survival and to ensure those systems reveive the correct priority in the subsequent business continuity plan.
Business Continuity Planning: Creating a Business Impact Analysis, InSide GartnerGroup This Week (IGG), January 15, 1997, C. Gooding

The following checklist summarises the steps to be undertaken to complete the analysis and determine a maximum acceptable outage for each key activity and resource. Each step in the checklist is supported by guidance and schedules contained in the Business Impact Analysis (BIA) questionnaire which is in the Workbook (p. II)that accompanies this Guide.

Checklist for analysing each key business process	
• Evaluate the impacts of a loss of the process from the perspective of the organisation's budget and outcomes and outputs—consider: - loss of revenue/increased expense - service delivery standards - public or political embarrassment - loss of client confidence - loss of management control - financial misstatement - regulatory, statutory or contractual liability - specific/unique vulnerabilities, and - political ramifications	✔
• Identify the critical success factors that ensure the process meets the organisation's objectives	✔
• Identify additional expenses incurred if activities are performed manually or in a substitute manner during an outage	✔
• Identify interim processing procedures (alternative or manual processing) techniques to be adopted during the recovery phase	✔
• Estimate the time it will take to overcome the backlog of work accumulated during the outage	✔
• Quantify the minimum resource requirements necessary to perform the activity	✔
• Identify the records vital to the recovery process	✔
• Evaluate the adequacy of current BCP in place	✔

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Checkpoint: management sign-off

Obtain agreement from project committee/ project sponsor and chief executive regarding the MAO for each key process, critical activity and resource

Case studies

Small organisation

A small statutory body with 20 staff conducted a single workshop to determine the impacts of a disruption. The general manager and senior representatives from each activity attended the 2-hour workshop.

A 'disruption scenario' was presented with each of the participants describing the impact to their area at various timeframes. The participants were able to build on each other's analysis and a very clear picture of the impacts, interdependencies and recovery priorities was produced.

Medium-sized organisation

A state government body with around 150 employees conducted a series of workshops. Four 2-hour workshops were held which included a senior representative from each activity as well as management from underlying processes.

Given that the activities and processes were complex, it was necessary to spend extra time to determine the impacts, interdependencies and recovery priorities. An important extra step was also needed in this process in that all responses had to be compared to responses from other activities in order to limit any bias between the separate workshops. This often means revisiting business units or getting feedback from senior management.

Large organisation

A series of Business Impact Analysis interviews were conducted for a large and complex listed company with over 2000 employees. Due to the organisation's size, each business unit was examined separately, and in some cases processes within that business unit were reviewed separately.

The first series of interviews provided an understanding of the impacts from a loss of key activities and the interdependencies between the business units. Further interviews were then conducted with senior management to confirm the recovery priorities and maximum acceptable outage timeframes from an overall organisational perspective.

As per the medium organisation example, this approach also aided in limiting any bias that may have arisen between business units/interviewees.

Step four: design continuity treatments

This step identifies the treatments to address, and to minimise the effects of, disruptions to each critical business process for which an MAO has been established.

The treatment analysis identifies the requirements to ensure the continued availability of critical processes and resources during outages. These requirements are based on the rankings agreed in the BIA and provide:

- the basis for specifying and selecting alternate and redundant capacity to reduce likelihood or impact of an outage; and
- recovery and restoration requirements to be used if an outage occurs.

Recommendations for each service area are made based on the treatment options selected and, where identified, recommendations for improvement in business process to be implemented.

As part of this process, a review of vital records management and backup and recovery procedures must be undertaken. This will ensure records and data can be reconstructed following a disaster. Appendix 6 discusses the approach to quality review of the BCP, which includes evaluating backup processing and off-site storage. Appendix 9 provides checklists for review of off-site backup procedures

The outcome of the treatment analysis will form the basis of the business continuity plan.

Each phase of the treatment analysis is discussed in the following sections.

Identify and evaluate treatment options

For each of the key business processes identified and ranked in the BIA, there should be treatments that:

- reduce the exposure to, and impact of, loss of the processes and resources on which the functions rely; and
- implement alternate processes and resources to be used following an outage and plans to recover from the outage and restore normal operations.

Evaluating the options available to ensure the continuation of business will identify the alternate activities and resources to be used should an outage occur.

Variations to, or redesign of, existing activities and resources should be considered as a means of reducing the exposure to, or impact of, loss of a key business process.

In selecting alternate activities and/or resources, it is critical the following areas are addressed as part of the business continuity planning process in respect of

each identified disruption, regardless of the organisation's, objectives, size or complexity:

- people;
- facilities (including buildings and equipment);
- telecommunications;
- information systems; and
- business activities.

For all critical activities and resources, it is necessary to identify other arrangements that may be used in their place, should they be lost. From those identified, alternate activities and/or resources are chosen which allow that part of the business to continue with minimal disruption.

Alternate activities and resources may be a combination of different services or redundant capacity retained just in case (eg. hot, or cold, computer sites).

Checklist for evaluating activity and resource alternatives	
• Document a brief description of each viable option	✔
• Determine other resources required and the costs for each option (this may require information from vendors)	✔
• Compare recovery options to MAO:	
- Does the option meet the recovery needs?	✔
- Does the option exceed our needs?	✔

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

People

People are often overlooked as the most critical resource in ensuring continuity of business. The impact of an unexpected loss of key personnel, or a team, can have a significant impact on an organisation's business.

The impact of disruption on people should also be considered in isolation and as a resource that is interdependent with each of the areas below—facilities, telecommunications, information systems and business processes.

The business continuity plan needs to include treatments for people, which includes:

- approaches to communication;
- human resource issues, including short-term replacements and training;
- issues relating to the disaster event; and
- the psychological effects of the disruption on staff morale.

Example: treatment options for people

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

Facilities

The BCP should include treatments that concentrate on the most critical components of operations—usually people and their work environment. This segment addresses the physical environment (equipment and buildings) on which a business process depends.

Treatments should be developed for damage assessment, salvage and restoration of equipment and buildings. They should address the buildings in which the business process operates and the equipment and resources contained within those premises. The treatments should also aim to be developed to ensure timely restoration or relocation so the business process can be moved back to the restored premises or be relocated to new premises and continue essential business activities.

Arrangements and procedures for relocating facilities should be addressed. Additional issues to be addressed include:

- provision for backup processing services;
- agreements and activities required to transfer functions; and
- documented procedures to support business facility recovery and restoration.

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

Telecommunications

Communication is critical to continuity of business functions. The BCP should therefore include treatments that address recovery from loss or interruption of voice and data communications, both within and outside the organisation. In many organisations, voice networks are more critical than data networks.

Treatments that deal with communication loss can include:

- the 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 can be built into communications networks such as PABX and network systems which enable communications to be diverted to other locations if, and when, necessary;
- backup equipment and software which includes backing up PABX data, network software and acquiring necessary redundant equipment; and
- uninterruptible power supplies (UPS) and monitoring facilities which help prevent system loss during power failures.

Information systems

Information systems manage the organisations physical records (eg. correspondence, project and management files) and electronic records on computing facilities (eg. email, electronic policy and procedure manuals, forms and images), wherever they are housed.

The information systems treatments included in the BCP need to consider:

- 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); and
- off-site storage of critical data.

Preventative controls such as robust systems and application design, fault-tolerant hardware, uninterruptible power supplies, and monitoring facilities should also be considered. The result should be a complete and workable strategy for each part of the information process affected by identified disruptions.

Distributed handling and processing of information inherently spreads the business continuity risks across an organisation. However, as part of a comprehensive BCP, plans should be developed for each of these systems, and recognise any interdependencies between them (eg. single site of the management system).

Example: treatment options for facilities, telecommunications and systems

Treatments	Application
Purchase or lease redundant capacity	Pay for extra office space, IT infrastructure, communications, etc.
Contingency arrangements	Enter an agreement with an outside vendor to provide service in the event of an outage (ie. hot site, warm site, and cold site).
Mutually beneficial agreements	Enter into an agreement with another organisation to use part of their facilities in the event of a disaster. These types of agreements can be entered into with other organisations to achieve the other options (ie. purchasing a hot-site agreement together).

Business processes

As an outage may impact more that one business process, the treatments developed for each process need to be consolidated and, ultimately, individual business process plans are combined into an organisation-wide plan.

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

Business process treatments included in the BCP should address the activities and responsibilities of a business function to ensure continuity of essential business functions from the point of disruption to the return of normal operations.

Example: treatment options for business processes

Treatments	Application
Alter current arrangements	Often current processes and resources can be changed as a cost-effective solution. For example, splitting data processing between two offices. In the event of loss of one site, the other site is still functioning.
Alter current processes	Often a current (or even non-current) service provider would be willing to give a guaranteed level of service in a disaster situation to restore resources at minimal cost.

Select alternate 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, or a significant portion, of the costs until an event occurs and the continuity plan is activated. For example, restoration of essential phone communications maybe handled with the purchase of sufficient mobile phones when required, in the knowledge most carriers can provide them within hours. Agreements with vendors may be established to ensure timely delivery on demand at a set price.

The selected alternate processes and resources should be documented along with the rationale for their selection.

Case studies: alternate treatments

People

A statutory body had previously developed a Staff Communications Strategy outlining the methods to inform staff of events in the organisation. Following a review, it was determined that this strategy was suitable for a disaster situation and was incorporated in the BCP. By using policies already in place, the number of issues relating to people to be addressed was reduced.

Facilities

An organisation with a relatively large maximum acceptable outage determined there was no need to obtain facilities immediately following a disaster. It contacted a local real estate agent and asked it to maintain a list of suitable alternative office space, so that in the event of an outage this information could be easily obtained.

Telecommunications

A large public sector organisation had an agreement for supply of a Wide Area Network (WAN) with a large telecommunications provider. Their information systems recovery strategy suggested that they should move processing to their second office, however, the WAN to this location could not support the network traffic. Following consultation, the service provider agreed to provide extra bandwidth on a contingency basis to the second location at no cost.

In another example, and organisation defined its critical phone numbers, and the telecommunications provider agreed to switch these numbers to an alternative location immediately following an outage. This agreement was incorporated into the contract.

Case studies: alternate treatments (continued)

Information systems

An organisation with a maximum acceptable outage for information systems of five days, spoke to their current service provider who agreed to include as part of the maintenance/service contract a disaster recovery clause which stated that they would replace infrastructure within three days. This was obtained at no cost given that the organisation was an important customer of the service provider.

Step five: implement continuity treatments

Selection of continuity and recovery treatments will lead to:

- implementation of procedures to support recovery from a disruption to business; and
- documentation of the recovery arrangements.

Procedures implemented to support recovery will need to be both preparatory and reactive.

Preparing for recovery involves putting in place controls that will mitigate the consequences of a business interruption should it occur. Three of the most important such controls include back-up processes, records management, and formal contingency arrangements with external parties.

Documentation of the recovery arrangements to be implemented after an outage has occurred is the role of the Business Continuity Plan.

A series of checklists is included in the appendices to this Guide to assist with developing continuity treatments. The checklists cover:

- Alternate processing contract considerations (Appendix 1);
- Roles, responsibilities and a checklist for the Board and audit committee (Appendix 2);
- Roles, responsibilities and a checklist for the Chief Executive Officer (Appendix 3);
- Role and responsibilities of the Recovery Coordinator (Appendix 4);
- Roles and responsibilities of the service area recovery teams (Appendix 5);
- Checklists for quality assurance of BCP development (Appendix 6); and
- Limitations of BCPs (Appendix 7).

Implement preparatory controls

Back-up

Based on the results of the Business Impact Analysis, the resources required to recover and restore essential business processes are identified.

To activate a BCP it will be necessary to obtain access to information and resources supporting the key business functions. In the event of an outage it may still be possible to obtain these from the organisation's premises, but this will not always be the case.

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

Resources required for recovery such as documentation, forms, supplies, data and programs should be obtained (copies or backed-up in the case of electronic data) and be kept at a secure off-site facility.

Off-site storage facilities should have suitable environmental and security controls and the resources and information should be protected from unauthorised access modification, disruption or use during storage.

The following checklist describes the steps for evaluating off-site storage and back-up processing requirements.

Checklist for evaluating off-site storage and back-up processing	
• Ensure all resources required for the selected strategies are stored offsite	✔
• 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 there is adherance to procedures	✔
• Document key 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 Note: A better practice checklist for off-site storage is included in Appendix 9 to this Guide can be used as the basis for analysing issues with off-site backup processing	✔
• Schedule review of off-site storage facility. (complex organisation only)	✔
• Consider testing partial recovery from off-site facilities (complex)	✔

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Off-site storage procedures should be modified to align routine operational requirements with those identified in the recovery strategies to ensure resources stored off-site, and access to them, is available to meet both situations.

Records management

As part of the BIA, vital records supporting the critical business processes were identified. In order for these vital records to be properly restored it is necessary to ensure a suitable records management program is in place.

The impacts of not having proper document and data management treatments in place are many. They include the management of hardcopy and electronic records data as well as archiving policies for both forms of records.

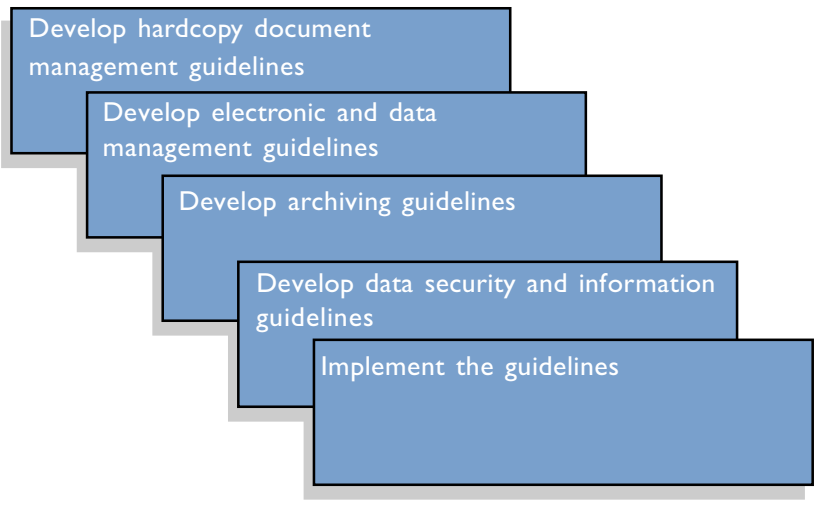
Continuity issues in record management extend beyond just keeping business processes in place. Record management has long-term implications for the organisation and strategies should consider:

- legal requirements and exposures;
- adverse affects on public image 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; and
- decision-making processes which will be affected.

Development and implementation of document management procedures should include the procedures necessary for management of both physical and electronic records.

Development of document management procedures is part of the organisation's overall information management strategy. Risks associated with information management should be addressed in the plans that underpin the strategy. Procedures can be broken into five parts:

Figure 8—Records management procedures



The *Australian Archives Handbook on Record Management*[4] says a good records management system will ensure:

- the right records are created;
- information is kept on who uses the records, why they are used and how they are manipulated;
- people who need the records can locate them;
- records are maintained in a useable format; and
- records are kept for as long as they are needed and for no longer.

The legal requirements to maintain records vary across organisations and should be considered in formulating a BCP. A good records management system will include consideration of the management of records vital to business continuity.

Checklist for assessing *vital* records management program	Current plan
• Does it provide a framework to ensure security of information developed?	Yes ❑ No ❑
• Does it establish a framework by ensuring integrity and completeness of information?	Yes ❑ No ❑
• Does it ensure only authorised personnel have access to information—including implementing a classification system?	Yes ❑ No ❑
• Does it ensure users of information are aware of and observe all relevant laws and regulations?	Yes ❑ No ❑

If the answer to any question is "No", that aspect of records management needs to be reviewed.

Case study

The Bankstown City Council fire was reported widely in the press for the impacts the disaster had on the Council and the community. The Council did not have a Business Continuity Plan.

The then Lord Mayor of Bankstown highlighted, that recovery of information technology systems was not, as some may have expected, a problem. There were sufficient backup and storage procedures in place, and it was not too difficult to reconstruct the information systems.

The biggest problem was that the fire burned a lot of vital records and historical artefacts beyond recovery and reconstruction. The lack of documented management procedures made recovery of information virtually impossible.

4 For this document and further information see the National Archives of Australia website http://www.naa.gov.au

Arrangements with external parties

It is necessary to formalise appropriate arrangements with vendor(s) selected as alternate suppliers.

The following checklist can be used to ensure such continuity treatments are properly implemented.

Checklist for evaluating implementation of external arrangements	
• Ensure for each treatment selected, the likely costs are the most commercially viable (ie. investigate other vendors in the marketplace)	✔
• Identify other requirements or changes that need to be made in order for the treatments to be effective	✔
• Changes to off-site storage procedures should be made as identified	✔
• Review contracts to ensure they demonstrate better practice for contract management as well as comply with internal guidelines for contract management	✔
• Finalise contracts	✔

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

A checklist to assist with consideration of alternate processing contract arrangements can be found at Appendix 1

Case study

An organisation had a maintenance agreement with a telecommunications provider. This organisation was only able to include a disaster recovery clause in their contract at a large additional cost. Another service provider offered to provide services with no additional cost for the disaster recovery clause. For this reason, the organisation did not renew its contract with its telecommunications service provider and changed to the more cost-effective provider that met their business continuity needs.

Prepare the Business Continuity Plan (BCP)

Business continuity plans are a compilation of individual recovery or contingency plans, brought together with an overarching management plan to coordinate the lower plans.

The BCP addresses business disruption from the initial disaster response to the point at which normal business operations are resumed. They may include disaster response plans that are service area specific, operational recovery plans, as well as restoration and transfer of operations plans and guidelines as appropriate.

The treatments to overcome identified disruptions need to address the stages necessary to complete recovery.

Figure 9—Stages in recovery of business operations.

Each phase is defined as follows:

- **Response:** the time from *disaster* declaration until critical systems and processes have been re-established using strategies documented in BCP.
- **Interim processing:** the period the organisation relies on alternate processes and resources.
- **Restoration:** the period the organisation returns from using alternate processes and resources back to use of its *usual* established systems and *business as usual*.

The business continuity plans produced should consist of detailed step-by-step procedures. They should contain action-oriented procedures to be used by recovery teams. These procedures are based on the approved recovery treatments and alternate activities and resources identified and take into account the recovery readiness procedures and arrangements.

Activities necessary to restore primary facilities and return to normal operations should be addressed more in the form of guidance than by detailed action steps which can quickly become dated an lack context.

To produce a comprehensive BCP the following steps are recommended:

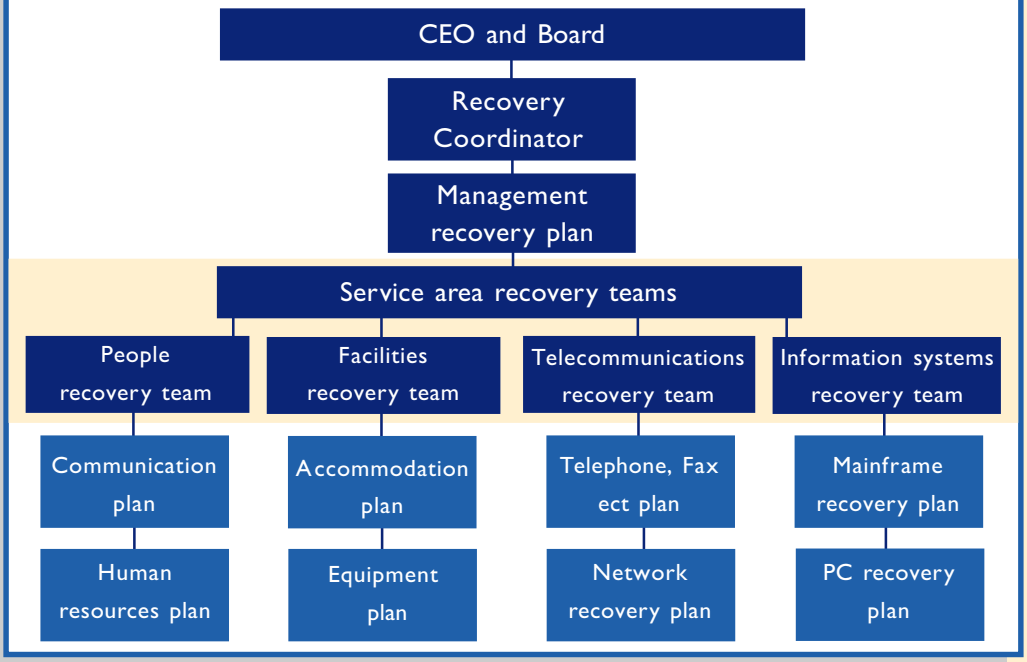
- define the recovery organisation;
- define the recovery team;
- develop and integrate *service area* recovery plans;
- develop the over-arching *management* recovery plan; and
- collate contact lists, inventory lists and other references.

The recovery organisation

Figure 10 provides a generic structure for the recovery organisation. The various layers in this structure are:

- Recovery coordinator—coordinates the various teams below and reports directly to the CEO and Executive.
- Recovery and management teams—service area teams responsible for implementation of BCP and recovery of systems following an incident.
- Recovery plan support processes—processes necessary to support the management and technical recovery plans including human resource management and communication.

Figure 10—A generic structure for the recovery organisation



For each recovery area, a team leader should be identified in the plan as being responsible for that area.

In a smaller organisation in may be possible to have only one person responsible for all communications, whereas in a larger organisation it may need to be split into its component parts.

Checklists to assist in defining the roles and responsibilities of the Board and CEO, can be found at Appendix 2 and Appendix 3, respectively

The roles and responsibilities of the Recovery Coordinator and the service area recovery teams, can be found at Appendix 4 and Appendix 5, respectively

It may also be the case that the executive wishes to take the ministerial and media communication/liaison role. It is important to ensure all service areas are sufficiently covered to ensure that responsibilities and workload are evenly spread.

Example: roles and responsibilities of key continuity players

Chief executive

- Brief Minister (and Board) on situation, expected impact and recovery timeframe
- Provide focal point for the organisation to ensure the media and public receive the correct, and non-contradictory information
- Ensure staff and stakeholders are made aware of the problems and the remedial action taken
- Ensure Recovery Coordinator and Recovery Teams have the resources and support necessary to do their jobs

Recovery coordinator

- Decision to activate the BCP
- Determine the recovery strategy for the given situation
- Assess the extent of damage to building, facilities and equipment and report to the CEO and/or Board; if necessary
- Contact the necessary staff required for the disaster (in the first instance)
- Assist in establishing of the recovery site, if applicable
- Coordinate media activities
- Direct, coordinate and monitor all recovery operations
- Convene recovery status meetings with the CEO
- Schedule subsequent recovery status meetings
- Liaise with real estate agent, if applicable
- Contact Insurance Assessors to determine their requirements and coordinate their on-going liaison with all recovery teams
- Minimise further losses and salvage recoverable resources
- Provide assurance and information updates to staff not involved in the recovery effort
- Prepare the recovery site

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Example: roles and responsibilities of key continuity players (continued)

Human resource team

Following notification from Recovery Coordinator of disaster escalation:

- contact the staff required for the human resource recovery team
- convene status meeting with team members
- continually assess and address human resource needs, liaising with other service areas, and
- provide regular updates to the Recovery Coordinator.

Communication teams

Following notification from Recovery Coordinator of disaster escalation:

- facilitate communication between recovery coordinator and the teams designated focus group
- convene status meeting with team members
- provide regular updates to Recovery Coordinator
- brief designated focus group on the disaster
- continually keep designated focus group informed of changes to what they have been informed, and
- respond to queries from designated focus group.

Other service areas

Following notification from Recovery Coordinator of disaster escalation:

- contact the necessary staff required to their particular service area
- convene disaster status meeting with team members
- assist with disaster assessment as required
- provide regular updates to Recovery Coordinator
- complete recovery plan for their service area
- determine requirements and coordinate acquisition of equipment, furniture, stationery and communications resources necessary for recovery, and
- liaise with other recovery teams.

The recovery teams

During recovery, a specialised organisational structure is established which varies from the organisation's structure during periods of normal operation. The roles in the *recovery organisation* need to ensure reporting lines and responsibilities are clear when the BCP is activated.

Small and non-complex organisations would only need one recovery team. Larger and complex organisations may need to consider a number of teams (constituted, for example, on a functional or geographical basis) which would be coordinated by a small management team.

Personnel need to be identified for the teams defined in the recovery strategy. The team members participate in customising their responsibilities and procedures and testing their recovery plan.

The make-up of the team may be based on consideration of an individual's personal characteristics as much as of their position within the organisation. Leaders and members of a recovery team need the following personal attributes:

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

Part of each BCP project should include a clear understanding of the human resource impacts and the issues to take into account in planning, implementing and testing.

Management and employees must understand, and be capable of carrying out, what is required of them in a contingency situation. As well, both groups must be aware of the possible disruptive consequences of some of their actions and inaction. This requires explicit communication and coordination through job descriptions, awareness programs, special training and testing of plans.

People need to be the major focus of an outage. Equipment, infrastructure and facilities may all be operational but if people cannot reach their work place, or perform their jobs, key business processes will cease.

People can be a major issue in successfully activating the contingency plan. For example, if the BCP calls for staff to pick up and move to another location, you may find that single parents and those incapacitated dependents, part-time students, people with second jobs, members of volunteer or paid public organisations, such as fire or emergency services, may not be available.

Service area recovery plans

An outline of the recovery plan should be developed for each service area identified in the recovery strategy. The plan should consider the people in the recovery teams and begin assigning individual responsibility for each action (ie. between team leaders, team members and other teams) as well as timing and expected outcomes for each action.

All the steps required for recovery of a business process must be documented in order of priority. The order of these steps should reflect the priority ranking for recovery and take into consideration any interdependencies between steps.

The recovery steps also need to consider issues reflecting interaction with other service areas and recovery teams.

Example: service area recovery plans

If the finance area recovery team relies on recovery of the information systems, and recovery of the information systems is the responsibility of another team—say, the information systems recovery team—the steps for recovery of the information systems are not part of the finance area recovery team's recovery plan.

The steps to recover the information systems are included in the information systems recovery team's recovery plan. The finance area recovery team's plan would merely make reference to the fact that the information systems must be recovered and that is the responsibility of the information systems recovery team.

Note: the person with responsibility for completion of a step in the recovery plan does not necessarily have to be the person who undertakes that step. While the recovery team leader is responsible for ensuring a task is completed, they may assign the step to the recovery team members.

A useful format for outlining service area recovery steps is:

No.	Action	Responsibility	Timing
1.	*<Action Title>* <Short description of action including references>	*<Team Member name>*	*<Due Date>* *<Resource estimate>*
2.			
3.			

As noted previously, the action steps should be considered in three parts.

It is usual to break each service area's recovery plan into these steps as a means of coordinating all plans.

Figure 11—Action steps in recovery plan

Note: at the end of each step in an actual recovery situation it is essential the Recovery Coordinator be briefed on the progress of the recovery effort. The next step should not commence until the previous step has been completed.

In establishing the recovery steps for each service area it is important that communications, including information flows, are fully effective. The following checklist outlines some key points to consider.

Checklist: adequacy of communication and information flows	Current plan
• Is the Recovery Coordinator kept adequately informed throughout the recovery process?	Yes ❑ No ❑
• Are the team members kept adequately informed of the recovery process?	Yes ❑ No ❑
• Are other interrelated teams kept properly informed of the recovery process?	Yes ❑ No ❑
• Are appropriate external parties/stakeholders kept informed (excluding those kept informed as part of the management plan) of the recovery process?	Yes ❑ No ❑
• Are external and internal parties that are part of the process informed up-front that their assistance may be called upon?	Yes ❑ No ❑
• Are human resource needs properly addressed?	Yes ❑ No ❑
• Is part of the recovery process the re-implementation of controls (physical, logical and environmental)?	Yes ❑ No ❑

If the answer to any of the above questions is "No", the recovery plan(s) should be reviewed and amended to ensure there will be adequate communication following an outage and during recovery of operations.

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

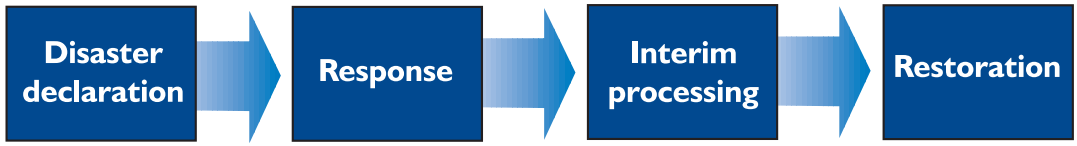
Following completion, it often becomes apparent that many of the recovery plans have some recovery steps in common. These steps should be integrated and assigned to one recovery team (usually that team which needs to complete that recovery step first). The other recovery teams should still include the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

The management recovery plan

The management recovery plan combines individual service area recovery plans into one coordinated effort. The recovery steps common to service areas should be combined into this plan (ie. inform staff of outage).

As well as combining the individual service area plans, the management recovery plan contains the criteria for activating the plan. Hence, the management recovery plan has an additional phase—*disaster escalation*. As shown in Figure 12, *disaster declaration* precedes the response to an outage.

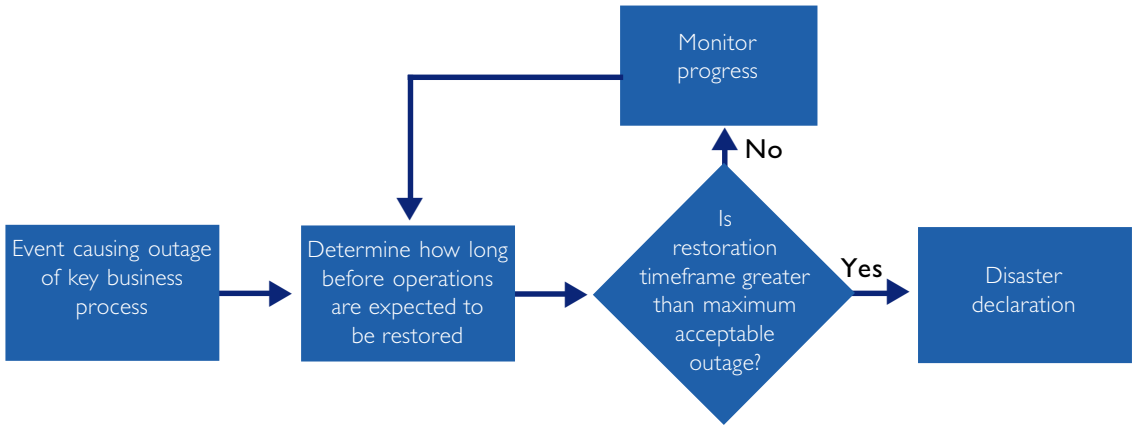
Figure 12—Disaster escalation



The management recovery plan should also address the issues to which the organisation, as a whole, must respond following the *disaster declaration.*

Declaration of a disaster is a generic decision, based on organisation-specific information—the decision process is shown in Figure 13.

Figure 13—Decision process for declaration of a disaster



Discussion: what constitutes a *disaster*?

As noted in Part One of this Guide an outage is not just an event that reduces the effectiveness of systems, but an event that is extraordinary, causes a loss of key business processes and has a high impact on the organisation. **A disaster is an outage that exceeds the MAO.**

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

It is possible for a management issue to turn into a continuity issue, if the issue begins to affect business processes. Continuing the court case example, if the pay-out created cash flow problems, this might interrupt business processes and lead to business continuity issues.

Individual components of the plan can be effectively utilised in non-disaster cases. For example, the communications plan might be effective in communicating an event to staff or the public, as may the information technology recovery plan may be effective in recovering a computer server that has failed.

The first step in the disaster declaration process is to determine how long it is before restoration of the business function can be expected. Guidelines to estimate the duration of an outage need to be established.

The following checklist may assist in establishing guidelines to estimate the duration of an outage.

Checklist: guidelines for estimating duration of an outage	Current plan
• Are the people involved in the disaster assessment process clearly identified?	Yes ❑ No ❑
• Are notification procedures for those involved in the disaster assessment process clearly identified?	Yes ❑ No ❑
• Are timeframes for the disaster assessment clearly identified?	Yes ❑ No ❑
• Are safety procedures for disaster assessment identified in line with Occupational Health and Safety Standards?	Yes ❑ No ❑
• Do outside parties need to be part of the disaster assessment?	Yes ❑ No ❑
• If yes, are they all identified?	Yes ❑ No ❑
• Are all relevant insurance companies appropriately informed of the incident before disaster assessment takes place (some insurance is void if certain disaster assessments are carried out without the insurance company present or without their knowledge)?	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Other details

There will be an array of other details to be included in the BCP. Each organisation should analyse their needs (ie. what information can't we do without?). The minimum recommended requirements are discussed below.

Event log

The management recovery plan should also log the events for later debriefing and review. An event log should be included which allows the recovery coordinator 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. For an example event log, see Appendix 8.

Contact lists

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

- emergency contact lists;
- recovery team contact lists;
- stakeholder contact lists;
- recovery participant contact lists; and
- complete staff lists with after hours contact details (if too large, details of where to locate a copy).

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. Consider modifying the existing internal directory to accommodate the extra details required. This will assist in keeping the details up to date and simplify the maintenance of lists.

Inventory list

An inventory of all materials needed for the BCP to be effective should be included as part of the plan, and the items stored offsite.

If inventory items have a limited life, normal operating procedures should include responsibility for review of stored inventory and replacement with fresh stores. In the case of consumables, this may become part of normal stores and distribution in the organisation.

Other references

Any other detailed references should be included. If this is not appropriate or practical, they should be included as part of the inventory and stored offsite. It may be possible to obtain and store much of this material electronically to save on space and possible degradation. However, recovery arrangements need to include arrangements to reprint paper versions when needed.

Format and contents of the BCP

The format and content of the BCP is extremely important. In a disaster situation, the reader should be able to pick up the document having not read it (although it is preferable that they have), and be presented with action-orientated points they can follow, with references contained in the back.

There should also be sufficient room for the person carrying out the recovery process to place comments on timing, or issues at each step. This will allow the recovery process to be critically reviewed as well as used as a source for debriefing staff on the issues that arose.

The BCP does not need to contain contextual information (eg. background, executive summaries, etc) as this was part of the development and approval process and should be stored on official files. The plan should simply start at the point the plan has been instigated and guide the reader through each step in the response and recovery process.

The example opposite illustrates a suggested structure for the BCP.

Quality assurance

Quality assurance reviews of the BCP during its preparation and throughout its life are recommended to ensure its content remains relevant. It is recommended the Recovery Coordinator and management committee responsible for the BCP ensure this is undertaken, in conjunction with routine testing.

A series of checklists is included at Appendix 6 to assist in the quality assurance of the BCP development

Checkpoint

Upon completion of the plan it must be reviewed and signed-off. A suggested list for review and signoff might include:

- internal audit
- audit committee
- BCP steering committee
- senior executives, and
- CEO

Example: suggested structure for a business continuity plan

Part		Information contained
1	Cover page	❑ Title ❑ Concise statement of objective of continuity plan ❑ Organisational signoff
2	Table of contents	❑ Contents of document
3	Event log	❑ Event log page to be filled in by Recovery Coordinator after an outage
4	Management recovery plan	❑ Disaster escalation process ❑ Team assembly arrangements ❑ Recovery phase steps ❑ Interim processing phase steps ❑ Restoration phase steps
5	Service area recovery plans	❑ Recovery phase steps ❑ Team assembly arrangements ❑ Interim processing phase steps ❑ Restoration phase steps
6	Referenced procedures	❑ Telephone re-direction procedures ❑ Outsourced vendor agreements
7	Technical recovery items	❑ Server configurations ❑ Communication configurations ❑ Pre-written programs for IT recovery
8	Contact lists	❑ Internal contact lists ❑ Emergency services contact lists ❑ External/stakeholder contact lists ❑ Staff contact lists
9	Inventory	❑ Supply inventory ❑ Additional resources/budget required
10	Limitations	❑ Limitations under which the plan was developed (refer Appendix 7 for an example set of limitations)
11	Testing and maintenance	❑ Schedule of testing to be performed ❑ Review/update timetables and deadlines (refer to step 6 for information on testing and maintenance)

Regular testing is necessary to maximize the chances of a successful plan in the event of a disaster and should familiarize the [Information System] organization with an unexpected interruption of critical applications — A business continuity plan is only as useful as effective testing proves it to be.
Business Continuity Planning: Maintaining Good Testing Practices, InSide GartnerGroup This Week (IGG), January 22, 1997, C. Gooding.

Step six: test and maintain the plan

Review of the BCP is essential to ensure it reflects the organisation's objectives, its key business functions, the corresponding processes and resources and an agreed priority for recovery. Testing and maintenance of the recovery process documented in the BCP will provide management assurance that the plan is effective—that is, it will ensure continuity of business should key functions be lost.

Test the plan

No matter how well designed and thought-out the BCP may seem, realistic and robust testing will reveal areas requiring attention. If test results are flawless, you should examine the adequacy and realism of your tests.

The major components of the BCP should be tested annually and updated based on the results of each test. It is important each component be individually tested. Testing can be disruptive—it requires commitment from management to ensure sufficient resources are available.

It is not recommended the BCP be tested as a whole as this would be resource intensive and may affect normal operations. It has been the case that testing the whole BCP at once, has itself created an outage and major disruption to business.

The service area recovery and management recovery parts of the BCP should be tested together. An approach may be to set the scene at the first hour, the first day, to the point of access to a temporary site. Each recovery team explains the process they would go through in recovering their operations.

The other teams challenge the approach and point out 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?"

There are several approaches that may be adopted to test the plan.

Paper—ensures there is adequate capacity and availability of resources when the BCP is activated.

The test requires calculating requirements such as floor space, air conditioning and power requirements for the equipment to be used when the BCP is activated.

Manual verification—ensures the required recovery material is available as stated in the BCP.

This test requires checking all required data, supplies and/or other hardcopy documents (as documented in the BCP) are actually backed up and correctly stored off-site.

Supply validation—validates all supplies required will be available in the event of a disaster.

The test compares the list of forms and supplies used during a test to the items documented in the BCP to ensure the list is complete and that an adequate supply will be available.

Supplies, equipment and services availability test—ensures information and lists of the forms, supplies, equipment, inventories and associated vendor contact details are accurate.

To conduct this test, one or more teams with critical support vendors would contact each vendor on their list to ensure that all information is accurate including phone number, address and key vendor contracts. They would verify whether the listed supplies, equipment or services are available for delivery or what the current lead time is. This lead time should be compared to the expected lead time in the BCP.

Structured walk-through—ensures the BCP procedures are adequate.

The test requires the Recovery Coordinator to develop a disaster scenario and lead the service teams through a mock recovery.

The test is conducted as follows:

- all team leaders meet in a room to be given the scenario;
- they each work through their recovery team plans paying particular attention to the interaction with other teams; and
- issues identified should be immediately noted by the Recovery Coordinator.

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 test is conducted as follows:

- The Recovery Coordinator contacts number of team members on the notification contract list.
- The tests should be conducted, on a rotating basis, at the following times:
  - during normal work hours;
  - during lunch time;
  - after normal work hours on a weekday; and
  - during the weekend.
- The Recovery Coordinator notes the time the calling process starts and the time at which each team member was contacted.
- Team members do not actually need to assemble.
- The Recovery Coordinator will report on the test results.

Maintain the plan

Individual recovery team plans must be *continually* maintained to provide support for business continuity. Administrative procedures and guidelines should be developed to provide for periodic testing and documentation maintenance of the service area recover plan(s) and ongoing training. Responsibilities for various aspects of BCP maintenance are also established.

Ongoing responsibilities should be defined to ensure appropriate BCP maintenance. The following groups have specific BCP maintenance responsibilities:

Role	Responsibilities
Recovery Coordinator manages the BCP, coordinates the recovery teams and liaises with the CEO and Executive	At regular intervals (eg at least six monthly): • Maintain alternate processing site contracts/agreements • Coordinate regular review of the BCP documentation, annually at a minimum • Coordinate review and approval of changes to the BCP • Coordinate BCP training • Perform administrative aspects of updates to the BCP (ie. reproduction and redistribution) • Maintain the BCP distribution lists • Schedule and coordinate the BCP tests
Recovery teams responsible for undertaking steps documented in the BCP to recover identified systems	At regular intervals (eg at least annually): • Maintain respective service area team procedures • Maintain the reference information that is part of the service areas' BCP procedures • Participate in BCP testing
End Users need to ensure they are aware of the contents of BCP and how it affects them	End users should: • ensure information necessary to continue critical functions, for which they are responsible, is stored offsite as part of the BCP • participate in contingency plan training • participate in contingency plan testing

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

A BCP is easily maintained if changes in the business and/or data processing environment initiate reviews and update the BCP.

When any component of the BCP is affected, the following steps should be taken:

- the Recovery Coordinator should be notified of the change;
- the effect of the change should be evaluated using a BIA focussing on the new component(s) and any new interrelationships which occur;
- the BCP should be modified by the appropriate service area to reflect the change; and
- the Recovery Coordinator should determine testing requirements and schedule a test, if necessary.

Appendices

Appendix I

Alternate processing service contract considerations

Checklist: alternate processing service contract considerations

Task	Completed
General Issues	
The description of the alternate processing facilities should indicate adequate physical security and appropriate environmental controls	Yes ❑ No ❑
Availability of alternate vendor sites and the rights of individual subscribers in the event of multiple disaster declarations should be specified	Yes ❑ No ❑
Amount of nature of support services the vendor will provide should be defined relative to: • implementation assistance • support for testing • logistical support, and • after hours support	Yes ❑ No ❑
The vendor should have limits relative to the total number of clients that may subscribe to any given facility	Yes ❑ No ❑
The vendor cannot renew (except by automatic renewal clause) or renegotiate the contract while the subscriber is experiencing a disaster or in recovery phase	Yes ❑ No ❑
The amount and scheduling of test time should be defined	Yes ❑ No ❑
Subscriber should have the right to periodically audit the installation to ensure that the specified configuration is maintained	Yes ❑ No ❑
An escape clause should allow the subscriber to terminate the contract without penalty for any of the following reasons: • failure to maintain technical compatibility • failure to provide agreed support services • failure to maintain suitable environmental support, and • any breach of contract	Yes ❑ No ❑
The contract should provide an annual window of opportunity to terminate without penalty	Yes ❑ No ❑
The monthly fees should not be subject to change without the written consent of the subscriber	Yes ❑ No ❑
The contract should not be assignable without written consent	Yes ❑ No ❑
The vendor should be subject to appropriate consider non-disclosure conditions	Yes ❑ No ❑

Checklist: alternate processing service contract considerations (continued)

Task	Completed
IT Recovery Specific Issues	
Definition of the backup capability of the vendor site should be clear and consistent throughout the contract	Yes ❑ No ❑
Occupation of the hot site for a minimum of six weeks	Yes ❑ No ❑
Conditions under which the subscriber can continue to occupy hot site facilities after the six week period should be defined	Yes ❑ No ❑
The number and description/type of locally attached terminals and/or other devices available while on-site should be defined; this is particularly important for data entry requirements	Yes ❑ No ❑
Continuing technical compatibility should be assured throughout the life of the contract	Yes ❑ No ❑
The contract should specify a guarantee of access to the hot site (including after hours access) during period of disaster and recovery	Yes ❑ No ❑
The nature and extent of IT support services to be provided by the vendor has been defined relative to: • network diagnostic capabilities and implementation assistance • support for testing activities • assistance in configuring facilities (ie. equipment acquisition, transportation, storage, removal and return) • access and use of vendor software, documentation, ancillary facilities (ie. photocopying, food services), and • logistical support.	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Appendix 2

Roles, responsibilities and a checklist for the Board and audit committee

Roles and responsibilities
• Ensure governance framework supports business continuity
• Ensure approach to risk management support strategic goals of organisation

Task	Completed
Is the scope of the business continuity process appropriate given the organisation's circumstances and risk management strategy?	Yes ❑ No ❑
Is BCP properly coordinated to take into consideration other risk management initiatives?	Yes ❑ No ❑
Are synergies between other risk management initiatives (ie. Y2K projects) and business continuity fully used?	Yes ❑ No ❑
Are internal and external audit recommendations regarding BCP properly followed up?	Yes ❑ No ❑
Are the maximum acceptable outages (MAO) determined as part of the business impact analysis in line with the audit committee's understanding of the business?	Yes ❑ No ❑
Are the recovery strategies recommended appropriate given other business initiatives?	Yes ❑ No ❑
As part of the review of the internal audit strategic and annual work plans is business continuity and more specifically, business continuity testing and maintenance properly addressed?	Yes ❑ No ❑
Are business continuity initiatives properly communicated to all levels of management and across the organisation (this is an important part of any successful business continuity project)?	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Appendix 3

Roles, responsibilities and a checklist for the Chief Executive Officer

Roles and responsibilities
• Brief Minister and Executive Board on business interruption event, expected impact and recovery timeframe • Provide a focal point for the organisation to ensure the public and media receive the correct, and non-contradictory information • Ensure staff and stakeholders are made aware of the problems • Ensure Recovery Coordinator and Recovery Teams have the resources and support necessary to do their job

Task	Completed
Have management and staff adopted an attitude of continuity management planning which ensures that a positive control environment is maintained?	Yes ❑ No ❑
Does the organisation regularly communicate the organisation's vision, goals and objectives to staff members?	Yes ❑ No ❑
Does management take a balanced approach to risk taking, carefully analysing and assessing risks and potential benefits before authorising new ventures or significant changes?	Yes ❑ No ❑
Does the BCP complement the organisation's corporate governance and risk management framework?	Yes ❑ No ❑
Is the organisation responsible for providing a unique service to the public or the Government?	Yes ❑ No ❑
If yes, what would the implications be if the service were unavailable for an extended period of time?	Yes ❑ No ❑
Are BCP practices and procedures in place to ensure timely decision making during a disaster and to instil accountability into staff?	Yes ❑ No ❑
Does a business impact analysis exist that identifies the recovery timeframes of the critical business processes?	Yes ❑ No ❑
Does the organisation have a person identified that is responsible for BCP?	Yes ❑ No ❑
If so, has the person been provided with adequate training and resources to perform the role?	Yes ❑ No ❑
Has the organisation's BCP been subject to independent review (eg. by internal audit)?	Yes ❑ No ❑
Are the BCPs linked to the emergency management plans for the organisation?	Yes ❑ No ❑

Task (continued)	Completed
Is there a process in place for BCP review?	Yes ❑ No ❑
If the organisation has a BCP, does it reflect the current and future needs of the organisation?	Yes ❑ No ❑
Have the current and future BCP needs been formally evaluated as part of the organisation's overall corporate governance arrangements?	Yes ❑ No ❑
Has the organisation undergone considerable organisational change, or changes in organisational focus and direction or changes to business resources (personnel, facilities, information technology, and communication)?	Yes ❑ No ❑
When were the continuity plans last tested?	Date: __/__/__
What were the results of the tests?	
Were recommendations for change or improvement taken up and tested?	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Appendix 4

Role and responsibilities of the Recovery Coordinator

- Decision to activate the BCP
- Determine the recovery strategy for the given situation
- Assess the extent of damage to building, facilities and equipment and report to the CEO, Executive and/or Board; if necessary
- Contact the necessary staff required for the disaster (in the first instance)
- Assist in establishing of the recovery site, if applicable
- Coordinate media activities
- Direct, coordinate and monitor all recovery operations
- Convene recovery status meetings with the Executive
- Schedule subsequent recovery status meetings
- Liaise with real estate agent, if applicable
- Contact Insurance Assessors to determine their requirements and coordinate their on-going liaison with all recovery teams
- Minimise further losses and salvage recoverable resources
- Provide assurance and information updates to staff not involved in the recovery effort
- Prepare the recovery site
- Schedule and conduct test of the BCP

Appendix 5

Roles and responsibilities of the service area recovery teams

Human resource management team	Following notification from Recovery Coordinator of disaster escalation: • contact the staff required for the human resource recovery team • convene status meeting with team members • continually assess and address human resource needs, liaising with other service areas, and • provide regular updates to the Recovery Coordinator.
Communications team	Following notification from Recovery Coordinator of disaster escalation: • facilitate communication between recovery coordinator and the teams designated focus group • convene status meeting with team members • provide regular updates to Recovery Coordinator • brief designated focus group on the disaster • continually keep designated focus group informed of changes to what they have been informed, and • respond to queries from designated focus group.
Other service areas	Following notification from Recovery Coordinator of disaster escalation: • contact the necessary staff required for their particular service area • convene disaster status meeting with team members • assist with disaster assessment as required • provide regular updates to Recovery Coordinator • complete recovery plan for their service area • determine requirements and coordinate acquisition of equipment, furniture, stationery and communications resources necessary for recovery, and • liaise with other recovery teams.

Appendix 6

Checklists for quality assurance of BCP development

The BCP plan proposal

The business continuity project plan should adequately describe the project, its objective and scope, the project team and its responsibilities, and the resources required. The Chief Executive or management committee responsible should formally approve the plan. The checklist below, provides a quick reference point for ensuring the plan has sufficient detail. In addition, a suggested format for a project plan is described at Step one of the Workbook.

Checklist: developing the business continuity project plan

Task	Completed
Document the project's objectives	Yes ❑ No ❑
Define and document the project's scope and any limitations	Yes ❑ No ❑
Explain any assumptions made	Yes ❑ No ❑
Detail members of project team	Yes ❑ No ❑
Assign responsibility for project tasks	Yes ❑ No ❑
Present the budget, including staff resources, required for the project	Yes ❑ No ❑
Set project timeframes and deliverables for tasks	Yes ❑ No ❑
Plan is formally approved by appropriate management committee	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Identifying key business processes, activities and resources

The BIA needs to assess the impact of an outage to all key business processes. It ranks these processes in order, to determine recovery priorities and identifies the activities and resources which comprise each process, again, ranked in order of priority to determine recovery priorities.

To ensure the BIA is complete each business unit or service area needs to identify the processes for which they are responsible and then determine which of these are critical to the organisation achieving its objectives. These key business processes should then be ranked in order priority to the business (thus indicating their recovery priority) and the activities and resources of each process should be similarly ranked.

Checklist: ensuring all key business functions, processes and resources are identified and included in the BIA

Task	Completed
Document and confirm organisational objectives, outputs and performance criteria	Yes ❑ No ❑
List all business processes which underpin achievement of objectives and delivery of outputs	Yes ❑ No ❑
Rank the processes in order of importance to the organisation's objectives and exclude those processes considered not key to achieving the objectives	Yes ❑ No ❑
Review the functional organisation chart to identify general areas of operational responsibility	Yes ❑ No ❑
Interview managers responsible for key business functions to confirm understanding of business processes	Yes ❑ No ❑
Meet with service area management and support personnel to gain an understanding of each function included in the scope	Yes ❑ No ❑
Obtain any supporting documentation that is available which would provide a summary of key business functions	Yes ❑ No ❑
Document the activities and resources essential to each key business process. Ensure all resources groups are identified (ie. people, facilities, telecommunications, information systems, business support processes)	Yes ❑ No ❑ Yes ❑ No ❑
Formally communicate the list of key business processes and supporting processes and resources, with their respective ranking, to the project steering committee	Yes ❑ No ❑
Consider interdependencies that exist between areas	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

The BIA

The BIA determines the length of time the organisation can be without key business processes before remedial action must be taken. As the key business processes are made up of activities and resources, it is actually about making an assessment about the time you can be without the activities or resources before the key business process would fail. The BIA establishes the Maximum Acceptable Outage for each activity and resource that supports the key business process—the MAO should reflect and confirm the priority ranking made in the earlier step.

Checklist: analysing each key business function for a BIA

Task	Completed
Evaluate the impacts of a loss of the function from the perspective of the organisation's budget and outcomes and outputs—consider: • loss of revenue/increased expense • service delivery standards • public or political embarrassment • loss of client confidence • loss of management control • financial misstatement • regulatory, statutory or contractual liability • specific/unique vulnerabilities, and • political ramifications	Yes ❑ No ❑
Identify the critical success factors that ensure the function meets the organisations objectives	Yes ❑ No ❑
Identify the processes and resources which underpin the key business functions	Yes ❑ No ❑
Identify additional expenses incurred if process(es) are performed manually or in a substitute manner during an outage	Yes ❑ No ❑
Identify interim processing procedures (alternative or manual processing) techniques to be adopted during the recovery phase	Yes ❑ No ❑
Estimate the time it will take to overcome the backlog of work accumulated during the outage	Yes ❑ No ❑
Quantify the minimum resource requirements necessary to perform the function	Yes ❑ No ❑
Identify the records vital to the recovery process	Yes ❑ No ❑
Evaluate the adequacy of current BCP in place	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Selecting alternate activities and resources

To select alternate activities and resources to be used during an outage, consideration of all viable options is paramount. This consideration encompass each options ability to substitute for the lost activities and resources in terms of cost, quality and, most importantly (considering the MAO) timeliness. An added benefit of this process it that it may identify better activities and resources than those currently in place, providing on-going cost savings as an outcome of this process.

Checklist: selecting process and resources alternatives

Task	Completed
Document a brief description of each viable option	Yes ❑ No ❑
Determine other resources required and the costs for each option (this may require information from vendors)	Yes ❑ No ❑
Compare recovery options, including cost, with recovery priorities and the MAO. Consider:	
• Does the option meet the recovery needs?	Yes ❑ No ❑
• Does the option exceed our needs?	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Evaluating backup processing and off-site storage

For a BCP to work, and work reliably, some proactive measures will need to be established to ensure relevant resources are available if the BCP is activated. Fundamental to recovery from an outage is access to record and information—both electronic and physical. Backup processing and off-site storage are fundamental to most business processes today—the checklist below provides a list of issues to consider when reviewing the requirements for the BCP

Checklist: evaluating backup processing and off-site storage

Task	Completed
Ensure all resources required for the selected strategies are stored offsite	Yes ❑ No ❑
Review documented off-site backup processing standards and procedures, if they exist. If standards and procedures do not exist, ensure they are developed	Yes ❑ No ❑
Interview personnel responsible for implementation of backup procedures to see if procedures are being adhered to	Yes ❑ No ❑
Document key elements of the off-site backup procedures for inclusion in the appropriate sections of the contingency plan	Yes ❑ No ❑
Analyse off-site backup processing procedures and document concerns	Yes ❑ No ❑
Schedule review of off-site storage facility	Yes ❑ No ❑
Partial recovery from off-site facilities has been tested	Yes ❑ No ❑

Note: A better practice checklist for off-site storage is included in Appendix 9. This can be used as the basis for analysing issues with off-site backup processing.

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Implementing continuity strategies

It is essential that the selected continuity strategies are implemented properly and tested. The BCP will rely on the selected continuity strategies being in place prior to finalisation of the BCP. The checklist below will provided assistance in ensuring the identified continuity strategies have been implemented.

Checklist: ensuring continuity strategies are properly implemented

Task	Completed
Ensure for each strategy selected, the likely costs are the most commercially viable (ie. investigate other vendors in the marketplace)	Yes ❑ No ❑
Identify other requirements or changes that need to be made in order for the strategies to be effective	Yes ❑ No ❑
Changes to off-site storage procedures should be made as identified	Yes ❑ No ❑
Review contracts to ensure they demonstrate better practice for contract management as well as comply with internal guidelines for contract management	Yes ❑ No ❑
Finalise contracts	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Evaluating the level of communication in the BCP

When activated, the success of a BCP will rely heavily on open communication and sharing of relevant information. Following declaration of a disaster, information on implementation of alternate activities and resources, recovery of lost systems and the next stage of the plan to be implemented, needs to be concurrently available to all recovery teams, senior management and affected staff. The following checklist can be used to ensure the communication in the service area plans and the management plan is adequate.

Checklist: ensuring communications and information flows in service area recovery plans are adequate

Task	Completed
Ensure the BCP has communication flows which the enable the Recovery Coordinator to be kept adequately informed by the service area recovery teams throughout the recovery process	Yes ❑ No ❑
The BCP ensures service area recovery team members are kept adequately informed of where the organisations is in the recovery process	Yes ❑ No ❑
Ensure service area recover team working to recover interrelated business processes are kept properly informed of the recovery process and keep other team informed of their progress	Yes ❑ No ❑
Ensure 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	Yes ❑ No ❑
Ensure external and internal parties included in BCP are informed immediately that their assistance may be called upon	Yes ❑ No ❑
Ensure all human resource needs are properly addressed. Consider: OHS, counselling and other support lines of communication, etc	Yes ❑ No ❑
Ensure the recovery process addresses re-implementation of routine controls (physical, logical and environmental)	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Checklist: ensuring communications and information flows in the management plan is adequate

Task	Completed
Ensure the BCP communication flows keep underlying service area recovery teams informed throughout the process	Yes ❑ No ❑
Ensure the executive is kept properly informed throughout the process	Yes ❑ No ❑
Ensure are appropriate external parties/stakeholders are kept properly informed throughout the process	Yes ❑ No ❑
Ensure the BCP provides specific protocols for media liaison and management	Yes ❑ No ❑
Ensure external and internal parties included in BCP are informed immediately that their assistance may be called upon	Yes ❑ No ❑
Ensure all human resource needs properly addressed. Consider: OHS, counselling and other support, lines of communication, etc	Yes ❑ No ❑
Ensure the recovery process addresses re-implementation of routine controls (physical, logical and environmental)	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Disaster assessment

The BCP need to outline the steps and issues that need to be considered when assessing the impact of a disaster. The Recovery Coordinator must be able to advise the Chief Executive and senior management on the impact of an outage and assess the time the business process may be affected—**if the MAO is exceeded, a *disaster* is declared and the BCP is activated.**

Checklist: developing the disaster assessment guidelines

Task	Completed
The BCP clearly identifies the people involved in the disaster assessment	Yes ❑ No ❑
The notification process for those involved in the disaster assessment is clearly identified in the BCP	Yes ❑ No ❑
The timeframes for the disaster assessment are clearly identified in the BCP	Yes ❑ No ❑
Safety procedures for disaster assessment identified in the BCP are in line with Occupational Health and Safety requirements	Yes ❑ No ❑
The outside parties which are part of the disaster assessment process are identified in the BCP along with their contact details	Yes ❑ No ❑
Steps are in place to inform all relevant insurance companies are appropriately informed of the incident before or during the disaster assessment taking place (some insurance is void if certain disaster assessments are carried out without the insurance company present or without their knowledge)	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Appendix 7

Limitations of BCPs

The BCP should recognise the factors that may limit recovery from a business interruption event. These factors should be documented in the BCP to ensure they are brought to attention of management.

Example: factors which may limit recovery from a business interruption event

Resource	Possible limiting factors
People	• Insufficient number of personnel possessing the appropriate skills available to implement business continuity operations • Critical operations and systems documentation for each platform are not stored off-site • Insufficient number of qualified personnel will be available to perform user tasks during the recovery phase • Personnel who play a role in recovery are unaware of their responsibilities and have not been adequately trained to perform the recovery tasks • Staff support areas are not prepared to support the recovery operation
Facilities	• The Recovery Plan will NOT cover any event which simultaneously renders both the primary and all alternate data centre facilities inoperable • The Recovery Plan will NOT cover any event which simultaneously renders the data centre inoperable and the essential off-site storage inaccessible • The disaster that renders the data centre inoperable may impact large geographic areas, public utilities, the transportation infrastructure or other facilities and/or services ordinarily available (Note that this excludes an electrical distribution failure) • 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 allowable outage period • Periodic testing of the BCP not is conducted • Critical systems are not periodically evaluated and their minimum essential features can not be provided for a disaster • A complete listing of production files and their location on backup tapes is rotated off-site with adequate frequency • The organisation may experience voluntary or involuntary separations of employment or relationship with any employees, suppliers, or other vendors between the occurrence of the disaster event and complete recovery • Off-site storage locations are not intact and accessible • Off-site information backup and rotation procedures are inadequate to implement full recovery within maximum allowable outage time frames • Daily transactions needed to reconstruct critical data are not rotated off-site with adequate frequency

Example: factors which may limit recovery from a business interruption event (continued)

Resource	Possible limiting factors
Telecommunications	• Ready access to public network • Untimely access to replacement mobile phones • Delay in re-routing critical phones number to new location • Lack of access to other communications hardware (eg. pagers, fax, email connections, etc.)
Information Systems	• Lack of alternate processing facilities available as and when, required • The organisation lacks access to a fully configured second processing site sufficient in capacity to support data processing for essential business functions with critical application support needs • Critical users do not have the ability to reconstruct any lost work-in-progress • Critical users do not have recovery plans developed to be able to process at the alternate processing facility
Business Processes and Resources	• The organisation has adequate financial resources to implement the contingency plan according to the time frames established by the business impact analysis • Inadequate maintenance of all business continuity procedures is performed • No ongoing effort to minimise exposures to disasters will continue and operations/ systems vulnerabilities • Designated user representatives are not promptly notified if a disaster occurs

Appendix 8

Event log

During a business interruption event it is important to record important information and decisions which were made during the outage. This information provides an important input to revising the BCP by incorporating actual event experiences in the plan. The event log may also be a useful tool for the Recovery Coordinator to use during BCP tests to record the scenario set and the outcomes of the test results.

The Recovery Coordinator should complete this Event Description shortly after notification of a disaster. The form is used to record the facts and wording of the disaster declaration statement to allow the Recovery Coordinator to relay accurate information to other members of the team and as a means of review after the event.

The following example shows the information the Recovery Coordinator should collect in the case of a business interruption event.

This form should be adapted to suit the specific requirements and structure of the organisation.

Example: a business interruption event log

Event Log:	
Initial Notification: Disaster Declared ❑ or Standby Requested ❑ ? (Please Tick)	**Briefly describe the event:**
Date:	
Time:	
Notified by:	Estimated Time to Event Resolution Days: ☐☐ Hrs: ☐☐
Disaster Declared:	
Date:	**Recovery Site**
Time:	
	<RECOVERY SITE ADDRESS>
Authorised by	

Appendix 9

Checklists for review of off-site backup procedures

Checklist for review of non-IT off-site backup procedures

Area for Review	Completed
Identify all categories of off-site backup addressed by the procedures. Consider: • hard copy documentation • forms (application forms, manual receipts; cheque blanks#, etc) • supplies, and • equipment # It may be possible to make special arrangements with your bank, including guaranteed delivery time, which will enhance security of these forms	Yes ❑ No ❑
For each of the categories of items identified as being backed up, identify the triggers for adding/replacing/deleting off-site backup items	Yes ❑ No ❑
Identify persons responsible for determining what is to be backed up	Yes ❑ No ❑
Identify persons responsible for review and approval of changes/terminations of off-site backup items	Yes ❑ No ❑
Determine if an inventory of items is available and how the inventory is maintained	Yes ❑ No ❑
Determine whether a hardcopy of the off-site backup inventory is stored off-site	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

Checklist for review of IT off-site backup procedures

Area for Review	
Identify all types of files being backed up off site. Consider:	
• system software:	
- operating systems	
- support software	
- utility packages	
- communications software, and	
- Job Control Language (JCL), etc.	Yes ❑ No ❑
• application software:	
- source libraries	
- production libraries (Executable Code)	
- data dictionary files	
- Job Control Language, etc, and	
- production data disk files and databases	Yes ❑ No ❑
• user files:	
- on-line documentation	
- Production Scheduling	
- computer operations documentation (eg. recovery/restart), and	
- application system/program documentation	Yes ❑ No ❑
• archival files	Yes ❑ No ❑
For each of the categories of items identified as being backed up, identify the method(s) of backup. Consider:	
• full saves (entire file or database backed up)	
• incremental saves	
• production job stream	
• on request by user	
• application nightly backup batch run, and	
• special job stream	Yes ❑ No ❑

Checklist for review of IT off-site backup procedures (continued)

Area for Review	Completed
Determine the backup frequency and number of cycles retained off-site for each category of backup	Yes ❑ No ❑
Identify persons responsible for determining what is to be backed up	Yes ❑ No ❑
Identify persons responsible for review and approval of changes/terminations of off-site backup cycling	Yes ❑ No ❑
Note the reason(s) why any types of files are not being backed up off site	Yes ❑ No ❑
Determine if backup procedures are applied application by application or to an entire category of applications such as those designated *critical* NOTE: When the term "application(s)" is used above, it refers to operating system software, support software, utilities, and communication software in addition to end user business applications.	Yes ❑ No ❑
Identify the tool(s) used for identifying and recording off-site backups. Consider: • tape library management software packages • manual logs • special program/system with manual input, and • special program/system with automated input	Yes ❑ No ❑
Determine if vendor provided software products are used to perform backups	Yes ❑ No ❑
If a third party provides off-site storage, does the existing contract for retrieval and recovery of storage media match the requirements of the BCP?	Yes ❑ No ❑

Source: Deloitte Touche Tohmatsu Protech/IPS Methodology, 1999

AUSTRALIA

Business Continuity Management

Workbook

Keeping the wheels in motion

Better Practice

Australian National Audit Office

A Guide to Effective Control—December 1999

Australian National
Audit Office

Business Continuity Management

Workbook

Guide to Effective Control—January 2000

Better practice

The Australian National Audit Office produces better practice guides as part of its integrated audit approach which includes information services to audit clients.

A Better Practice series has been established to deal with key aspects of the control structures of entities—an integral part of good corporate governance.

This Workbook forms part of that series. The accompanying Guide deals with business continuity management within a risk management framework.

ISBN 0 644 39018 2

Information on Australian National Audit Office publications and activities is available on the following Internet address: http://www.anao.gov.au

Disclaimer

The Auditor-General, the ANAO, its officers and employees are not liable, without limitation, for any consequences incurred, or any loss or damage suffered by an organisation or by any other person as a result of their reliance on the information contained in this Workbook or resulting from their implementation or use of the accompanying Guide, and to the maximum extent permitted by law, exclude all liability (including in negligence) in respect of the Guide and the accompanying Workbook.

Designed by Art Attack Pty Ltd Canberra

Printed by Pirie Printers Canberra

Contents

Introduction

This Workbook is designed to assist organisations in the development of a comprehensive business continuity plan.

It is designed to lead operational and service area staff through the process of:

- identifying key business processes;
- establishing a maximum acceptable outage for each key business process; and
- designing appropriate cost-effective treatments in the event of an outage.

The results from this Workbook can be used by the Business Continuity Project Manager to develop a Business Continuity Plan.

The structure of the Workbook is based on the steps detailed in the *Business Continuity Management* Better Practice Guide published by the Australian National Audit Office. It is recommended that users of this Workbook first familiarise themselves with the concepts and processes discussed in the Guide.

The content of the Workbook comprises of general guidance, examples and worksheets. These should be adapted as required to ensure that key information and decisions are fully documented.

It is intended that the steps in the Workbook be followed sequentially. The Workbook may be completed individually or be used as the basis to facilitate group sessions.

Step one: Project initiation

A plan should be prepared to manage the business continuity project. The following outline is a suggested structure for this plan. If a plan has been completed, insert it in this section.

1. Introduction	
1.1 Background/Introductions	Why is the project being conducted?
2. Business objectives	
2.1 Objective of the project	Detailed objectives and outcomes of the major steps below
3. Requirements specification	
3.1 General requirements	Project sponsor Project manager Business unit involvement
3.2 Contracting considerations (if expert contractors are engaged)	Primary contractor Intellectual property Project reporting Variations to cost Warranty Rights
3.x Phase (for each phase of the project)	Objective of the phase The steps involved The outcomes for the phase Organisational resources that will be allocated to the project team The project team's roles and responsibilities Reporting requirements for the phase

4. Project deliverables and milestones

4.1 Project reporting	How will the project team report to the Organisation? What information the project team will provide? Status of the project Percentage completed Expected deliverables Issues for note or action
4.2 Deliverables and milestones	Tables listing the deliverables and receivables that are required to meet the objectives of the project

5. Project budget and administration

5.1 Budget	Staff resources Contract resources Sources of funds
5.2 Administration	Change control Resources and payment plan linked to deliverables Resources constraints Critical success factors

6. Roles and responsibilities

6.1 Responsibilities	Approvals for budget, sign-off phases, acceptance and implementation of recommendations
6.2 Project hierarchy	Chief Executive, Project Steering Committee, Project Manager, Project Team(s) reporting to Project Manager
6.3 Service provider/contractor responsibilities	Expectations and deliverables of the service provider

Step two: Key business processes identification

Introduction

Business processes are made up of the activities undertaken within each process and the resources consumed by, or applied to, each activity.

The objective of this step is to identify, and rank in priority order, those strategic, operational and support business processes that are critical to the production of organisational outputs and hence fulfilment of business objectives.

The identification of key business processes may already have been completed in other risk management and business planning activities undertaken in the organisation. The Organisation's Corporate Plan, Business Plans and Risk Management Plan are good starting points. If this is the case, this step in Business Continuity Management should confirm that the process descriptions are still valid and rank the processes in terms of their relative importance to achieving organisational objectives.

The following instructions will assist organisations identify and rank their business processes. The results of this activity should be entered on the worksheet at Appendix 1.

Instructions for completing the worksheet (Appendix 1)

1. Determine and document overall business objectives

Obtain or establish the business objectives for the business unit. The objectives for each business unit should support, and be consistent with, the overall organisational objectives, vision and mission established in the Corporate Plan.

Objectives are usually framed in terms of the effectiveness of outputs and may have a time, cost, quantity and/or quality dimension.

Document the business unit objectives on the worksheet.

2. Identify business processes

For each business objective, map all of the business processes undertaken within the business unit or service area.

The structure of many organisations mirrors the strategic, operational and support business process categorisations discussed in the accompanying Guide.

Page 32 of the Guide provides an outline of generic *mega* and *major* business processes that apply to most public sector organisations, under each of these categories. This structure may be a useful starting point for establishing a common language and understanding of what a business process is.

3. Determine and rank key business processes

Once an inventory of all business processes has been established for the business unit or service area it is necessary to determine which of these are critical to achieving organisational objectives.

All business processes will contribute in some form to organisational objectives. One approach is to first determine which objectives are the most important and to match the business processes to those objectives. It is then necessary to determine from within these processes those that are integral to achievement of the key objectives.

Generally, all operational processes can be considered to be key. It is more likely that some support processes—such as publishing and public relations—and some strategic processes—such as those associated with process improvement and quality assurance (but not quality control)—will not be mission critical.

It is suggested this ranking of processes is undertaken as a facilitated group session using a vertical slice of employees from with the business unit or service area.

4. Analyse key business processes into activities and resources and rank in priority order for recovery

Each key business process should be dissected into the activities undertaken for that process and the resources consumed or applied to the activities. This can be achieved by first considering the critical success factors required for the process to met its business objectives.

Resources applied to activities should be considered in terms of people, facilities, telecommunication information systems and business processes.

Operational areas should consider only the operational activities and resources that pertain to their processes. The support activities and resources will be analysed by the support areas.

The most critical activities and resources for each key business process will be afforded the highest priority in recovery. Therefore it is necessary to rank these also within each process.

Once a ranking has been agreed for each activity and resource these should be entered on the worksheet. The Chief Executive Officer and/or an appropriate management committee should agree the ranking of activities and resources.

The following example shows worksheets for an operational process and a support process completed to this step.

Priority listing of key business processes, activities and resources

Example: business support process

Objective: support the organisation by providing timely, accurate, reliable quality services

Rank	Process	Critical success factors	Activities and resources	MAO
1	Payroll	Payment of fortnightly salaries and allowances to all staff on time	1. Payroll team 2. HRM system 3. Payroll system 4. Communications link to bank	
2	Billing			
3	Paying Accounts			

Example: operational process

Objective: process and pay benefits to bona fide recipients on time, for the correct amount

Rank	Process	Critical success factors	Activities and resources	MAO
1	Pay benefits	Payment on time	1. Benefits payment teams 2. Benefits payment system 3. Communications link to bank 4. Cheque production system Also note reliance on mail room for timely dispatch of cheques	
2	Process new applications			
3	Modify payee details			

Notes:

1. The MAO (maximum acceptable outage) has not been completed at this stage—that is the next step in the process.
2. The benefits payment process has noted its reliance on a business support process—that is, the mail room (Registry). A separate analysis should be conducted for Registry.
3. The results of all analyses are combined to determine reliance on common resources and activities and inter-dependencies between resources and activities.

Step three: Business impact analysis (BIA)

The objective of this step is to determine a maximum acceptable outage (MAO) for each critical activity and resource identified in step two.

The BIA is undertaken for all key business processes and sets the recovery priorities, should those processes be disrupted or lost.

The following concepts are relevant.

Business continuity concepts relevant to the BIA

Concept	Description
Outage • *extraordinary event* • *loss of key business processes* • *high impact*	An outage is an extraordinary event, causing a disruption to, or loss of, key business processes, which has a high impact on the organisation This is distinct from downtime or systems failures that may occur as a part of normal operations where the impact simply reduces the effective utility of processes in the short term
Maximum Acceptable Outage (MAO) • *threat to achieving business objectives*	The MAO is the time it will take before an outage threatens an organisation achieving its business objectives The MAO defines the maximum time an organisation can survive without key business functions before recovery procedures must commence

Business impact analysis scenario

It is useful to establish a scenario in which the organisation has suffered an outage. This assists the people undertaking this exercise to consider their business processes in that context.

The following scenario is recommended as a starting point:

- a flood or fire has occurred and the building is inaccessible—all computer systems and supporting services are unavailable for a period of at least 30 days;
- assume a worst case, that is, the total destruction of workplace resources and information technology systems at the worst possible time; and
- authorisation has been given for additional staff, overtime, employee food, travel and accommodation expenses etc, for assistance in restoring essential business activities.

Do not consider any current continuity plans when determining impacts resulting from loss of services.

All days referenced are calendar days, not business days.

Establishing a framework for assessing the impact of a business interruption

We are making an assessment from the point of view an outage has occurred. This outage has affected the performance of key processes in that critical activities have ceased and critical resources are not available. We need to make a judgement on how long the organisation can survive without these key processes before it threatens the ability of the organisation achieving its objectives.

Once its occurs, and outage may have many ramifications. We need to assess the impact of the outage against an agreed framework to determine and establish the maximum acceptable outage (MAO) for each business process. This needs be considered at two levels:

- assessing the overall impact of loss of a process—this has probably been achieved (at least in part) by ranking the processing in order of priority to the organisation; and
- assessing the impact of the loss of the corresponding activities and resources to determine how long the process can be without that activity or resources until its own success is threatened.

The framework

An objective and consistent basis on which to assess the impact of an outage needs to be established. This will ensure the organisation is considering the same factors when determining the MAO. The level of impact can be assessed for each activity and processed using a scale similar to the table below.

Example: scoring level of impact of business disruption

Level of Impact	Assessment	Score
Extreme	Threatens political and business viability	5
Major	Significant impact on business drivers	4
Moderate	Major 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 resource	1

The MAO is set at that point where there would be a major impact (Score–4) on the ability of the activity or resources and therefore the process would fail. In effect, we are saying the business process can do without this activity or resource for any time under that point where there is a major impact and it will not affect the organisation achieving its objectives.

Below is an example of detailed criteria with which to determine the level of impact of an outage for a particular activity or resource. These criteria should be consistent with any such criteria established for the *top down* risk management process.

Example: detailed evaluation criteria for assessing business impact

Area of impact					
Rating	**Outputs (time, cost, quality)**	**Resources (staff, information, financial assets)**	**Reputation**	**Clients/ stakeholders**	**Compliance**
5 (Extreme)	Greater than ten per cent impact on achievement of key performance targets	Death of staff Financial loss in excess of $1 million Destruction or serious damage to most assets	Royal Commission Organisation found liable in legal action	Death or serious injury to clients Financial loss to clients in excess of $1 million	Breach of Constitution
4 (Major)	Up to ten per cent impact on targets	Injury to staff, loss of critical mass of staff Financial loss of up to $1 million Destruction or serious damage to key physical or information assets	Parliamentary inquiry Organisation, CEO and the Board the subject of legal action	Significant loss of access to service e.g. inability to provide mandatory opinions within legislative timeframe	Breach of Commonwealth law and regulations
3 (Moderate)	Up to five per cent impact	Permanent loss of key staff Financial los of up to $100,000 Damage to physical or information assets	Ministerial question in the Parliament	Major disruption of access to service	Failure to comply with Financial Directors and Chief Executive instructions
2 (Minor)	Up to one per cent impact	Temporary loss of key staff Financial loss of up to $10,000 assets in value	Adverse comments in press	Minor disruption of access to service	Failure to comply with internal guidelines
1 (Negligible)	No impact on achievement of output targets	Key staff available for a few hours	Internal impact only	No impact on clients/ stakeholders	Failure to comply with internal instructions

The assessment of the MAO practice

Using the earlier example, the MAO for each activity and resource is scored—the score is based on consideration of the impact of its loss. The assessment in the following table is based on the impact criteria detailed on the previous page.

Example: assessing MAO for activities and resources

Key business process	Activities and resources required	Impact of Interruption					MAO
		1-2 days	3-5 days	6-15 days	16-30 days	> 30 days	
Payroll	1. HRM—salaries team	1	4	4	4	5	2 days
	2. Salaries system	1	2	4	4	5	15 days
	3. HR system	1	1	1	2	4	30 days
	4. Communications link to bank	1	1	2	3	4	30 days
Payment of benefits	1. Benefits payment team	1	2	4	4	5	5 days
	2. Benefits payment system	1	1	2	4	4	15 days
	3. Communications link to bank	1	1	4	5	5	15 days
	4. Cheque production	1	1	2	3	4	30 days

Notes:
1. The MAO for each activity/resource is set at the point where a 4 rating and above is assessed.
2. The MAOs established should be agreed to by the Chief Executive and the Business Continuity Management Steering Committee.

Details of the agreed MAOs should be entered on the worksheet in Appendix 1.

Consolidation of MAOs by resource

The above example demonstrates a common resource that is used in both processes. To assist in determining inter-dependencies and to establishing the MAO for common resources the organisation may wish to consolidate the MAO schedule on a resource basis. The following table can be used for this purpose.

Example: consolidation of common resources

Resources	Impact of interruption					MAO
	1-2 days	3-5 days	6-15 days	16-30 days	> 30 days	
Operational staff (by business unit)						
Support staff (by service area)						
Operational IT systems (by system)						
Support IT systems (by system)						
Communications—voice						
Communications—data						
Facilities—buildings (by location)						
Facilities—plant and equipment (by category)						
Information—physical records						
Information—electronic data						

Step four: Design continuity treatments

The objective of this step is to determine cost-effective treatments for responding to an outage, establishing interim processing arrangements and restoring the lost activity(ies) and resource(s).

The accompanying Guide (at page 39) discusses a range of possible treatment options for various resources. Each option needs to be evaluated first in terms of its time to implement and then in terms of its cost.

The time to implement each option is compared to the MAO for the resource/activity. Only those options that can be implemented within the MAO need to be considered further. The relative cost of these options is then compared to determine the most cost-effective solution.

A simple example involves the choice between a hot site and a cold site for back-up computer processing. If both options can be implemented within the MAO for the activities and resources they replace, it will generally be less expensive to maintain a 'cold' site. However, if maintaining a hot site is the only means of re-establishing the activity or resource within the MAO, then cost is not so much the issue—but how to achieve it at the best cost.

The following costs may be relevant in the recovery period for interim processing arrangements:

- outside services;
- temporary employees;
- emergency purchases;
- rental/lease of equipment;
- wages paid to idle staff; and
- temporary relocation of employees.

The worksheet at Appendix 2 can be used to document this process and as a rationale to support the treatments options selected.

Appendices

1. **Worksheet for key business processes identification and business impact analysis**

2. **Worksheet for evaluation of treatment recovery options**

Appendix 1. Worksheet for key business processes identification and business impact analysis

1.1 Business unit/service area details

Business unit/service area	
Contact name	
Title	
Phone number	
Location	
Email	

1.2 Business unit key objectives, outputs, and performance indicators

Business unit objectives (in priority order)	Outputs or services for each objective	Performance indicators
1		
2		
3		

1.3 Identification of key business processes and business impact analysis

Business objective:			
Column 1	Column 2	Column 3	Column 4
Key business process	Critical success factors	Activities and resources required	MAO
1		1 2 3	
2		1 2 3	
3		1 2 3	
4		1 2 3	

Appendix 2. Worksheet for evaluation of recovery treatment options

Resource(s):

Options	Time to implement (days)	Within MAO Yes/No	Full cost (list components)	Cost-effective Yes/No
Response 1 2 3				
Interim processing 1 2 3				
Restoration 1 2 3				
Other issues 1 2 3				