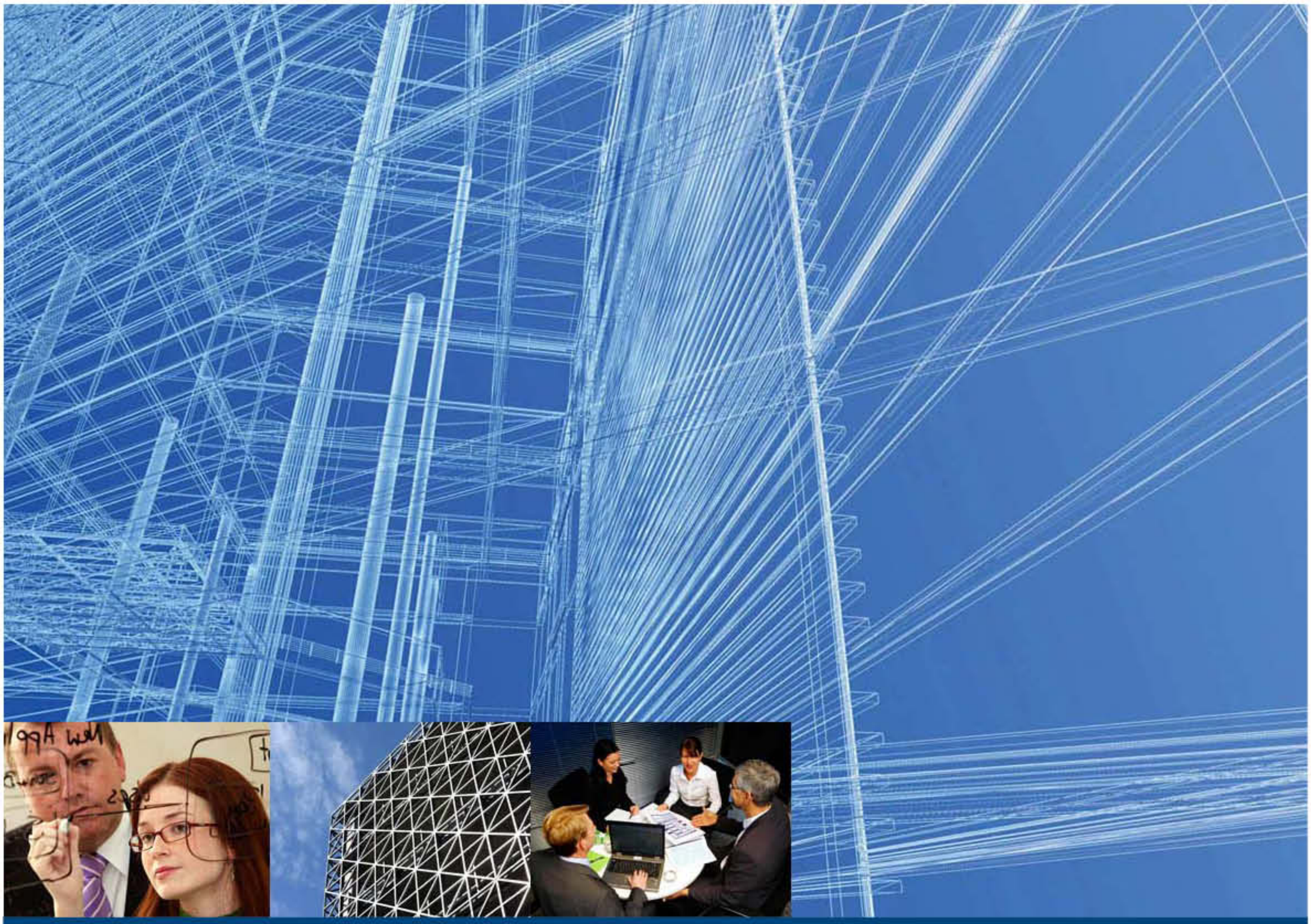

ICT asset disaster recovery planning guideline

Final

November 2010

v1.0.0

PUBLIC

Queensland Government Enterprise Architecture

ICT Policy and Coordination Office
Department of Public Works

Queensland Government

Document details

Security classification	PUBLIC		
Date of review of security classification	November 2010		
Authority	Queensland Government Chief Information Officer		
Author	ICT Policy and Coordination Office		
Documentation status	Working draft	Consultation release	☑ Final version

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Executive Director
ICT Policy and Coordination Office
ICTPolicy@qld.gov.au

Acknowledgements

This version of the *ICT asset disaster recovery planning guideline* was developed and updated by the ICT Policy and Coordination Office.

Feedback was also received from a number of staff from various agencies, including members of the Information Security Reference Group, which was greatly appreciated.

Copyright

ICT asset disaster recovery planning guideline

Licence

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

Figures

Tables

1 Document overview

This guideline has been developed for agencies to use when documenting their ICT asset disaster recovery (DR) arrangements. It has been developed under Information Standard 18: Information Security (IS18) to support implementation of Principle 9: Business continuity management. This document also supplements the:

- Guide for business continuity planning (GovNet users only) developed by the Security Planning and Coordination group and Counter-Terrorism and Coordination Unit within the Queensland Police Service (this unit was formerly within the Department of Premier and Cabinet)
- Business continuity plan documentation guideline (GovNet users only) developed by the Queensland Government Chief Information Office.

The remainder of section 1 provides background information to assist agencies to understand the guidelines. Section 2 provides an outline of common ICT asset DR considerations. Section 3 contains outlines of sample plan structures to assist agencies when developing their documentation.

This document does not address disaster recovery planning for information assets that are not ICT enabled. For guidance on recordkeeping and disaster recovery refer to the Queensland State Archives.

1.1 How to use this document

This guideline is a high level, general purpose tool to assist agencies to develop ICT asset DR plans.

As illustrated in Figure 1, agencies will need to conduct preparation activities before the plan is developed, and ensure maintenance exercises are carried out to keep plans current.

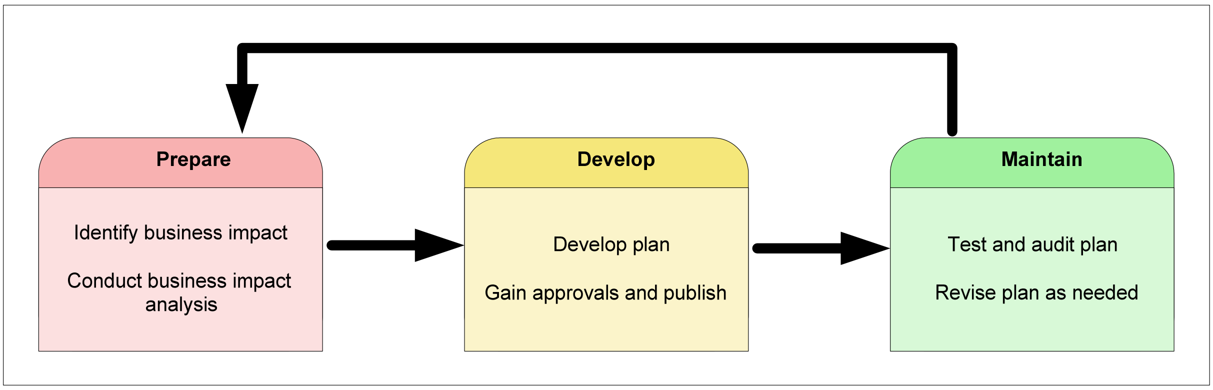

Figure 1: ICT asset DR planning lifecycle

2 Preparing ICT asset disaster recovery plans

2.1 Use of names versus roles in planning documents

Before documenting their ICT asset DR arrangements, agencies must determine their preferences with regard to identifying responsibilities – ie. if they will link responsibilities directly to staff, or if responsibilities will be mapped to organisational roles. The preferred approach will be an organisational choice and based on agency processes, culture and expectations.

Both approaches have a number of advantages and disadvantages, as listed in Table 1.

Type of responsibility	Advantages	Disadvantages
Individual-based responsibilities	Makes the plan easy to enact as people are clearly identified.	The plan may require frequent updating as staff change roles. More difficult to embed within role-based processes.
Role-based responsibilities	The plan requires fewer updates, as organisational roles tend to change less frequently than staff assigned to roles.	Enacting the plan is more difficult, as individuals are not directly identified. Additional resources mapping roles to individuals are needed.

Table 1: Advantages and disadvantages of individual versus role-based identification

2.2 Information security classification

Most ICT asset DR plans will contain sensitive information about an agency's services, infrastructure or staff. Each agency should follow the Queensland Government information security classification framework (QGISCF) process to determine appropriate classification levels for their plans, to ensure that appropriate security and management of the information is maintained.

For example, inappropriate controls on an ICT asset DR plan could lead to it being released containing full name, role and contact details of staff, which may have a measurable, significant or major impact on agency work if staff identities need to be concealed. In such a case, the plan should be security classified[1] and managed according to, or consistently with, the QGISCF process. An additional consideration for security classification of ICT asset DR plans is that they generally contain information which may be able to be used in reverse to plan disruption to agency services.

2.3 ICT asset disaster recovery plans in the context of business continuity

The *Counter-Terrorism Risk Framework for Queensland Government Agencies* (the 'GAP Framework')[2,3], (section 4.4) addresses ICT asset disaster recovery as a discrete element of business continuity[4] in acknowledgment of the existing mandatory requirements under IS18[5]:

> *Government agencies rely on the availability of information to conduct business. Generally, information disaster recovery is a component of each agency's overall business continuity arrangements. However, within the Counter-terrorism Risk Framework, information disaster recovery is addressed as a discrete element in acknowledgement of existing mandatory requirements under IS18.*

[1] Normally plans will be classified at the 'in-confidence' level

[2] GAP URL: http://premiers.govnet.qld.gov.au/security/gap.html

[3] Counter Terrorism Risk Framework URL: http://premiers.govnet.qld.gov.au/security/gap_ctframe.html

[4] 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. http://www.anao.gov.au/uploads/documents/Business_Continuity_Management.pdf

[5] Page 19, *Counter-Terrorism Risk Framework for Queensland Government Agencies* (March 2004).

Under the GAP Framework, all agency CEOs have responsibility to develop and maintain plans covering arrangements for business continuity of core services and information disaster recovery.

As discussed above, and acknowledged by the GAP Framework, ICT is just one element of a business continuity plan and an agencies broader business continuity arrangements. From an ICT point of view, business continuity plans need to be supported by disaster recovery plans for ICT systems and services.

Each business service may require the support of none, one or more ICT systems. Even where business services rely on ICT systems, the business continuity plan for the service may be to implement a manual service delivery process, and thus business service continuity can be established without immediate or early recovery of the associated ICT systems. Agencies therefore need to establish which of their ICT systems will require disaster recovery plans, and maintain this list of key ICT assets in a ICT asset disaster recovery register as a way of ensuring all critical assets are appropriately covered. This is illustrated in the diagram shown here.

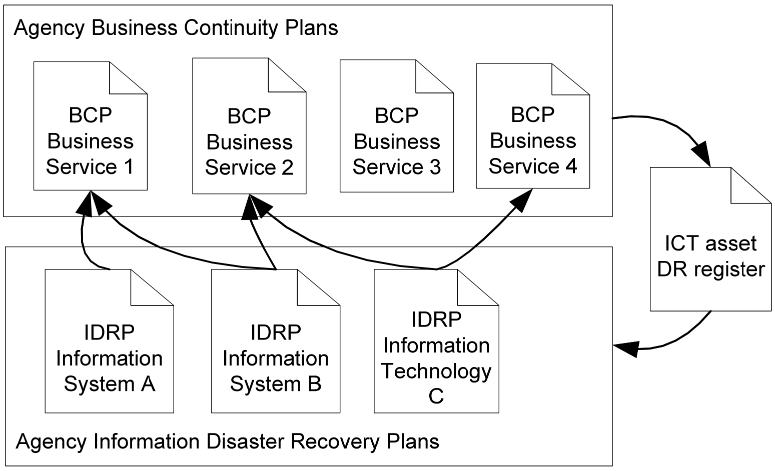
Agency Business Continuity Plans
BCP Business Service 1
BCP Business Service 2
BCP Business Service 3
BCP Business Service 4
ICT asset DR register
IDRP Information System A
IDRP Information System B
IDRP Information Technology C
Agency Information Disaster Recovery Plans

Figure 2: Relationship of key elements of business continuity planning in the context of ICT asset disaster recovery planning

There are several other plans within the GAP Framework that the ICT asset disaster recovery plan may also need to link, however the agency business continuity plan is the primary one. See the GAP Framework for further information.

2.4 Links between agency ICT asset disaster recovery plans

Agency ICT asset DR arrangements may be recorded in a single plan, but are more commonly spread across several documents with varying amounts of detail. Therefore agencies may have a number of ICT asset DR plans, serving different levels or functions of their organisation, as shown in Figure 3 and Figure 4 (page 7).

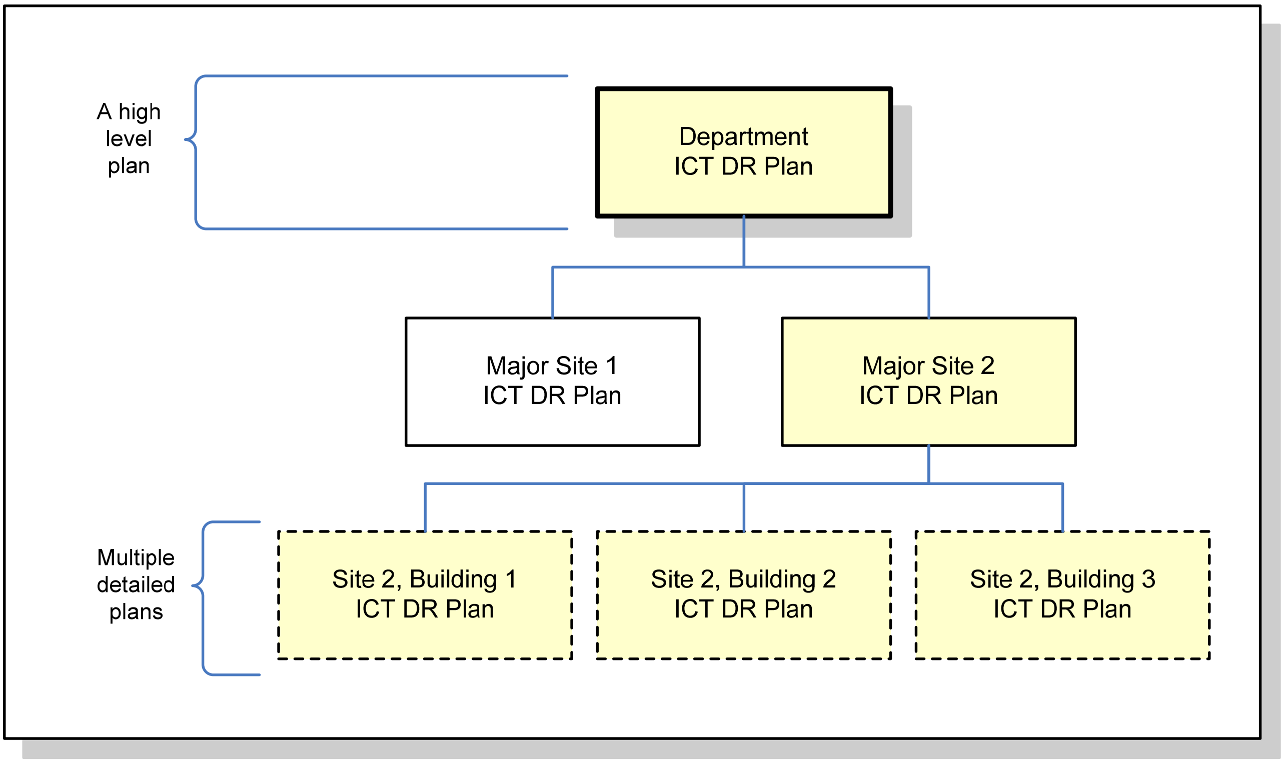

Figure 3: ICT asset DR plans by location

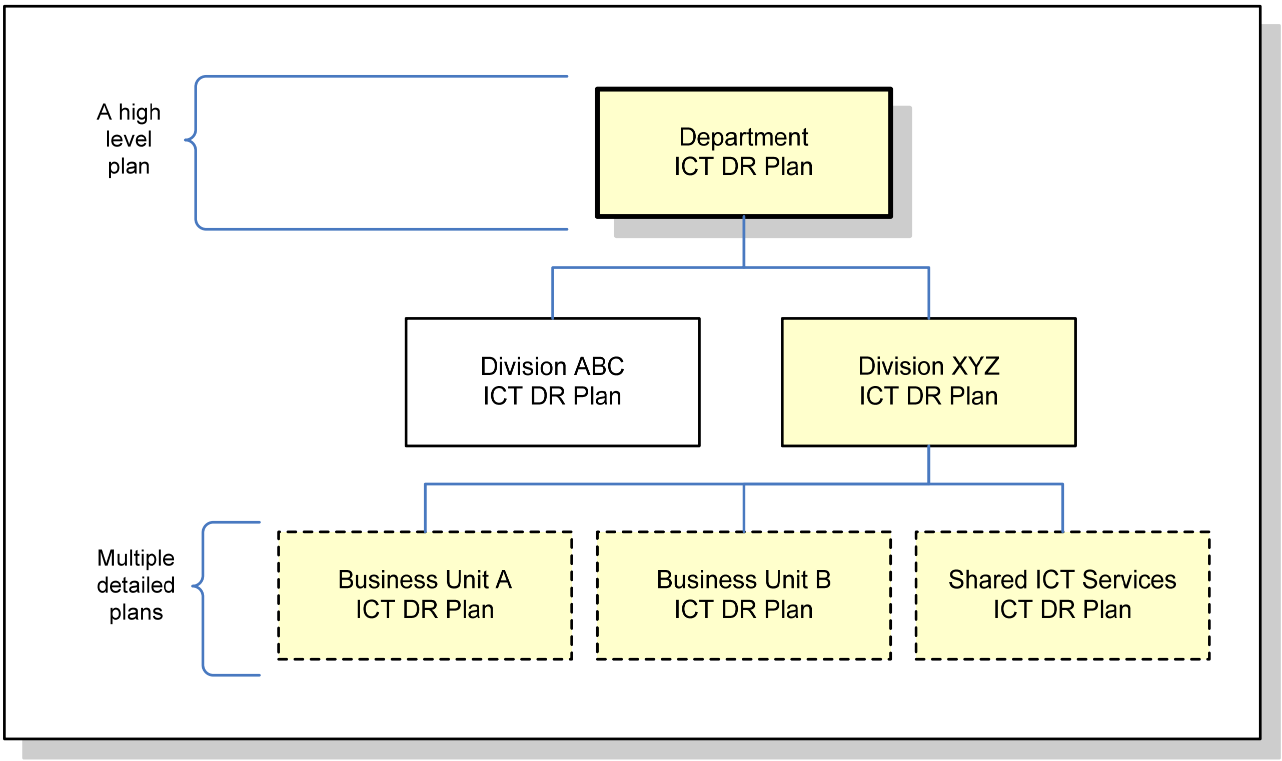

Figure 4: ICT asset DR plans by business area

Multiple plans are generally developed so that their content is tailored for the document's audience. There is no 'right' number or hierarchy of plans. The overriding consideration is to ensure that the plans are understandable to those who need to execute them, and contain only the level of information required for DR activities to be enacted.

Small agencies are likely to have fewer plans than large agencies, due to reduced complexity within the organisations. Similarly, agencies organised around specific functions may find they have a brief high level plan supported by many detailed functional unit plans that encompass all aspects of services and their support needs.

When multiple ICT asset DR plans exist, they must complement each other if they are to be effective. As shown in Figure 5 multiple ICT asset DR plans may contribute to support critical organisational functions. Activities that are high priority for the overall organisation may have a different criticality for the unit that owns the activity. The dependencies between organisational and unit priorities must be considered for an effective continuity response to occur.

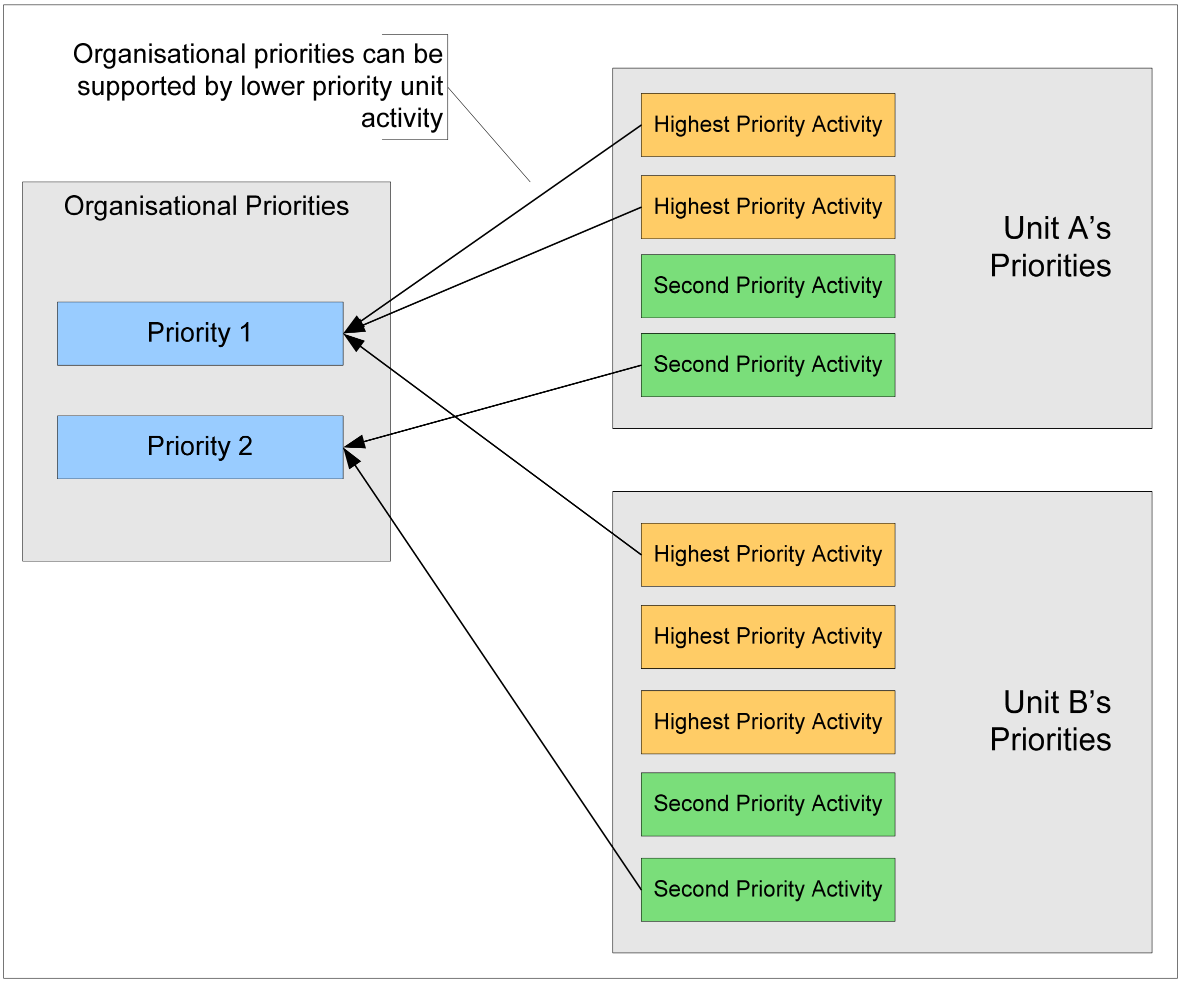
Organisational priorities can be supported by lower priority unit activity
Organisational Priorities
Priority 1
Priority 2
Highest Priority Activity
Highest Priority Activity
Second Priority Activity
Second Priority Activity
Unit A's Priorities
Highest Priority Activity
Highest Priority Activity
Highest Priority Activity
Second Priority Activity
Second Priority Activity
Unit B's Priorities

Figure 5: ICT asset DR plan relationship between department and agency critical functions[6]

[6] Diagram adapted from the State of Oregon Enterprise BCP Program Overview, available online at http://www.oregon.gov/DAS/EISPD/BCP/docs/BCP_Overview_0305.ppt

3 Developing ICT asset DR plans

Each agency's ICT asset DR plans will cover similar content areas to other agencies, although they will all be presented differently. This section and section 5 provide an outline of the topics and considerations that ICT asset DR plans should cover.

It is impossible to predict every kind of incident that may lead to an ICT asset DR plan being activated. Instead plans should document a generic, flexible set of actions that the agency agrees are an appropriate response to any foreseeable crisis situation. Plans should allow the agency to respond to an incident without needing to consider the cause of the incident. Investigation of the cause of an incident resides with the agency's information security and protective security incident management processes.

3.1 Business priorities

An ICT asset DR plan must reflect business priorities if it is to be effective, as it is important that business functions are recovered in an appropriate order.

The *Financial and Performance Management Standard (2009)* requires all agencies to have a risk management framework[7], that ensures that risks are identified and managed. When identifying risks, agencies should identify their critical functions and priorities. These functions and priorities must be addressed in business continuity and ICT asset DR plans and activities.

Most agencies will confirm business priorities through activities such as a business impact analysis (BIA). A BIA can form the basis of many DR and business continuity plans, not just the ICT asset DR process. For example, the BIA may be a key input into an agency's ICT, infrastructure and human resources DR plans, as shown in Figure 6.

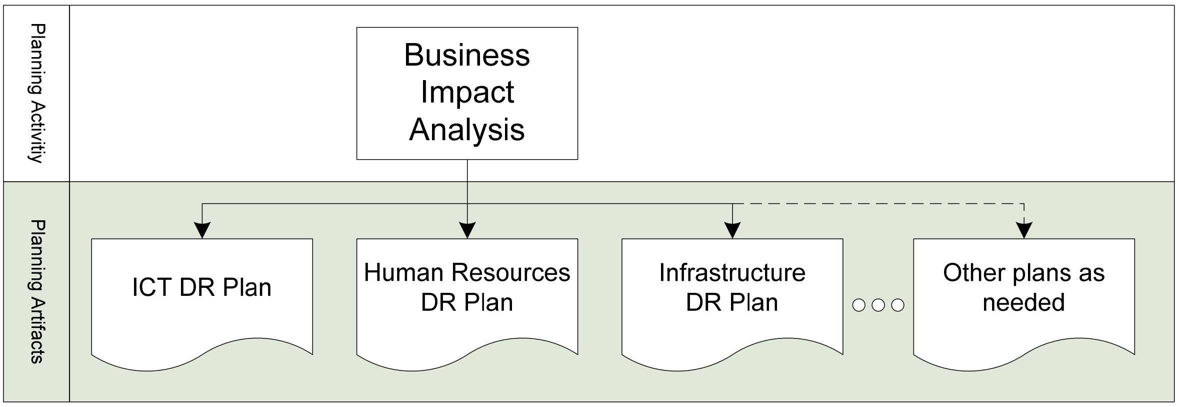

Figure 6: Use of business impact analysis

Business priorities can be identified in a number of ways, including by:

- agency services
- system or group of systems
- locations
- any combination of the above.

[7] When assessing the vulnerability of ICT assets, agencies should consider adapting the *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*. Further information can also be found in the *Information risk management best practice guide*.

The agency's approach to identifying business priorities should be reflected within the ICT asset DR plan. For example, if the agency identified its priorities by systems or groups of systems, the ICT asset DR plan should provide guidance on how to respond to a disaster that affects one or many of the identified systems.

Some agencies will choose to rank their business priorities by criticality to the business. This ranking can be used to inform the ICT asset DR plan and guide agency recovery. However, ranking will not always be necessary or possible. In most instances just an understanding of what the agency feels is critical, important and peripheral can be a useful tool in a disaster incident so that efforts can be focused on restoring high value systems.

3.2 Process outline

A process outline is used to document the agreed, standard agency response(s) to an ICT asset DR incident. The inclusion of a process outline within ICT asset DR plans ensures a consistent and comprehensive reaction to an ICT asset DR episode and provides the best chance of ensuring ongoing continuity of agency ICT infrastructure.

Depending on agency needs, the ICT asset DR plan may include a mix of the following processes (as well as any other processes the agency deems necessary):

- activation processes
- ICT asset DR treatments and actions
- escalation processes
- stand down processes.

These four processes are described in Table 2 below.

Process	Description
Activation	Activation processes outline how and when the ICT asset DR plan will be invoked and should be informed by business priorities. A key part of activation processes is often listing the management and key employees who should be contacted in an emergency situation. In this section, processes may also be needed to guide what should happen if the disaster recovery coordinator or members of the team fail to respond to messages within expected timeframes. Key questions addressed in this stage include: • What is the maximum acceptable downtime? When will the plan be activated? • How will the plan be activated? • Who approves the plan's activation? • Who needs to be communicated or informed of the plan's activation?
ICT asset DR treatments and actions	Treatment and actions outline what will be done in response to an ICT asset DR incident and activation of the plan. Often treatments address worst case scenarios, and are accompanied by scoping guidelines to scale actions to meet smaller incidents. Alternatively, different actions may be specified for different categories of incidents (ie. an incident within one unit, across multiple units or across the entire organisation). Treatments and actions are usually grouped reflecting the organisation and its infrastructure. Common groupings include by system (the application and supporting technology), by types of systems or technologies, by business units with shared services or infrastructure, by location or by provider – or by any combination of the above.

Process	Description
	Key questions addressed in this stage include: • What should be done to address the incident? For example: – Is an offsite capability or alternative site arrangement required? – What is the availability of alternate hardware? – What communication alternatives are available? – How will data and applications be recovered? – Will supporting resources be required?
Escalation	Escalation processes provide guidance on when and how to expand the disaster recovery activities. This process is especially important if a large hierarchy of ICT asset DR plans exist within an organisation. Key questions addressed in this stage include: • What are the critical dependencies between this ICT asset DR plan and other ICT asset DR plans or business continuity plans? • When and how will higher level plans and plans from other areas be invoked? • If the ICT asset DR plan has multiple stages, when and how will each stage be activated?
Stand down	Stand down processes signal the end of an ICT asset DR incident and the resumption of recovery activities or normal operations. Key questions addressed in this stage include: • When will the plan be de-activated? • What steps need to occur to finalise the activities of the plan and resume normal operations?

Table 2: Common ICT asset disaster recovery processes

These processes can be documented using textual descriptions, graphically or by a combination of text and graphics.

3.3 Supporting information

A successful ICT asset DR plan will provide a framework for responding to an ICT asset DR incident. Hence the plan should be simple to follow and user friendly, while containing the minimum detail to support its operation.

However, there are many supporting details that may be needed during DR activities. Some elements of supporting information will be placed within the plans (for example, the key ICT asset DR personnel), but often this information can be documented in appendices or in referenced documents.

While the exact amount and types of supporting information will vary between agencies, areas to consider including or linking to include:

- key ICT asset DR personnel
- a full outline of current ICT infrastructure
- staff contact lists (e.g. names, addresses)
- emergency recordkeeping arrangements and minimum expectations
- vendor agreements

- current service provider contacts, and details of services and agreements/expectations regarding the service
- testing and maintenance processes
- checklists for ensuring processes meet objectives, all ICT infrastructure elements are restored
- pre-prepared communication messages such as media releases and emails
- funding sources.

4 Maintaining ICT asset DR plans

4.1 Storage

In accordance with the mandatory clauses specified in the Information Security Policy – Mandatory Clauses document agencies must ensure that copies of their ICT asset DR plans are stored in multiple locations including at least one offsite.

4.2 Testing

Effective disaster recovery relies on aware and trained staff who can quickly apply agency plans. Testing ICT asset DR plans ensures that they can be successfully enacted, as well as providing staff training opportunities. Regular testing also provides an opportunity to update plans to accurately reflect the current organisational situation.

Each agency will have a different approach to testing their ICT asset DR arrangements. The chosen testing method will balance costs, time and will reflect the agency's risk profile. Common testing approaches include:

- discussion activities or seminars, where staff are brought together to learn about the ICT asset DR arrangements
- table top exercises, which involve a role play or walk through situation and that brings together key personnel who will be involved in the ICT asset DR plan to act out the plan in response to a crisis
- full rehearsals, where an ICT disaster incident is simulated and the agency or parts of the agency are suspended until the exercise is complete (finished or successfully resolved).

ICT asset DR plans may also be tested as part of the agency's business continuity tests.

5 Plan templates

The next four sub-sections provide examples of ICT asset DR plan structures. These can be used to inform the documented structure of ICT asset DR plans, but must be tailored to meet specific agency needs.

5.1 Simple or traditional plan

The simple or traditional plan groups similar ICT asset DR plan content into sections. This and the technology centric approach are the most common starting points for agency ICT asset DR initiatives.

1 Introduction

1.1 Objective of the plan

1.2 Scope

1.3 Key plan assumptions

1.4 Limitations

2 Initiation of emergency procedures

2.1 Key roles and responsibilities

2.2 Activating the ICT asset DR

2.3 Salvage operations at disaster site

2.4 Emergency procurement procedures

3 Initiation of recovery procedures

3.1 Recovery site requirements

3.2 Designated recovery sites

3.2.1 Site A

3.2.2 Site B (etc.)

4 Maintenance of the plan

4.1 Plan reviews

4.2 Training and testing of the plan

5.2 Technology-centric approach

The technology-centric approach plans ICT asset DR around the technology deployed in the agency. This approach and the simple/traditional ICT asset DR approach are the most common starting points for agency ICT asset DR initiatives.

1 Overview

2 ICT asset DR process

3 Declaration and escalation procedures

4 Technology response procedures

4.1 Application(s)

4.2 Data

4.3 Databases

4.4 Interfaces and middleware

4.5 Resource and supply issues

4.6 Systems support and help

4.7 Transmission, routing and network management

5 Large scale responses

5.1 Utility interruption and asset damage

5.2 Site damage and access issues

7 Ongoing testing and maintenance

5.3 State-based model

The state-based model approach is useful if agencies wish to track their current ‘state’ of ICT asset DR through the recovery process. To implement this approach, agencies must have a clear understanding of the difference between, and activities within, each stage of the disaster recovery processes. This approach is often taken as agency ICT asset DR initiatives mature.

1 ICT asset DR overview

1.1 Objective of the plan

1.2 Scope

1.3 Key plan assumptions

1.4 Essential ICT services

1.5 Primary locations

1.6 Emergency arrangements

2 ICT asset DR strategies

3 Phase I: Passive

4 Activating the plan

5 Phase II: Active

5.1 Emergency response

5.2 Recovery site preparation

5.3 Emergency communication arrangements

6 Phase III: Recovery

7 Ongoing testing and maintenance

5.4 Business process-based model

The business process-based model is best suited for use by agencies that closely align their ICT infrastructure with business processes. In this style of plan, business processes are used to group ICT asset DR arrangements.

1 Overview

1.1 ICT asset disaster recovery process

1.2 Limitations and assumptions

2 Processes and treatments

2.1 Business process continuity requirements

2.2 Business process continuity treatments

2.3 Process interdependencies

3 Supporting information

3.1 Activities and locations

3.2 Contact lists

3.3 Test and maintenance arrangements

5.5 Suggested appendices

There are a number of appendices that agencies could consider including in their plans. Some agencies will cover part of this information within the body of their plans, while others may instead choose to maintain these details in a separate (but linked) document or group of documents.

- Contact details – agency staff, ICT asset DR designated contacts, business unit contact details, BCP personnel, suppliers/vendors contact details etc.
- Department key contacts and expectations – If an ICT asset DR incident occurs, there may be a need to notify departmental corporate areas to ensure they are aware of alternative communication arrangements. If the ICT asset DR incident becomes a continuity episode, there are no surprises for the department.
- Recordkeeping plans – These plans should include how to identify and protect existing critical business records, as well as how to ensure that appropriate records will be kept during a disaster recovery incident.
- Training and awareness activities – that are to be undertaken as part of the plan development or promotion.
- ICT infrastructure details – such as a list of all the applications and technology in use within the agency.
- Emergency infrastructure details – an in-depth outline of the infrastructure that will need to be established in an emergency.
- Communication plans – how will clients, suppliers and other agencies that rely on your services be contacted if they are affected?
- Reciprocal arrangements – in some cases, agencies may have reciprocal arrangements that will allow them to re-establish operations with a partner.
- Links to business continuity and other ICT asset disaster recovery plans – with linkages and priorities clearly identified – so that if higher or lower level plans need to be invoked, they can be identified and activated quickly.

Appendix A Additional resources and references

- Government Services Group, Department of Treasury & Finance, Government of Victoria, *GLO6.1 Detailed recovery plan*
- Information Standard 18: Information security
- *Other Queensland Government information security resources*