GOVERNMENT OF
WESTERN AUSTRALIA

Whole of Government

ICT Disaster Recovery for Business Continuity Policy

A supplementary guide.

Document Control

The Western Australian Whole of Government
ICT Disaster Recovery for Business Continuity Policy: A Supplementary Guide
Version 1 – April 2017.

Produced and published by: Office of the Government Chief Information Officer.

Acknowledgements: The Policy was developed in collaboration with Western Australian public sector agencies.

Contact:

Office of the Government Chief Information Officer

2 Havelock Street

WEST PERTH WA 6005

Telephone: (08) 6551 3927

Email: policy@gcio.wa.gov.au

Document version history

Date	Author	Version	Revision Notes
April 2017	Office of the GCIO	1	Published.

Introduction

This document is to be read in conjunction with the Office of the Government Chief Information Officer (GCIO) whole-of-government Information and Communications Technology (ICT) Disaster Recovery for Business Continuity Policy (the Policy).

The purpose of this document is to provide:

- additional context to the Policy;
- guidance on how to meet the requirements of the Policy; and
- directional advice in achieving appropriate ICT disaster recovery and business continuity risk management outcomes.

The audience of this document is:

- those accountable for agency risk management;
- business function owners accountable for agency services; and
- ICT personnel responsible for ICT disaster recovery.

The Policy seeks to integrate the disciplines of ICT disaster recovery and business continuity in order to achieve better overall risk management outcomes. The Policy, and this guide, is intended to be read within the context of agencies' broader risk management framework.

Who Can Help?

While agencies can outsource a task or service, they can never obviate themselves of the responsibility for ensuring appropriate business continuity outcomes and the effective management of risk. Like all risk management activities, ICT disaster recovery must be embedded into existing practices to ensure the development of internal capability and continuous improvement – it is not a project that ends with the production of a document.

Where a skills gap is identified, agencies are strongly encouraged to reach out to their colleagues in other agencies who have experience, skills and capability in this area, and the Office of the GCIO is happy to help facilitate these connections for agencies who require assistance.

Why is ICT Disaster Recovery Important?

Digitally-enabled services can bring great benefits to citizens and government alike. However, if they are not available, the consequences can be costly and wide-ranging. Recent high-profile examples of government system outages – such as the 2016 Census and outages suffered by the Australian Tax Office – clearly illustrate the potential risks government organisations are exposed to.

Agencies must implement robust ICT disaster recovery and business continuity arrangements if they are to manage service availability risks within public expectations.

Where it is deemed necessary, agencies may wish to engage the services of external risk management or ICT disaster recovery planning specialists to assist them in building the required internal capability, or services such as auditing. Some risk management consultancy services can be sourced via the Department of Finance's Common Use Arrangement CUA23706 – Audit Services and Financial Advice. Suppliers on CUAICTS2015 – ICT Services may also be able to assist agencies in providing ICT governance and disaster recovery services and advice.

Meeting the Three Requirements of the Policy

It is intended that meeting the requirements of the Policy will assist agencies in developing the requisite ICT disaster recovery skills and capabilities. It is only by implementing a programmatic approach to managing risks to ICT service availability that an agency can be prepared for business continuity.

This guide contains checklists for each of the three policy requirements. These are provided to stimulate thoughtful discussion around the key success factors for ICT disaster recovery and broader risk management, rather than a checklist for compliance with best practice or any particular standard.

Requirement One: Establishing Appropriate Governance

Agencies must:

- Establish roles and responsibilities for ICT disaster recovery within the corporate risk management framework; and
- Ensure ICT disaster recovery management is undertaken within an ICT incident management framework.

The intent of this requirement is to ensure that:

- Risks related to ICT disaster recovery are visible to those with accountability for managing agency risks; and
- Roles and responsibilities for ICT disaster recovery (including incident identification and escalation) are established.

The Corporate Risk Management Framework

Agencies should have some form of risk management structure in order to meet their risk management obligations, as detailed in the Policy at *Section 6: Relevant Policy Obligations.* As ICT disaster recovery is primarily a risk management activity, it should be linked to organisational risk management arrangements and governance.

An agency's risk management arrangements are a natural starting point for assigning roles and responsibilities relating to the management of ICT disaster recovery risks. This will also assist in creating a proper link to an agency's business continuity planning arrangements.

Roles and responsibilities for ICT disaster recovery may include such key tasks as:

- Developing whole-of-organisation ICT disaster recovery plans;
- Implementing and testing system-level ICT disaster recovery;
- Coordination with business continuity planning;
- Triggering ICT disaster recovery plans; and
- Reporting to the agency risk management body on the outcomes of testing.

These are suggested roles only. The key desired outcome of allocating roles is proper governance and accountability.

Proper governance can provide accountable authorities, business service owners and ICT practitioners with confidence that an appropriate ICT disaster recovery capability exists, and that this capability is aligned with the requirements of core business service delivery. It can also assist agencies in identifying and minimising the likelihood of disruptions impacting business functions, and ensure integrated responses from both the business and ICT areas in the event of disruptions occurring.

In developing and assigning roles, agencies should ensure that any roles:

- Are relevant to an agency's risk management practices and business arrangements;
- Support business-ICT alignment and engagement with agency executives;
- Ensure the appropriate response in the event of an outage;
- Assign risks to those who are best able to monitor and treat them; and
- Report risks relating to the unavailability of ICT services to the risk management body.

Roles should be built around agency services, and informed by Business Impact Analysis, which is discussed further in this guide. An individual or group must have responsibility for ensuring that disaster recovery skills, documentation and capabilities are up to date and coordinated within the agency's broader risk management approach. Assigned roles should distinguish between the strategic responsibilities for approving, and operational responsibilities for conducting or implementing.

Business-Driven Planning

By ensuring the oversight of the peak risk management body, agency executives and business service owners can make informed decisions regarding ICT disaster recovery and the appropriate level of priority and investment. It is important to recognise that appropriate ICT disaster recovery outcomes are dependent upon commitment and planning that involves senior management, ICT practitioners and business service owners.

A multidisciplinary approach is required to ensure these outcomes. For example:

- Business people must be involved in ICT disaster recovery planning to ensure decisions are based upon the needs of the agency and the public. Business service owners should be responsible for decisions concerning how long their business can acceptably tolerate downtime.
- In the event of a disruption, all areas of a business should know how to respond – not just ICT staff. Staff must know how to continue their business if ICT systems cannot be restored.

Most importantly, a multidisciplinary team supports an integrated approach to organisational resilience that maximises an agency's capacity to continue business function in the event of a disruption. It is good practice for agency business service owners and risk managers to have a good understanding of the risks they are exposed to resulting from the unavailability of ICT services, and of how the availability of ICT systems will be maintained to an appropriate level in the event of a disruption.

While the Policy only focuses on ICT disaster recovery requirements, agencies are strongly encouraged to link their ICT disaster recovery activities to broader business continuity management.

ICT Incident Management

Agencies must ensure ICT disaster recovery management is undertaken within an ICT incident management framework. That is, agencies have a capability and a process for identifying and escalating incidents of a severity that require an ICT disaster recovery response. The key outcome for this requirement is that agencies will ensure that there is a process for identifying incidents which may, or already have, become a disruption, warranting the triggering of the ICT disaster recovery response.

Without a formal process, an agency's response to a disruption can only be undertaken on an *ad-hoc* basis, slowing down the recovery process and creating difficulties for root cause analysis.

Checklist

- **Business service owners are aware of the risks posed by the unavailability of ICT systems.**
- **Roles and responsibilities for disaster recovery have been approved by the agency's corporate risk management body.**
- **The agency risk register includes risks relating to the unavailability of ICT systems.**
- **Risk owners are confident that the treatment options specified can meet their stated capability.**
- **The agency has arrangements for whole-of-business business continuity that provide for service continuity during ICT system recovery.**
- **Business service owners have alternative arrangements for providing services during the disruption.**

Requirement Two: Formalise ICT Disaster Recovery Arrangements

Agencies must plan, document and implement formal procedures for ICT disaster recovery.

A programmatic approach is at the heart of best practice in ICT disaster recovery and business continuity. Without formally defined processes, it is difficult for agencies to evaluate their risks and ensure they can quickly respond to, and recover from, disruptive events. Implementing complementary standards for ICT disaster recovery and business continuity will help agencies to ensure holistic risk management outcomes.

Agencies should have an ICT Disaster Recovery Plan in place by **1 April 2018**.

A number of resources are available to agencies to assist with such an approach.

Standards and Guidance

Government Published Risk Guidance

The Insurance Commission of Western Australia, via RiskCover, publishes guidelines for both business continuity and risk management. While their use is not mandated, the documents are useful, high-level guides.

In 2009, the Australian National Audit Office published a Better Practice Guide for Business Continuity. It is understood that this guide is in the process of being revised.

ISO Standards

There are numerous relevant third-party ICT disaster recovery business continuity standards that agencies may wish to utilise. Agencies are strongly encouraged to research and consult widely regarding which best suits their needs.

The following ISO standards are provided as suggestions for agency consideration on the basis of their currency and wide support in literature and practice. The Office of the GCIO does not endorse or mandate any specific standard, but strongly encourages agencies to implement a program that is appropriate to their organisational needs, context and overall approach to risk management.

Business Continuity

ISO/IEC 22301:2012 Business Continuity Management Systems specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

ISO/IEC 27031:2011 Guidelines for Information and Communication Technology Readiness for Business Continuity describes the concepts and principles of ICT readiness for business continuity – that is, ICT disaster recovery. This standard provides a framework of methods and processes to identify and specify all aspects for improving an organisation's ICT readiness to ensure business continuity. It encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

Business Impact Analysis

Conducting a business impact analysis (BIA) is the cornerstone of informed ICT disaster recovery decision-making. A BIA provides the basis for aligning ICT disaster recovery plans (and broader business continuity management) to business priorities.

A BIA is a systematic process to determine and evaluate the potential effects of an interruption to critical business functions as a result of an incident. A BIA will identify business functions, the critical systems supporting them, and their dependencies. Without a process to understand these, agencies are unable to make properly informed decisions about ICT disaster recovery strategies or investments.

A BIA maps business processes to business resources, can inform the recovery point and recovery time objectives, and help agencies to understand the potential cost of downtime.

Support from risk managers, business services owners and ICT practitioners is fundamental to ensuring that the BIA reflects the needs of the business. The BIA is also a good starting point for determining roles and responsibilities for ICT disaster recovery, as per Policy Requirement One.

A basic example of an ICT systems focussed BIA is provided at Appendix 1: ICT Disaster Recovery Business Impact Assessment Example. This is a hypothetical example that agencies may find useful in understanding the BIA process, and it may form a basis for their own process and supporting documents. Agencies may also wish to conduct this in tandem with the Business Continuity Business Impact Analysis process and tools found at https://www.icwa.wa.gov.au/riskcover/risk-management .

ICT Disaster Recovery Planning

By using the outputs of the BIA, disaster recovery planning can begin or existing arrangements can be revised. It may be the case that existing systems are unable to meet agency business requirements for technical reasons, or may require additional investment in order to do so. For ICT practitioners, finding a language and approach that is relevant to your agency’s business owners is important in communicating these requirements. Communicating risks relating to ICT system unavailability to the corporate risk body is a key step in creating accountability for accepting or treating these risks.

Regardless of what standard or model an agency chooses to utilise, the ICT Disaster Recovery Plan will be an important document containing process and procedures to recover and protect a business' IT infrastructure in the event of a disruption. Such a plan, ordinarily documented in written form, should include system level recovery arrangements and include sufficient information to be useful to personnel who are not familiar with the specific system. ICT Practitioners should ensure that plans are in place to ensure that business service owners (or delegates) will be contacted in the event of a disruption.

In developing or revising ICT disaster recovery plans, ICT practitioners are encouraged to investigate developments in cloud-based infrastructure and "Disaster Recovery as a Service" offerings, which may offer cost-effective solutions to achieving ICT disaster recovery goals.

Incident Response Planning

An Incident Response Plan is a general plan for dealing with any number of crises that could negatively impact an agency's business. An Incident Response Plan will be broader than just ICT disaster recovery considerations, and should include specific references to the triggering of the Disaster Recovery Plan. ICT practitioners should consider specifically how they can contribute to this, and how incident response planning can be linked to the ICT Disaster Recovery Plan.

Developing and implementing ICT disaster recovery plans enables agencies to be prepared for a disruption. Planning enables agencies to establish the necessary tools to recover within acceptable time frames, and to understand what to do in the event of a disruption.

Checklist:

- **The organisation has identified and adopted a business continuity and/or ICT disaster recovery system.**
- **A BIA, or equivalent process, has been performed that identifies agency business functions and the systems that support them.**
- **ICT practitioners understand the recovery time and recovery point objectives the business requires, and these are agreed with the business service owners.**
- **The ICT Disaster Recovery Plan reflects the priorities of the business.**
- **Outstanding ICT disaster recovery risks are identified and reported to the corporate risk management body.**
- **System-level ICT disaster recovery plans are in place.**
- **Current, offsite copies of the ICT Disaster Recovery Plan are available in the case of an incident.**

Requirement Three: Continuous Improvement

Agencies must ensure that ICT disaster recovery arrangements include formal mechanisms for continuous improvement.

ICT disaster recovery arrangements must be routinely monitored, reviewed and tested.

Exercising and Testing

Testing is vital to ensuring that the business continuity and ICT disaster recovery plans are ready for use in the event of a disruption. In particular, testing ICT disaster recovery plans verifies that an agency's strategies can meet its recovery point and time objectives. Testing is a major contributor to overall business continuity and disaster recovery capability and awareness.

Each agency will have a different approach to testing its ICT disaster recovery capabilities and arrangements. The testing method and frequency should balance costs and time, and reflect the agency's risk profile. Agencies are encouraged to develop a risk-based testing schedule informed by business impact analysis. This will ensure that the regularity of a system's ICT disaster recovery testing should reflect its criticality to the business.

It is important to test the ICT disaster recovery capabilities in a manner that will give assurance that the technology and methods chosen will work as expected should they be required.

Any testing plans and activities, and their results, should be escalated to the risk management body, so they can be informed about outstanding risks and ensure appropriate action is taken. For ICT practitioners, this can be an important step in making a case for additional funding where investment in ICT disaster recovery is required. Test results, or identified shortfalls in ICT disaster recovery capability, should be presented in terms of their relationship to important agency services. This will help business people understand their importance, and enable risk owners to make informed decisions regarding accepting a risk or take action to treat it.

ICT Disaster Recovery in Action

In 2016, a Western Australian agency suffered the disruption of its primary data centre during a major storm. This data centre hosted a public facing system critical to agency business.
Because the agency had designed and architected the system based upon business impact analysis, the system was only affected for the 5 minutes it took for it to fail-over to the secondary facility – well within the business-defined tolerances.
By consulting with their business, the agency was able to design and architect a system that delivered agency and community service needs despite the protracted outage of a primary facility.

Most importantly, reporting risks to the risk management body ensures that the appropriate parties are aware of, and accountable for, outstanding risks due to inadequate ICT disaster recovery arrangements.

Continuous Improvement

The Policy states that agencies should review their ICT disaster recovery arrangements at least every 12 months. The intent is that agencies will formally review the relevance and currency of their arrangements annually. This does not mean that every system need be tested at the same time, or every year.

An agency's corporate risk management body is responsible for approving an annual testing regime of systems based upon criticality and risk. This includes the systems to be tested and frequency of testing. The risk management body is also responsible for approving the classification of business systems in terms of criticality.

Business continuity management and disaster recovery is a process of continuous improvement, and agencies are strongly encouraged to ensure they have the necessary skills and capabilities to guarantee ongoing risk management for their business. Continuous improvement is also about making sure that the relevant governance, planning and testing arrangements are working. Where issues or failures are reported to the risk management body, action must be taken to resolve them. This should include root cause analysis, and investigation of all relevant issues from governance down to technical faults.

Continuous improvement requires not only resolving individual issues, but maintaining the health, effectiveness and relevance of an agency's ICT disaster recovery capability to support business continuity capabilities.

Checklist:

- **ICT disaster recovery arrangements, including the testing schedule are risk-based, and reviewed annually.**
- **The regularity of testing detailed in the schedule is reflective of the criticality of the systems to the business.**
- **ICT Disaster recovery arrangements are approved annually by the corporate risk management body.**
- **ICT practitioners are reporting the outcomes of testing to the risk management body.**
- **Root causes of incidents and disruptions are investigated.**

- **Changes to business processes that impact on system criticality are reflected in the ICT disaster recovery arrangements.**

Appendix One: ICT Disaster Recovery: Business Impact Assessment Example

		Government Service			
		Deliver key services relating to the support of an [example].		Provide frontline [example] services	
		Business Function		Business Function	
		Corporate Services	Records Management	Field-based [example] services	Office-based [example] services
		Business Function Owner	Business Function Owner	Business Function Owner	Business Function Owner
		Director, Corporate Services	Director, Records Management	Director, Field Based Services	Director, Office Based Services
		↑ ↑	↑ ↑	↑ ↑	↑ ↑
		Dependence on ICT System	Dependence on ICT System	Dependence on ICT System	Dependence on ICT System
ICT Systems	HR/Payroll	**Important**	**Useful**	**Useful**	**Useful**
	Finance	**Critical**	**Useful**	**Useful**	**Useful**
	Records Keeping	**Important**	**Important**	**Useful**	**Useful**
	Email & Calendar	**Important**	**Important**	**Critical**	**Critical**
	CRM	None	None	**Important**	**Important**
	Corporate Website	**Useful**	None	**Useful**	**Useful**

Dependency to System Legend:

	Critical	**Important**	**Useful**
Risk assessment:	Key agency services are directly impacted without this supporting system. Significant reputational and financial losses may be incurred if recovery time and recovery point objectives are not met.	Key agency services are moderately impacted without this supporting system. Moderate reputational and financial losses may be incurred if recovery time and recovery point objectives are not met.	Key agency services are mildly impacted without this supporting system. Minor reputational and financial losses may be incurred if recovery time and recovery point objectives are not met.
Recovery time objective:	10 Minutes	Two hours	Six Hours
Recovery point objective	10 Minutes	Five hours	One business day
System testing interval	12 Months	24 Months	24 Months

Conducting the Business Impact Analysis

- Agencies should list all business services across the top of the table. These may begin at the highest level with the services listed in an agency budget, which may then be decomposed to as many levels as are necessary to make the assessment meaningful. Only two levels are provided here.
- Each ICT system should be listed along the left hand side of the table. ICT practitioners should be able to provide a full itinerary of an agency's systems.
- Business service owners must be responsible for determining criticality.
- Example criticality ratings are provided, but agencies are encouraged to develop their own based on their individual requirements. For agencies with life-critical services, these ratings should be changed to reflect this. These could be linked to the risk rating system utilised in the agency whole-of-business risk matrix.
- Agencies may wish to allocate recovery point and recovery time objectives based on criticality, or they may find it more useful to allocate these to each system individually. The times provided here are examples only; these should be based on business service requirements.
- A system's ICT disaster recovery arrangements should be based on its highest level of criticality; that is a system that is critical to only one business function but useful to all others should have arrangements based on it being a critical system.
- Agencies may wish to use the BIA as a method for determining and agreeing a system-level testing schedule for the relevant ICT disaster recovery arrangements. However, this approach will not cover any infrastructure-level testing requirements.