GOVERNMENT OF
WESTERN AUSTRALIA

Whole of Government

# ICT Disaster Recovery for Business Continuity Policy

# Document Control

**The Western Australian Whole of Government**
**ICT Disaster Recovery for Business Continuity Policy:** Version 2 – 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**

| Version | Author | Version | Revision Notes |
|---|---|---|---|
| May 2016 | Office of the GCIO | 1 | Initial release. Titled "ICT Business Continuity and ICT Disaster Recovery Policy." |
| April 2017 | Office of the GCIO | 2 | Reviewed and aligned with supplementary guide. |

# 1. Purpose

Citizens expect Government to continue delivering services and products despite disruptive events, and meeting this expectation is an essential capability of Government. Information and Communications Technology (ICT) is now central to almost all Government activities, and agencies must effectively manage risks related to the unavailability of ICT systems.

The purpose of the ICT Disaster Recovery for Business Continuity Policy (the Policy) is to:

- support agencies in ensuring services are available:
  - at a level which enables them to meet their objectives and obligations, and
  - within reasonable community expectations;
- ensure that ICT disaster recovery is integrated within agencies' risk management and business continuity frameworks; and
- support agencies in improving their ICT disaster recovery skills and capabilities.

# 2. Definition of Terms

**Business Continuity** is the holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause. It also provides a framework for building organisational resilience, wherein the organisation can respond effectively to safeguard the interests of its key stakeholders. Business continuity is a subset of risk management.

**Business Function** is the process or operation of work performed to accomplish an agency's government service responsibilities.

**Business Function Owner** is an individual with the responsibility for delivering a business function.

**Disruption,** or disruptive event, is a significant incident which cannot be controlled within a predetermined timeframe that is acceptable to the agency. This may be anticipated (e.g. hurricane) or unanticipated (e.g. power failure/outage, earthquake, or attack on ICT systems/infrastructure) which disrupts the normal course of operations at an agency location. A disruption causes a loss of, key business activities, which has a significant impact on the organisation. A disruption is distinct from minor interruption of services such as system glitches, processing errors and brief loss of communication links that may occur as a part of normal operations where it does not have any significant impact on the agency.

**ICT Disaster Recovery**, or DR, is the ability to restore the ICT elements (people, process information and technology) of an organization to support the continuity of its critical business functions within a predetermined period of time. Disaster recovery includes the prevention, preparedness, response and recovery from a disruption. Disaster recovery is supported by policies and procedures.

**ICT Disaster Recovery Plan** is a defined and documented plan that details how ICT capabilities will be restored following a disruptive event.

**Incident Management** is the process of identifying, analysing, and correcting incidents. It includes classifying and escalating incidents which cannot be resolved and are thus classified as a disruption, triggering ICT disaster recovery activities.

**Recovery Point Objective** is the longest agreed period in which data loss from an ICT system is acceptable.

**Recovery Time Objective** is the longest agreed period in which an ICT system can be unavailable. This time is essentially the time ICT practitioners have available to restore an ICT system following a disruption.

**Risk Management** is the practice of systematically identifying, understanding, and managing the risks encountered by an organisation. This includes the process of implementing, maintaining and embedding risk management in an organisation.

## 3. Background

In 2016, the Auditor General found that 64% of audited agencies in the Western Australian public sector did not have adequate disaster recovery and business continuity arrangements in place.[1] The community served by these agencies are potentially exposed to unacceptable levels of risk relating to the unavailability of ICT systems. With proper ICT disaster recovery planning, undertaken within the oversight of a risk management framework, agencies are able to properly identify and manage these risks.

The whole-of-government ICT Strategy, *Digital WA*, is driven by a vision of better services, supported by technology, via a public sector that is mature in its digital capabilities. ICT is increasingly crucial to agencies' service delivery operations. Ensuring that >90% of government digital services meet or exceed agreed and published service levels is a key performance indicator target within the *Digital WA* strategy.

Within this context, the Office of the Government Chief Information Officer (GCIO) seeks to support agencies in building their ICT-specific disaster recovery capabilities to ensure better business continuity outcomes.

## 4. The Risk Management Context

ICT disaster recovery supports business continuity, and both are activities under the broad umbrella of risk management. Western Australian government agencies have risk management obligations (see *Section 6: Relevant Policy Obligations*), and generally have some form of corporate risk governance to enable them to meet these obligations.

In a modern ICT-enabled organisation, ICT disaster recovery, linked to business continuity management, is an integral component of that organisation's ability to ensure continuous business function and meet its risk management obligations.

Agencies can only make informed decisions regarding risk once they are aware of them. Adopting a risk management perspective to ICT disaster recovery within the oversight of the

[1] *Systems Audit Report*, Office of the Auditor General, June 2016.

peak corporate risk management body enables agencies to ensure that ICT disaster recovery is appropriately planned, implemented and resourced within business needs and risk appetite.

## 5. Policy Requirements

The requirements of the Policy are as below.

### 1. Establish Governance and Accountability

*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.*

ICT disaster recovery should be linked to an agency's risk and ICT governance frameworks to ensure a unified approach to disaster recovery and the highest level of executive support.

Agencies should ensure that a process and capability exists for identifying and analysing incidents that escalate into disruptions, and thus require a disaster recovery response.

### 2. Formalise ICT Disaster Recovery Arrangements

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

These procedures must ensure that critical business functions dependent on ICT have appropriate mechanisms in place to manage the relevant corporate risks. Agencies should have appropriate arrangements in place to:

- reduce the risk of disruption to ICT services (*prevention*);
- mitigate the consequences of disruptive events (*prepare*);
- respond to disruptive events (*response*); and
- recover from disruptive events (*recovery*).

These arrangements should:

- include documented procedures (e.g. a disaster recovery plan) to restore ICT systems in the event of a disruption; and
- prioritise system recovery on the basis of their importance to the business, as determined via consultation with business service owners.

### 3. 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.*

Disaster recovery arrangements should be updated in response to the findings of tests, changing organisational needs and evolving business processes.

Agencies should adopt a risk-based approach to their ICT disaster recovery arrangements, which should reviewed and approved by the corporate risk management body annually.

## 6. Relevant Policy Obligations

Agencies are required to comply with this Policy as per *Premier's Circular 2016/03: Mandatory Implementation of Whole of Government Information and Communications Technology (ICT) Strategy and Associated Policies*.

> *All Western Australian state government agencies are expected to apply the principles and requirements contained within the strategy and policies into all current and future projects as well as normal operational procedures and practices.*

The Public Sector Commission and the Department of Treasury mandate the following generalised business continuity and risk management obligations for the public sector.

*Public Sector Commissioner's Circular: 2015-03 Risk Management and Business Continuity Planning* stipulates that:

> *All public sector bodies should manage the risks associated with the activities performed by their organisation. This involves prudently conducting risk assessment processes to identify the risks facing organisations, being able to demonstrate the management of risks and having continuity plans to ensure they can respond to and recover from any business disruption.*
>
> *Public sector bodies should ensure policies and continuity plans are maintained to ensure they are up to date with the activities performed by their organisation.*

*Treasurer's Instruction 825: Risk management and Security* stipulates that the *Accountable authority shall ensure that:*

> *i. there are procedures in place for the periodic assessment, identification, and treatment of risks inherent in the operations of the agency; and*
>
> *ii. suitable risk management policies and practices are developed.*

The Policy is an ICT disaster recovery specific supplement to these existing policy obligations.

## 7. Standards

The Policy is designed to be applied in conjunction with agencies' existing policy obligations and be compatible with a broad range of business continuity and ICT disaster recovery standards. In acknowledgement of the variety and diversity of agency requirements, no standards are mandated by this Policy. Notwithstanding, agencies should adopt and implement disaster recovery and business continuity standards that are:

- appropriate to their unique circumstances;
- aligned to industry best practices; and
- aligned with the requirements of this policy.

## 8. Reporting

Self-assessment of compliance with this Policy will be included within agencies' annual reporting requirements to the Office of the GCIO.

Agencies may also be assessed as part of the Auditor General's annual Systems Audit Report.

## 9. Supporting Material

RiskCover publishes both Risk Management Guidelines and Business Continuity Management Guidelines for the public sector.

These are available at https://www.icwa.wa.gov.au/riskcover/risk-management.

A supplementary guide, that assists agencies in understanding and meeting the Policy requirements, is available from the Office of the GCIO website at www.gcio.wa.gov.au.