**NSW Government**

**Disaster Recovery**

Contact:

informationsecurity@finance.nsw.gov.au

Strategic Policy Branch

Services and Digital Innovation Division

Department of Finance, Services and Innovation



**Table of contents**

|  |  |  |
| --- | --- | --- |
| [**1.**](#page4) | [**Introduction**](#page4) | [**1**](#page4) |
| [**2.**](#page7) | [**Developing a DR Policy**](#page7) | [**4**](#page7) |
| [**3.**](#page8) | [**Recovery strategy and solution design**](#page8) | [**5**](#page8) |
| [**4.**](#page13) | [**Recovery Plans**](#page13) | [**10**](#page13) |
| [**5.**](#page17) | [**Plan testing, exercising and verification**](#page17) | [**14**](#page17) |
| [**6.**](#page22) | [**Program maintenance and continual improvement**](#page22) | [**19**](#page22) |
| [**7.**](#page26) | [**Training and awareness**](#page26) | [**23**](#page26) |

[**Appendix A - Implementing an DR program**](#page27)

[**Appendix B – Policy Examples**](#page28)

[**Appendix C –Test Plan Example**](#page35)

[**Appendix D – Resources**](#page37)

[**Appendix E – Glossary**](#page38)

**Document control**

**Approval:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Name & Position** |  |  |  |  | **Date** |
|  |  |  |  |  |  |  |  |
|  | Information Security Steering |  |  |  |  |  |
|  | Group |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | ICT Leadership Group |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | **Version** | **Status** | **Date** | **Prepared by** | **Comments** |
|  |  |  |  |  |  |  |  |
|  | 0.1 | Initial draft | Nov 2014 | DR/BCM WG |  |  |
|  |  |  |  |  |  |  |
|  | 0.2 | Initial draft | Dec 2014 | DR/BCM WG |  |  |
|  |  |  |  |  |  |  |
|  | 0.3 |  | Jan 2015 | OFS |  |  |
|  |  |  |  |  |  |
|  | 0.4 | Commented draft | June 2015 | OFS | Ref change |
|  |  |  |  |  |  |  |
|  | 0.5 | Revised draft | Nov 2015 | DFSI |  |  |
|  |  |  |  |  |  |  |  |
|  | 1.0 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Review:** |  |  |  |  |  |  |

These Guidelines will be reviewed in July 2017.

They may be reviewed earlier in response to post-implementation feedback or as necessary.

1. **Introduction**
	1. **Purpose**

****

Under the *NSW Government Digital Information Security Policy* (DISP) (refer to Circular OFS-2015-05) agencies must implement business processes and continuity controls to counteract interruptions to business activities. It is essential that critical business processes are protected from the effects of major failures of digital information systems and services or disasters.

Disaster recovery focuses on the information or technology systems that support business functions. It is a subset of business continuity, which involves planning to keep all aspects of a business functioning in the midst of disruptive events. From a digital government perspective, controls and protections can be broadly grouped under the term Disaster Recovery (DR). In these Guidelines, disaster recovery is defined as:

The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organisation after a disaster or outage.

The purpose of the NSW Government Disaster Recovery Guidelines (the Guidelines) is to assist agencies to implement the NSW Government Digital Information Security Policy by developing their own disaster recovery plan and the capabilities to restore and recover their critical digital information systems if they are disrupted.

1. **Scope and structure of the Guidelines**

These Guidelines include:

* policy
* recovery strategy and solution design
* recovery plans
* plan testing and verification
* program update, review and maintenance
* training and awareness.

The Guidelines are structured around the continuous improvement cycle: plan, go, check and act.

Page 1

Figure 1: Disaster recovery Plan-Do-Check-Act



**PLAN establish policy, objectives, targets, identify**

**processes & procedures to manage risk & improve ICT readiness to support business continuity following disruption**

|  |  |  |
| --- | --- | --- |
| **DO implement & operate** | **CHECK assess / measure performance** | **ACT to correct & prevent** |
| **the policy, controls, processes** | **against policy, objectives & practical** | **issues based on results of** |
| **& procedures** | **experience & report results for** | **management review to achieve** |
|  | **management review** | **continual improvement** |

****

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | **ICT DR Solution** |  |  |  |  |  |  | **ON-GOING** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | **ICT DR Policy** |  |  |  |  | **Implementation** |  |  |  |  |  | **Monitor, review** |  |
|  |  |  |  |  |  |  |  |  | Implementation of |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | recovery: |  |  |  |  |  | **evaluate:** |  |
|  |  |  |  |  |  |  |  |  |  |  |  | strategy |  |  |  |  |  | Monitoring, |  |
|  |  |  |  |  |  |  |  |  |  |  |  | capability |  |  |  |  |  | detection & analysis |  |
|  |  |  |  |  |  |  |  |  |  |  |  | options |  |  |  |  |  | of threats |  |
|  |  |  |  |  |  |  |  |  |  |  |  | processes |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Business impact** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **Reporting:** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **analysis =** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | measuring against |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | **Plans** |  |  |  |  |  | performance targets; |  |
| ICT business |  |  |  |  | **ICT DR Strategy** |  |  |  |  |  |  |  |  |  |  |  | program outcomes |  |
|  |  |  |  |  |  |  |  |  | ICT response and |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| continuity |  |  | **Formulation and** |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | disaster recovery plan/s |  |  |  |  |  |  |  |  |
| requirements |  |  | **Solution Design** |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | and procedures |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **ANNUAL REVIEW** |  |
|  |  |  |  |  |  | Consider: |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **ICT DR Testing** |  |
|  |  |  |  |  |  |  | resilience |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | enhancement needs |  |  |  |  |  |  | **Implement** |  |  |  |  |  |  | Test Calendar |  |
| ICT Service Provider |  |  | skill & knowledge |  |  |  |  |  |  |  |  |  |  |  |  | Test plan |  |
|  |  | facilities |  |  |  |  |  |  | **awareness,** |  |  |  |  |  |  | Run test |  |
| Disaster Recovery |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | technology |  |  |  |  |  | **competency and** |  |  |  |  |  |  | Report test |  |
| and Business |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | data |  |  |  |  |  | **training program** |  |  |  |  |  |  | results |  |
| Continuity capabilities |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | suppliers |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | ICT readiness |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | performance criteria |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | **Document control** |  |  |  |  |  |  | **Audits** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | version control |  |  |  |  |  |  | Internal |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | availability, |  |  |  |  |  |  | External |  |
| Understand critical ICT |  |  |  |  |  |  |  |  |  |  | accessibility |  |  |  |  |  |  |  |  |
| services and continuity |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| readiness requirements |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



**Management**

**review**

**DR Risk**

**Management**

* issues management
* control / treat non conformities
* act on reviews / reports / audit recommendations

**Continual improvement**

Implement review of program / activities / define ttimeline, triggers and maintenance drivers

1. **Elements**

The elements of DR under the *ISO27031 Information technology* *–security techniques* *–* *Guidelines for* *ICT readiness for business continuity -* Stages in ICT Readiness for Business Continuity (IRBC) are:

* ICT DR policy (overall governance)
* ICT DR strategy and solution design (operational governance)
* ICT DR solution implementation – DR strategy, DR capability
* ICT DR training and awareness
* ICT DR plan and procedures
* ICT DR testing
* ICT DR program monitoring, review, evaluation and reporting
* ICT DR program risk management - control, treatment of non-conformities
* ICT DR program continual improvement.

These elements may either relate to, integrate, connect with and/or depend on other management, organisational and business functions and structure.

Page 2

The success of implementing and managing DR capability will be increased by:

* grouping DR components under a program of ongoing activities or functions, which will result in improved monitoring, review and evaluation of both the program and individual activities. The DR program must be documented, progress tracked and staff given clear guidance about their DR tasks. For detailed information on developing an implementation program see [Appendix A -](#page27) [Implementing an DR program.](#page27)
* identifying the Executive Sponsor whose role is to promote the importance of DR at the senior management level and influence strategic alignment of the DR program with the organisation’s vision and goals.
* establishing, for example the DR with a dedicated role, accountable for the coordination and overall management of the DR program across the organisation (this may be the DR manager).

Page 3

1. **Developing a DR Policy**

****

This section outlines the policy requirements based on the continuous improvement cycle that will assist agencies with different business needs and degrees of operational complexity to develop DR capability for their environment.

1. **DR Policy**

The DR policy sets out the DR scope, capabilities and principles, providing governance for the agency’s DR operational effectiveness.

Policy should be considered in the context of:

* other agency policies and strategic objectives, such as its business continuity policy, information security policy, and other ICT and non-ICT policies and strategies; and
* the size, nature, and complexity of their business and operating environment.

This policy should be written, approved, published and communicated in accordance with agency policy protocols. It is to be reviewed at planned intervals and updated in accordance with agency needs.

The policy should clearly state:

|  |  |
| --- | --- |
| DR strategy and objectives | Including answers to: |
|  | What is our DR strategy? |
|  | Why is DR important to the agency? |
|  | What will it help achieve? |
| Scope of DR | This should range from DR governance management including |
|  | outsourcing, to the operational management requirements and |
|  | identification of individual applications that require DR capability. |
| Key dependencies on other | Including information security, business continuity, risk |
| agency and NSW government | management, asset management, service delivery, information and |
| policies | records management, change management. |
| Key DR documentation | Including policy document, DR plan structure and possible references |
| hierarchy | to other agency documentation mandatory testing criteria (method |
|  | of testing and frequency) |
| Training and awareness of DR | Supports the ongoing improvement and maturity of the DR program |
|  | and its targeted audience. |
|  | The training and awareness process will: |
|  |  determine appropriate level of training |
|  |  | determine targeted audience |
|  |  develop a training calendar |
|  |  report awareness across the agency. |
| Auditing | Audits may be either internal or external, but must be independent |
|  | and undertaken according to an agreed Audit schedule and |
|  | methodologies. |
| Key personnel and delegations | People who have the authority, responsibility and accountability for |
|  | the agency’s DR. For instance, what roles are responsible for: |
|  | • | the policy and plans |
|  | • | developing and maintaining the policy and plans |
|  | • | ongoing testing and verification |
|  | • | developing and delivering training and awareness |
|  | • | ongoing management and improvement of DR |
|  |  | processes. |
|  |  | Page 4 |

1. **Recovery strategy and solution design**

****

This section outlines the requirements of the recovery strategy and solution design. The strategy ensures DR solutions and plans are technically aligned with the organisation’s policies and objectives.

Creation of DR solutions and plans for single systems or an entire agency are ongoing activities. Organisational change at a high level (structure, responsibility, strategy) and low level (personnel, location, evolution of systems and technology) will require that the DR solution and plan are updated together. All changes, along with the updated solutions and plans, create the need to continually test systems and train staff, to evaluate and review the DR program and processes, which may involve third party service providers.

1. **Key components of disaster recovery strategy and solution design**

DR strategy documents the process by which an agency’s ICT infrastructure is restored following an unplanned outage.

The DR strategy should:

* ensure the disaster solution is aligned with other organisation strategy, policies and requirements. For example, those related to business continuity, cloud strategy, procurement strategy, innovation strategy, mobility, ICT service continuity and information security
* cater for the recovery requirements of simple or complex ICT systems, applications, data and infrastructure
* categorise each ICT service (systems, applications, data and infrastructure) into recovery categories/tiers
* define disaster recovery service level requirements for establishment of service level agreements
* provide a direction to define recovery category/tiering and testing requirements
* create an opportunity strategy to optimise technical architecture(s) for disaster recovery.

Agencies should consider the following essential criteria during the development of their DR strategy:

* Understand the critical business processes and their reliance on critical ICT services including ICT Infrastructure, business applications and data. The business will usually provide this information by conducting a business impact assessment (BIA).
* Classify the business applications and ICT services into categories based on the BIA, recovery priorities, and dependencies. Sometime the classification can be in tiers for easier management.
* Consider technology and operational issues such as third party dependencies, system dependencies, risks, resilience technology, recovery and testing.

The disaster recovery solution design provides options so that agencies can categorise their needs based on BIA requirements and choose the recovery tiers to use**.** Another important consideration during the DR strategy and solution design is to consider the whole DR process from an event perspective where the BIA requirements depict the event timeline requirements.

The following diagram shows the relationship between the Maximum Acceptable Outage (MAO), the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO).

Page 5

Figure 2: Relationship between MAO, RTO and RPO



The disaster recovery strategy and solution design sets the scope and the recovery time frames and priorities, including the considerations of site details, required investments and limitations for business consideration.

**3.1.1** **Disaster recovery tiering**

A DR tier model can be used to:

* clearly define the priority and sequence in the recovery of systems and services
* provide service availability and DR requirements in defining service level agreement
* support business continuity management to determine the frequency of testing based on risks at each tier.

Once developed, the recovery tier model optimises the agency’s ICT systems/application architecture for disaster recovery.

The recovery sequence moves from Tier 1 through to Tier 5.

Table 1 Recovery tier model.

|  |  |
| --- | --- |
| Recovery Tiers | Description |
| Tier 1 | Foundation services that must be recovered before any other systems, |
|  | service and functions can be recovered. These include networking, |
|  | connectivity, directory and domain name services |
| Tier 2 | Mission critical services that generally impact revenue or key organisational |
|  | objectives |
| Tier 3 | Critical services being internal operations or customer relationship focused |
|  | where data collection is affected or transaction processing is delayed |
| Tier 4 | Important internal services that can be recovered by manual operations. |
|  | These may slow operations but will not stop critical activities |
|  | Page 6 |

|  |  |
| --- | --- |
| Tier 5 | Non-critical services that are generally for test and development or non-time |
|  | critical application |

**3.1.2** **Alignment of service requirements**

The classification of applications and/or ICT services by tier will establish the necessary recovery sequence for each service. The following table gives an example of this alignment. Numbers in the table below should be determined by agencies through their BIA exercise.

Table 2: Example of alignment to tiering model

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Tier | Criticality | Services | Impact/Measure | RTO | RPO | Data/DR |
|  |  |  |  | (hrs) | (hrs) | Protection |
|  |  |  |  |  |  |  |
| 1 | Foundational | Domain Name | Critical core |  |  | Replication |
|  |  | Services (DNS) | infrastructure for |  |  |  |
|  |  | Directory Services | networking and |  |  |  |
|  |  | (AD) | connectivity |  |  |  |
|  |  | IP Allocation (DHCP) |  |  |  |  |
| 2 | Mission | External: | Critical services | 0-1 | 0-1 | Database |
|  | Critical | Customer facing | impacted Revenue |  |  | logs |
|  |  | Revenue streams | stops |  |  | replication |
|  |  |  | Multiple agencies are |  |  |  |
|  |  |  | impacted |  |  |  |
| 3 | Critical | Internal: Email | Data collection | 1-4 | 1-4 | Continuous |
|  |  | Customer | affected |  |  | replication |
|  |  | relationship | Transaction processing |  |  | snapshots |
|  |  |  | Delayed |  |  |  |
| 4 | Important | Internal: | Can be failed to | 4-48 | 2-24 | Daily |
|  |  | Financial systems | manual operations |  |  | replication |
|  |  |  | May slow operations |  |  | backups |
|  |  |  | Will not stop critical |  |  |  |
|  |  |  | activities |  |  |  |
| 5 | Non Critical | Internal: | Automated systems | 48+ | 24+ | Periodic |
|  |  | Test systems | Experimental systems |  |  | replication |
|  |  | Development | Marketing systems |  |  | backup |
|  |  | systems |  |  |  |  |

**3.1.3** **Common design considerations**

When designing a DR solution, agencies should take into account:

* The requirements arising from its business impact assessment. This should include RTO/RPO of business application systems, the outage impact (criticality) of ICT services to the business.
* System hardware including both server and storage hardware.
* System software.
* Network infrastructure including all LAN and WAN routers, switches, network security devices, connectivity including pipes, bandwidth and inter-site connectivity.
* Common services such as DNS, DHCP, active directory, access control, remote access, file & print, phone, etc.
* Time constraints (fall-back, service level agreement commitments, RTOs and RPOs).

Page 7

* Inter-system dependencies such as data synchronisation between different applications; inter-system functional dependencies such as internet connectivity depends on DNS.
* Site dependencies - data centre distances and their functional relationships (e.g. active/active versus active/passive or manual configuration, distance & time for tape backup retrieval, etc.).
* Data corruption issues.

During the detail design phase, the following areas should also be considered for procedure development:

* Types of services ICT offered to the business.
* Existing service level agreements or business arrangements.
* Physical and environmental considerations such as:

o Facility ownership, parties involved in controlling the facilities, systems, and services

* 1. Services and recovery sequence required from each site including physical access and equipment required for recovery such as tapes, etc. This is especially important when dealing with critical infrastructure which might be remote and hard to access.
* Data backup, replication, restoration and system configurations methods.
* Level of recovery capability expected by the agency/business (full or partial data centre recovery).
* Handling of network failover, IP address space, CNAME records, DNS settings and other related issues.
* Service management (resource, configuration, change, capacity, availability, security, etc.).
* Application interfaces including data synchronisation issues, recovery points of different systems supporting a related business process or service.
* Information security such as access control, authentication and authorisation, encryption, logging, etc.
* Lessons learnt from DR testing and incident events.

**3.1.4** **Minimum design considerations**

As a minimum, an agency should assess and document its current disaster recovery solution. This capability should be communicated to the business systems owner.

For any new or updated systems, it is recommended that ICT staff establish a risk process based on BIA inputs and implement a capability that suits the agency’s need.

The DR design process should achieve these objectives:

* a formalised methodology to design and implement DR solutions for new and updated systems
* communicate and review with the business to ensure the DR solution meets their needs
* have an agreed allocation of resources (including budget) to operate, monitor, review, maintain and improve overall disaster recovery capabilities.
* The key components below are common to most of the solution designs:
* critical applications with levels of recovery objectives (RTO/RPO) defined
* recovery strategy and recommendations

Page 8

* recovery resource (including capability) requirements
* definition of service levels
* third party dependencies
* current production environment
* proposed recovery strategy and solution options
* issues and concerns, lessons learnt.

**3.1.5** **Completing the solution design**

The solution design process will enable you to create a recovery solution that aligns to the organisational strategy, policies and requirements. The solution, once implemented, would become a business recovery service. In most cases, the business recovery services initially implemented may not be fully capable and may not be mature enough to fully protect in the event of multiple disasters. Also, for each disaster, the actual damage, strategy and tactical efforts required to rebuild the damaged services back to normal are unknown at the solution design stage.

Hence, to complete the solution design, incorporate a strategy for return to normal (business-as-usual) operation. You can consider the solution to be complete when the end result will be:

* full capability and capacity as before the disaster
* full DR capability as before the disaster.

There will be some period where the system operates in an interim operational state, during which capability, capacity and protection against failure may be reduced. The solution design should clearly identify this interim state, and set a time for full return to normal operation. These stages are shown in Figure 2 as “Recovery to DR site” and “Restoration to Production site”.

Page 9

1. **Recovery Plans**

****

This section highlights the essential elements and key considerations of a disaster recovery plan.

The strategy for creating and managing disaster recovery plans will vary according to the size of an agency’s ICT operations. A very small agency with one or two key systems may be able to produce a single holistic plan that encompasses complete recovery of those systems in the event of a disaster. However, as the number of systems and their interdependency increases, it becomes necessary to apply more complex structures to the planning. This may result, for example, in a hierarchy of documents rather than a single comprehensive document.

The advice provided here is for guidance only. Each agency should develop recovery plans relevant to its own environment. The most important question to ask of any disaster recovery plan is “Does it work?”

That is, does the plan deliver what it set out to achieve in terms of data centre recovery, infrastructure recovery, application recovery, service recovery, and so on?

1. **Organising recovery plans**

Agencies should aim to develop self-contained recovery plans without unnecessary reference to other disaster recovery, service recovery or application recovery plans. This is reasonable for small numbers of systems and simple services, and it makes it easier for agencies to procure services and move to different service providers. For more complex system and services, incorporating all elements of recovery into a single plan document becomes more difficult. In this case it can help to create a hierarchical structure of plans.

Figure 3: Basic plan hierarchy.



Whole of ICT DR Plan

Business Service Recovery

Whole ofPlansICTDR Plan

Whole of ICT DR Plan

Application Recovery Plans

Whole of ICT DR Plan

Whole of ICT DR Plan

Technical Recovery Plans/

Procedures

Core Services Recovery Plans

Whole of ICT DR Plan

Whole of ICT DR Plan

Infrastructure Recovery Plans

Whole of ICT DR Plan

Whole of ICT DR Plan

Data Centre Facilities

WholRecoveryofICT DRPlansPlan

Whole of ICT DR Plan

Each element of the hierarchy references the element immediately below rather than explicitly reproducing its contents. This can be a “one to many” relationship or vice versa. Instead of filling a document with all of the information to recover 25 business servers, the *Whole of Disaster Recovery* *Plan* will say“refer to these 25 differentBusiness Service Recovery Plans,” and so on.

When the level of application recovery plan is reached, it and the elements below will each refer to associated technical recovery plans. The recovery plans in the hierarchy are meant to be used by a person coordinating disaster recovery activities. They would usually follow the structure set out in

Page 10

section [*4.2 Anatomy of a disaster recovery plan*.](#page14) On the other hand, a technical recovery plan is intended for technical and functional support teams to use. It will spell out in detail the systematic actions to be taken to recover an ICT service or system.

Agencies may have multiple business services that feed into each other. To make maintenance of the plans easier and less time consuming, do not:

* repeat information at different places in a document
* repeat information at different levels of the hierarchy (for example, don’t repeat the site details from a facilities recovery plan in all of the application recovery plans)
* refer upwards in the hierarchy, only down (for example, do not refer from an application recovery plan up to a service recovery plan).
1. **Anatomy of a disaster recovery plan**

An effective DR plan should consider both the restoring and reconstitution of ICT services. Below is a high level outline of sections that should be considered in a DR plan. Adoption of a standard template for DR plans can assist ICT staff to reliably execute DR procedures or conduct DR testing of ICT services.

The suggested sections are:

|  |  |
| --- | --- |
| Sections to be considered | Comments |
| Introduction |  |
| Scope | What is this plan meant to achieve (data centre recovery, |
|  | infrastructure recovery, application recovery, service recovery, etc.)? |
| Applicability | Under what circumstances can this plan be used? |
| Inclusions | What is specifically dealt with? |
| Exclusions | What is not covered (for example, simultaneous recovery of both |
|  | primary and backup sites; recovery of ancillary systems)? |
| Assumptions | For example, it is an assumption that the backup/standby |
|  | infrastructure will be available and in good working order at the time of |
|  | a disaster? |
| Associated documents | It is probably better to avoid referring to international standards or |
|  | other external documents here as these just add to the document |
|  | maintenance burden without adding much value. Such standards could |
|  | instead be referenced in an overarching DR strategy |
|  | document. Examples of associated documents would be the recovery |
|  | plans for essential ICT services on which your service depends, such as |
|  | the plan for recovery of the underlying network |
| Glossary of terminology, | It is very useful to expand and explain in-house terminology or |
| abbreviations and acronyms | abbreviations for uncommon technologies. Avoid defining or |
|  | expanding on industry standard terminology or abbreviations |
| System profile | What is it? What is it for (from the business point of view)?, What does |
|  | it comprise?, How is it constructed? How is it protected? |
| Scenarios and responses | Specific examples of failure scenarios and brief commentary on how |
|  | the DR plan should be used to address them |
| High-level DR solution | High-available solution or restored from tape (or other backup media), |
|  | DR distributed across active sites or active passive sites etc. |
| Recovery strategy | High level description of the recovery strategy. It is recommended that |
|  | the metrics - RTO, RPO, etc. are referenced here |
| Recovery process map | It is worthwhile to include a flowchart showing the steps required to |
|  | have a disaster declared and execute recovery. Explain the roles that |
|  | have authority to declare and manage a disaster and disaster recovery |
|  | operation. Ensure that back-up personnel for these roles are included |
|  | and make it clear that the responsibilities are role-based and, |
|  | Page 11 |

|  |  |
| --- | --- |
|  | therefore, would be assumed by anyone acting or relieving in those |
|  | roles. Provide information about escalation paths |
| Communication plan | Plan for incident response and escalation |
| Recovery team | Who do you need to recover the service? |
| Recovery gaps/risks/issues | Identify any known gaps in the recovery plan. This in particular is a |
|  | living section of the document that should be updated to reflect |
|  | defects encountered during testing. For example, it might be known |
|  | that firewalls are always an issue and that the process for firewall rule |
|  | changes is particularly difficult and onerous, which poses a threat to |
|  | the RTO |  |
| Return to normal operation | How does the service return from its DR state to business-as-usual |
|  | operation? This includes the return to having a full production and DR |
|  | capability |
| Supplementary information | References to: |
|  |  | contact details |
|  |  | site details |
|  |  | critical supplier details |
|  |  | software licences |
|  |  how to source key password information (location only). |

1. **Technical recovery plans**

A technical recovery plan or procedure provides a systematic recovery protocol that can be executed by any suitably qualified person. It should not rely upon any organisational or environmental knowledge, but rather should either be explicit about the exact parameters of a particular task or should refer to another document in the DR plan hierarchy that provides the necessary information (for example, how to change DNS entries).

Technical recovery plans or procedures are not intended to cover the same elements as DR plans. They don’t usually refer to the business. An example of an implemented technical recovery plan may have the procedures shown in the following diagram.

Page 12

Figure 4: DR plan stages



|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Start |  |
|  | End | Determine DR |  |
|  | Scenario |  |
|  |  |  |
| DR Policy, | ICT DR Plan | DR Scenario |  |
| Strategy | Plan |  |
|  |  |
|  | Recovery to Production |  |  |
|  |  | Recover to DR site | Restore to Production |
|  |  | Site |
|  |  |  |
|  |  | Infrastructure | Infrastructure |
|  |  | Recovery |
|  |  | Procedure | Restoration |
|  |  |  | Procedure |
|  |  | Application | Data |
|  |  | Recovery |
|  |  | Restoration |
|  |  | Procedure |
|  |  | Procedure |
|  |  |  |
|  |  | DR UAT | Application |
|  |  | Restoration |
|  |  | Procedure |
|  |  | Procedure |
|  |  |  |
| Application |  |  |  |
| System Operations |  | Determine DR | DR UAT |
| Manual |  | Procedure |
|  | Scenario |
|  |  |  |

Page 13

1. **Plan testing, exercising and verification**

****

This section provides high level guidance on testing, exercising and verification of the DR plan. Testing and verification is a major component of the DR framework and reference should be made to the DISP which recommends a minimum requirement to be included within the DR policy. *Please refer to section* *3 for details on Policy and Framework.*

Testing of the DR plan verifies the agency’s DR strategies against expected criteria that are measurable. These criteria are developed in the DR design process and give the business a degree of confidence that it can meet its recovery time objectives. Conduct of exercises should practise personnel in the performance of their allocated responsibilities. Both testing and exercising areimportant elements in the maintenance of an agency’s business continuity, disaster recovery capability and awareness.

Each agency will have a different approach to testing and exercising its DR capabilities and arrangements. The chosen testing methods employed and exercise frequency should be balanced against costs and time to reflect the agency’s risk profile. For example, sometimes, it is important to test the detailed DR capabilities at the functional and components level to ensure the DR or fail-over technology works according to expectation. These technologies include redundancy, resilience, auto-recovery, auto-restoration, virtualized environment, etc.

1. **Progressive test and exercise program**

The ISO27031 standard suggests an organisation should test and exercise all of its ICT service recovery plan as appropriate to its size, complexity and scope. These exercises should not only focus on the recovery of services but also examine the resilience of the ICT framework, system monitoring and alarm management. Below is a diagram to consider when developing the testing strategy.

Figure 5: A progressive test and exercise program, ISO27031:2011



Desktop process

Recovery simulation

review



Integrated



Component

Familiarisation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Desktop walk |  | Individual |  | Integrated end- |
| through of |  | application or |  |
|  |  | to-end service |
| invocation and |  | infrastructure |  |
|  |  | recovery tests |
| recovery process |  | component |  |
|  |  |  |
|  |  |  |  |  |



Operational



ICT Services

Resiliency



ICT component and end-to-end services switching between primary and secondary

Page 14

1. **Testing the disaster recovery plan**

Planning for a test to validate the DR plan is paramount. Testing represents opportunities to:

* identify deficiencies in an agency’s disaster recovery processes so they can be corrected
* train staff in the agency’s DR response and improve their technical capabilities through practical rehearsal
* verify that the DR environment will perform as expected (within published recovery times and acceptable outage limits)
* update plans to ensure they accurately reflect the agency’s current situation.

Figure 3 in section 3 also represent the end to end disaster recovery operational sequences.

See [Appendix C –Test Plan Example.](#page35)

**5.2.1** **Test planning**

Planning for a test comprises:

* agreeing on scope and objectives that validate the detail in the DR plan
* defining scenarios with clearly defined entry and exit criteria, including test acceptance criteria
* Identifying test participants, including any business test users
* identifying risks associated with the test and arriving at risk mitigation strategies and actions, noting any residual risks
* identifying key stakeholders and establishing a briefing process including frequencies during the test
* documenting the plan for the test. The test plan should not duplicate processes and procedures in the DR plan
* socialising the test plan with the business and key stakeholders and having it endorsed accordingly.

**5.2.2** **Test roles and responsibilities**

It is important to assign someone the role of a disaster recovery manager or coordinator to facilitate and plan the test. The role should also be responsible for:

* engaging all stakeholders and test participants
* tracking the risks associated with the test
* monitoring and tracking the test schedule
* briefing during the test
* conducting post-test reviews
* writing the test report and obtaining business and/or stakeholder endorsement/approval
* logging of all issues encountered as part of the test
* ensuring the ICT disaster recovery plan is updated as appropriate
* assigning responsibilities for each follow-up test action.

Page 15

1. **Testing of outsourced ICT**

Under the DISP each agency remains accountable for DR testing when their ICT is outsourced or procured “as a service”. Under such arrangements, it is essential that the agency confirms the service provider’s DR capability and compares it to the requirements of the business. Ideally, the agency should stipulate the DR requirement in the service contract. Under an outsourced arrangement a service provider should develop a DR policy, strategy and solution, and undertake testing. The agency should also consider periodically observing the testing processes as part of the service level monitoring and audit processes.

The agency should include the following DR requirements in the third party provider service contract agreement, with performance measurement defined:

* + the required service/system recovery time objectives (RTO) and recovery point objectives (RPO)
	+ documented DR plans, review and testing frequencies of each of the plans
	+ provision of DR test reports and details of corrective measures
	+ assurance from the providers that they have a business continuity and disaster recovery program and are able to provide assurance that these are maintained and exercised annually.
1. **Types of testing**

The DR Plan can be tested in the following ways:

|  |  |
| --- | --- |
| Type of testing | Descriptions |
|  |  |
| Hypothetical testing |  Scenario-based desktop walkthrough simulated test to |
|  | confirm and validate the processes and procedures |
|  | documented in DR plans are relevant and practically |
|  | applicable. |
|  |  DR plans for DR (non-production) systems event simulation. |
|  | It is a scenario-based exercise from “system outages or |
|  | downtime scenarios” up to walkthrough of the execution of |
|  | “the technical recovery or restoration procedures” of the |
|  | overall and individual DR plan on the DR systems. |
| Simulation testing |  Component disaster recovery testing |
|  | Unit or component testing of the ICT disaster recovery |
|  | solution. These may include testing: |
|  | a. Back up and restoration procedures of a single system |
|  | b. Network switching from one site to another |
|  | c. Restoring one infrastructure environment. e.g. |
|  | mainframe LPARS. |
|  |  Multiple systems DR testing |
|  | This involves testing of clusters, including multiple systems |
|  | and services which have dependencies and increases the |
|  | complexity of the tests. Repeat this test with backup team |
|  | resources to ensure the plans and procedures are |
|  | validated. |
|  |  Full DR testing |
|  | This is listed for completeness but carries significant risk, cost |
|  | and impact for agency resources |
| Real incident/Near misses |  DR plans for single systems or hardware may have been used |
|  | Page 16 |

to restore service in a real incident. Agencies should take advantage of and record (under issues management) the lessons learnt and/or remedial issues identified that would apply to the DR steps/actions taken.

Agencies should consider a combination of testing approaches to test the response in terms of difficulty and complexity. For example, begin with hypothetical testing and progress to testing the DR plan in conjunction with the agency business continuity plan, or conduct surprise DR test scenarios.

1. **Test frequency**

The DR policy usually sets out the frequency of testing. Testing has cost and resource implications as it diverts resources and staff from daily activities. Agencies may develop a hierarchy of DR plans each of which will have different test frequencies. For instance, DR plans for mission critical applications may be tested quarterly or twice yearly while less critical system plans will be tested annually.

The following should be considered by an agency when planning tests:

* Develop a calendar for DR testing. This calendar should be developed jointly with the business and published.
* Make new projects or programs aware of the testing calendar before they begin their scheduling activities, as DR testing may make production unavailable.
* Postpone a scheduled test only as a last resort rather than a norm.
* Advise the business of the risk of not conducting a test in favour of other competing priorities so they can review and accept the advice.
* In scheduling full production DR tests, consider grouping testing systems according to their user base to minimise disruption to the business. This is not always practical or desirable as the demand on the staff executing and testing the DR plan may prolong the total outage.
* Government agencies often face constraints on their working hours and overtime budgets. If this is a factor, consider scheduling DR tests for some systems during core business hours. This is usually only acceptable for services that are invisible to the general public (such as a staff portal). Proceed carefully in such cases - unexpected faults or problems that cause a prolonged outage may cause unnecessary negative perceptions among the user community.
1. **Test reports and issue management**

Each agency should develop test report templates to standardise test reporting and align with relevant DR plans.

Each DR scenario test should generate a report to address:

* objectives
* scenario
* assumptions and prerequisites
* resources, including people, process and technology
* findings and observations, including:
	+ success, failure, self-recovered and unrecovered errors
	+ risks
	+ accuracy
	+ unplanned actions

Page 17

* + unpredicted events
	+ observation, including positive outcomes that would benefit future testing, etc.
* summary of issues and risks that should be addressed in order to prevent them from re-occurring
* completed test logs or checklist.

The objective of issue management in testing is to document issues or findings, remediation plans, and exception plans that result.

In order to support issue management in DR, DR testing needs to document issues, deficiencies, and lessons learned or gaps found through testing DR plans, performing assessments, and controlled testing. These items should be correlated to other like items already documented, analysed and resolved through an issue management process.

It is very important to have an issue management system to track the remediation of issues identified in DR testing to closure. Once an issue has been resolved, it needs to be successfully retested before it can be decided whether the solution is a permanent or temporary fix. Delays can then be escalated to management for action. These items should be captured, correlated to other similar items already documented, and resolved through an issue management process.

Page 18

1. **Program maintenance and continual improvement**

****

This section focuses on how to maintain the DR framework as a program, ensuring that the agency’s DR capability is maintained and continually improving its effectiveness. DR program maintenance is comprised of monitoring, reviewing and evaluating; reporting; auditing; control/treatment of non-conformities; and continual improvement.

DR program continual improvement collates inputs from monitoring, reviewing, evaluating; reporting; auditing; control/ treatment of non-conformity; DR risk management and changes and maintenance drivers to evaluate the overall program performance and identify improvements.

The DR program also ensures that DR policy, strategies, solutions and plans are up-to-date, viable and applicable. Testing, reviewing and validating are key components of the maintenance phase that will reassure management about the DR program and DR plan and highlight any risks associated with DR program that need to be escalated and treated.

DR program maintenance should incorporate a risk register, a remediation plan and cater for any changes in the program as well as the ICT environment.

1. **Monitoring, reviewing and evaluating**

While implementing this framework component, the following requirements should be observed:

* capture any threats or risks during any DR activities and enter them in the risk register
* measure performance targets especially when DR function is outsourced. For example, common measurements such as RTO/RPO are already incorporated during the strategy, design phase and subsequently integrated into the DR plans. These could also be part of the SLA agreements with the service provider
* monitor the performance targets set
* connect to ICT incident and problem management to monitor the impact on DR scenarios, plans and processes.
1. **Reporting**

Reporting is a key component of the DR framework implementation and underpins the success and continual improvement of the overall DR function.

During the implementation, the following reports should be considered and introduced:

* DR testing and verification (section [5,](#page17) DR testing report)
* DR audit report or any internal or external audit reports that have assessed aspects of DR or DR functions
* overall DR program review report.
1. **Auditing**

Auditing the program ensures that the DR plans are accurate, up-to-date and fit for purpose. An ongoing DR audit program should be implemented.

The following should be considered:

* develop an audit plan which outlines the scope of auditing, audit responsibility, frequency, method and audit criteria

Page 19

* appoint qualified staff to undertake ITSC audits
* ensure that audit deficiencies and remediation actions are assigned, prioritised and monitored for completion
* ensure that audit plans address both internal and external audit requirements
* ensure that internal audits are conducted on completion of major IT projects and implementation of large-scale IT changes
* ensure that results of all audits are recorded and reported.
1. **DR risk management**

These guidelines propose a simple method based on a risk register approach. Agencies should develop a risk assessment methodology with, for example, proper risk rating, risk acceptance criteria, that aligns with their own risk management framework in order to make it meaningful and practical.

The DR risk register enables an agency to capture the identified risks, evaluate them and determine the action required to mitigate them. These risks include those that could result in the failure of the disaster recovery process.

The DR risk register records:

* risks or threats identified during DR program planning and implementation (similar to project risks)
* risks or threats identified during DR testing and verification
* issues (eventuated risks) identified during actual disaster recovery events or tests
* non-conformities (control or process failure) identified during audits, reviews, operations, etc
* continual improvement actions items identified during monitoring, evaluation, reviews, etc.

The DR risk register should have the following elements:

* identified risk (a brief description) and possibly a reference identifier
* detailed descriptions of identified risks including source of risk, events, location, or refer to other documents
* vulnerability (usually this is the root cause of an issue) and threats (usually this is the issue)
* likelihood of recurrence
* degree of impact on the success of DR execution
* remediation control (solution to address the root cause of an issue or fixes of an issue)
* assignment of responsibility for remediation control
* control action implementation status
* control effectiveness measurements.
1. **Control and treatment of non-conformity**

DR controls are broadly interpreted as action items to address issues and to mitigate risks. These actions also include treatment of non-conformities identified during audits and control effectiveness assessments.

A control can be a one-off action, temporarily put in place, or a permanent solution that requires monitoring to ensure it remains functional and effectively addresses the identified risks or issues.

Page 20

If controls are not effective and fail to be functional, they need to be rectified by adding control/s or replacing the existing control.

1. **Control remediation**

The purpose of control remediation is to improve the effectiveness of the controls. Solutions should be defined to address the issues identified during an audit and control effectiveness assessment.

A consolidated remediation plan comprised of findings from multiple remediation projects is recommended, as it helps to identify larger issues and supports informed management decision making.

1. **Program changes and maintenance drivers**

The three primary drivers for undertaking maintenance of the DR program and DR plan are:

* **Testing and validating capability**

o Conducting capability exercises

o Conducting desktop exercise

* 1. Activation of the disaster recovery plan.
* **Changes impacting the program**

Changes in or to:

* 1. Location of normal place of business

o Business critical services

o Business functions / processes

o Recovery site

o Architecture / platform

o ICT systems or services

* 1. Third party service providers.
* **Changes impacting the plan**

Changes in or to:

* 1. Escalation strategy

o Communication strategy o Team membership

o Roles and responsibilities o Internal/external contacts o Recovery options

o Recovery procedures o DR testing calendar.

Page 21

1. **Program maintenance activities**

The following check list focuses on the key elements that underpin the DR program and plan, and that need to be considered as part of DR program maintenance:

* Ensuring the documented DR plan is current.
* Aligning DR objectives and strategy with business priorities.
* Ensuring that identified DR plan prerequisites are reviewed and actioned.
* Conducting a walkthrough for personnel requiring training.
* Validating the recovery procedures and options.
* Validating issues register activities have been actioned.
* Ensuring personnel understand their roles and responsibilities.
* Verifying alternate site technology.
* Verifying hardware platform requirements.
* Submitting DR status and recoverability reports.
* Checking version control is up to date and complete.
1. **DR program continual improvement**

DR program review inputs would include actions arising from:

* DR testing and verification
* monitoring, review and evaluation
* audits
* reporting
* controls
* remediation
* maintenance drivers or triggers.

Outcomes of the DR program review would be the inputs to DR program continual improvement action items. The DR program review should comprise the following components:

* overall DR objectives
* DR incidents and recovery events
* DR testing results
* evaluation of current DR risks identified, mitigation status and control effectiveness assessment
* non-conformities identified during audits, tests and recovery events
* initiation, endorsement, approval of continual improvement action items
* proposed changes to the policy, objectives, action items, etc.

A program review report should be produced to give management a snapshot of the DR program performance and recommendations. The aim of this report is to propose and seek management endorsement for the changes and/or improvements required as stated above.

Page 22

1. **Training and awareness**

****

During the development of DR plans, it is essential that staff, contractors and consultants are familiar with the functions implemented and that they are confident and competent in operating them. The effectiveness of the DR program will be greatly enhanced if everyone is aware of and understands the DR plan content, knows what is happening, knows what their roles and responsibilities are, and if everyone is working towards the same objective.

DR training and awareness program, agencies:

* develop an appropriate DR training program to ensure staff, contractors and consultants with DR responsibilities have the required knowledge and capability to perform that role:
	+ determine who the training is targeting and materials required for the targeted audience
	+ determine how training will be delivered to your audience (employee inductions, Intranet or online training system)
	+ decide whether the training is to be mandatory or optional for relevant groups of staff.
* undertake annual training and awareness and ensure that it is overseen by the relevant agency DR representative:
	+ determine the level of training and awareness for targeted audience
	+ schedule training and awareness into the annual DR test exercise calendar
	+ give management an annual status update on awareness across the agency.
* ensure that awareness activities include making staff aware of the business priority and impact of their roles, conducting workshops with staff, and recognising the positive contribution of staff where warranted:
	+ involve business owners, business operational staff and ICT staff in combined scenario testing, desktop walkthroughs and live exercises to increase knowledge and understanding.

Page 23

**Appendix A - Implementing an DR program**

****

**Strategise and plan:**

* draft a charter to gain agreement on the vision for the DR Program. Agencies may require a draft business case showing how it aligns with the agency goals
* confirm scope for the DR, establish resources and budget
* integrate with other dependent programs or business areas i.e. strategic and or operational IT; BCM program; information security management and or risk and audit
* define the program performance indicators (KPIs) and reporting processes.

**Develop program governance:**

* establish an optimal process for making decisions and assigning decision rights across the agency, including ICT, in respect of DR. For instance:
1. identify the executive sponsor whose role will be to promote the program at the most senior levels and influence the strategic vision or objective.
	1. assign a dedicated program manager (for smaller agencies this may be a part-time role). This person would be the primary point of contact for DR matters and is accountable for the growth of the program.
* identify and engage stakeholders and consider how the program will communicate with these stakeholders: :
	1. For larger more ICT complex agencies, for instance, it may be appropriate to establish an DR Committee or the matter may be a regular agenda item in the agency CIO Meetings or BCM Committee or Executive meeting.
* agree on authority and flow for decision-making
* implement and set up feedback mechanisms.

**Drive change management:**

* communicate and socialise ideas via multiple channels
* get buy-in from stakeholders at all levels
* implement agency process changes in a controlled manner
* assess progress and drive stakeholder commitment to change.

**Execute -implement:**

* develop an implementation plan for the DR activities to be under taken by whom with timeframes
* monitor and implement the necessary changes
* update and drive new elements of the initiative in response to changing agency requirements.

**Measure and improve:**

* measure how DR has affected agency outcomes. Has it met its KPIs?
* seek feedback from stakeholders
* drive improvements through process changes and upgrades.

**Appendix B – DR Policy Examples**

****

**Detailed Policy Example**

|  |  |
| --- | --- |
| Effective Date | ***<Insert policy issue date>*** |
|  |  |
| Version | 1.0 |
|  |  |
| Issuer | ***<Executive Sponsor>*** |
|  |  |
| Owner | ***< Office of the Chief Information Officer>*** |
|  |  |
| Executive Statement | ***<Agency>*** is committed to providing its stakeholders with an enterprise wide DR |
|  | Strategy<***or program>,*** including policies, standards, risk mitigation controls, procedures |
|  | and action plans. An DR Strategy **<program>**is a key component of <***our corporate*** |
|  | ***governance initiative or ICT strategy or continual improvement or risk management*** |
|  | ***commitment – specify >.*** |
|  | The DR program is designed to ensure that a risk management approach is in place |
|  | enabling ***<Agency>*** to have the appropriate ICT resiliency including ICT disaster recovery |
|  | planning so that the long term viability and continued service delivery to the agency is |
|  | maintained at predefined levels in the event of ICT interruptions. |
|  | This document establishes the DR program policy for ***<Agency>***, which is endorsed by |
|  | ***<Agency>***'s executive management team. |
|  |  |
| Definitions | *DR* is the practice of planning, building, running and governing activities to ensure that |
|  | ***<Agency>***: |
|  |  identifies and mitigates operational risks that can lead to ICT disruptions *before* |
|  | they occur |
|  |  prepares for and responds to disruptive events (natural or man-made, accidental |
|  | or intentional) in a manner that demonstrates command and control of the ICT |
|  | event response |
|  |  recovers and restores ICT systems, that support mission-critical agency operations, |
|  | within pre-defined timeframes and with acceptable data loss following a |
|  | disruption. |
|  | DR relates to other management process as these will facilitate the delivery of a holistic |
|  | DR program |
|  |  Business Continuity Management informs DR by identifying and prioritising the ICT |
|  | systems that support the most time sensitive – critical services for which alternate |
|  | workarounds are not practical |
|  |  risk management informs DR by identifying unacceptable ICT related risk, |
|  | establishing cost effective controls, DR Plans being one such control. Risk |
|  | management defines the agency risk appetite |
|  |  ICT service continuity informs DR by establishing the agency ICT incident, change, |
|  | release, problem management protocols which would continue to apply during an |
|  | DR response |
|  |  information security management informs DR by defining the levels of security |
|  | applicable to ICT systems including DR infrastructure and during recovery events |
|  |  asset / supplier management informs DR and vis a vis the timely supply of ICT |
|  | assets during a disruption will be negotiated prior to the disruption; appropriate |
|  | maintenance and SLA agreements will accommodate the agencies needs during |
|  | activation of its DR Plan. Where DR services are purchased this policy must be |

|  |  |  |
| --- | --- | --- |
|  |  | followed. |
|  | *Disruptive events* may be short term disruptions to service continuity where there is a |
|  | requirement to activate a single system DR plan or it may be a wider disruption |
|  | threatening business continuity where ***<agency >*** will activate its Business Continuity Plan |
|  | (BCP). In this latter scenario the agency wide DR Plan including any DR system plans will be |
|  | guided by the priorities of the BCP. |
|  |  |
|  |  |
| Guiding Regulations | ***<Insert a list of industry, contractual and national regulations and other guiding*** |
|  | ***directives requiring a DR program for your agency. Examples include:>*** |
|  |  |  ISO 27031: Information technology – Security techniques: guidelines for ICT |
|  |  | readiness for business continuity |
|  |  |  TPP15-03 Internal audit and risk management policy for the NSW public sector |
|  |  |  agency risk management policy |
|  |  |  agency business continuity policy. |
|  |  |
| Scope | ***<Insert a clear, concise description of the business entities, workforce components,*** |
|  | ***locations, facilities, business processes, assets, business partners and joint ventures*** |
|  | ***covered by this policy. Exclusions to this policy should also be stated here. Examples*** |
|  | ***include:>*** |
|  | This policy applies to |
|  |  | all full-time and part-time employees, contractors and consultants doing business |
|  |  | on behalf of the agency who must comply with the policy |
|  |  | all business units and divisions, regardless of their location, who must consider |
|  |  | how the DR policy factors into their operations and service delivery commitments |
|  |  | all legal entities, suppliers and vendors working on or supplying the agency with |
|  |  | ICT who must be familiar with this policy especially in relation to ICT recovery and |
|  |  | data loss recovery timeframes. |
|  |  |
| DR Objectives | The objective of DR is to ultimately enhance the agencies resiliency in regards to its ICT so |
|  | that it can effectively minimise, respond to and recovery from ICT threats. ICT resiliency in- |
|  | turn supports the agency’s overall business resiliency and business continuity |
|  | effectiveness. |
|  | ICT has a critical role in the business’ ability to deliver its services to the wider public |
|  | sector. The objectives of DR are to: |
|  |  | minimise the impact on the agency operations of ICT related disruptions by having |
|  |  | in place effective responses including ICT incident management and ICT disaster |
|  |  | recovery plans |
|  |  | support an agencies service level commitments so that ICT systems underpinning |
|  |  | the agencies most business and or time critical functions are recovered as a |
|  |  | priority to less time critical system |
|  |  | have staff, suppliers and vendors competent and familiar in there delivery of DR |
|  |  | provide evidence based criteria on which to develop DR strategy |
|  |  | implement a continuous improvement process aligned to business continuity. |
|  |  |
| Assumptions | ***<Insert a list of assumptions that impact — positively or negatively — the*** |
|  | ***implementation of the DR program. Remove this section if you don't have any.>*** |
|  |  |
| DR Program Policy | The goal of DR is to manage risk. |
|  |  |  |

|  |  |
| --- | --- |
| Statement | ***<Policy statement may articulate that the agency will adopt a risk- based approached to*** |
|  | ***DR activities by defining the accountability, roles and responsibilities, response, and*** |
|  | ***recovery which aim to protect the agency from the loss or disruption to its information*** |
|  | ***technology and communications.>*** |
|  | That DR will be aligned with the agencies BC policy, information security and risk |
|  | management policy, that this will be achieved by |
|  |  requiring all ICT projects or system enhancements to comply with DR policy and |
|  | framework including classification of new systems into the agency’s DR tiers and |
|  | having a documented DR asset / system plan |
|  |  requiring contracts for ICT services provided by vendors / supplies to include |
|  | assurances for DR including detailing system recovery times and potential data loss; |
|  | evidence of DR plans and regular testing of plans |
|  |  DR implemented and managed in accordance the processes and procedures set out in |
|  | the DR program framework. |
|  |  |
| Roles and | <I***nsert the roles and responsibilities of all stakeholders, identifying their specific*** |
| Responsibilities | ***responsibilities for any actions relating to the policy or to DR in general, as well as their*** |
|  | ***compliance responsibilities. >*** |
|  |  The board of directors and CEO: Responsible for ensuring that this policy is |
|  | adopted and implemented across the organisation. |
|  |  Executive management: Accountable for DR, and must ensure compliance with DR |
|  | policies, standards, risk mitigation controls, and procedures within their respective |
|  | areas of responsibility. |
|  |  Committee ***< eg DR program policy and program compliance governance/ DR*** |
|  | ***steering committee/ BCM Steering committee may also incorporate DR>:*** DR |
|  | program policy and program compliance governance is provided by a |
|  | multidisciplinary group, referred to as the <"BCM steering committee or DR |
|  | steering committee”>which reviews and endorses the DR program policy |
|  | objectives and strategies. The members of this group agree to the roles and |
|  | responsibilities of DR across the enterprise, as defined in specific policies. They |
|  | actively and visibly promote and provide business support for DR initiatives |
|  | throughout the enterprise. The governance group is led by ***<the BCM office or CIO*** |
|  | ***or IT Operations Executive>***and includes representatives from all major business |
|  | units, as well as ***< for instance, corporate security, facilities management, IT*** |
|  | ***strategy, IT operations, projects, business operational areas>*** |
|  |  Business unit management: Each business unit executive is responsible for |
|  | ensuring that their business unit implements the requirements of this policy and |
|  | builds resilience into day-to-day business operations. |
|  |  Risk management: Responsible for oversight and risk management advisory |
|  | activities of the DR program — one element of the enterprise risk management |
|  | program — including risk assessment, business impact analysis, and overall DR |
|  | program management integration, into the enterprise risk management program. |
|  |  Audit management: Responsible for the periodic audit of the DR program. |
|  |  Public relations/corporate communications/investor relations: Responsible for the |
|  | development and implementation of all communications to all stakeholders |
|  | regarding the details and impact of the ICT business disruption. |
|  |  CIO: Responsible for ensuring that the IT disaster recovery management program |
|  | is implemented according to business recovery requirements. |
|  |  Chief information security officer: Responsible for ensuring that information |

security risks that could be exploited and lead to a business disruption are addressed in the DR program.

* BCM office: The BCM office is responsible for planning, building, running and governing the implementation of ***<Agency>***'s BCM program. The office is responsible for ensuring that appropriate preparedness, response and recovery policies, standards, risk mitigation controls, procedures, plans, and solutions exist and are applied throughout the agency. This office is responsible for determining the methods used to implement and enforce BCM policies, for measuring and reporting on the level of compliance to such policies, and for advising the enterprise on preparedness, response and recovery-related issues on a day-to-day basis. The BCM office ensures, in particular, that BCM awareness is increased, and that all risk mitigation controls, plans and solutions are exercised on a regular basis. The office is responsible for reporting the status and effectiveness of the BCM program to ***<agency>***'s executive management team and board of directors. The BCM office is also the enterprise's primary representative in interactions with external emergency management authorities and forums.
* DR program implementation office / team ***<or Office of the CIO>*** in collaboration with executive management and the ***< DR / BCM steering committee>,*** determines the formation and reporting relationships of the DR office/ team. This includes appointing and managing individuals with appropriate skill sets to staff the DR office / team, as well as requesting the appointment of DR representatives in all business units to be part of the agencies DR implementation team. All business unit DR representatives will be empowered by their respective management teams to fully represent them in the development and exercising of all components of ***<Agency>***'s DR program.
* ***< May be that the BCM Office also reports and monitors the DR Program as well as BCM Program >***
* HR: Responsible for developing and coordinating all workforce recovery activities.
* Legal and compliance: Responsible for developing and coordinating all legal and regulatory issues related to the continuity of operations, as well as managing the legal consequences of a business disruption.
* Health/safety/medical: Responsible for developing and coordinating all health, safety, and medical strategies and activities resulting from a business disruption. This includes coordination with external entities, such as first responders, medical services and so forth.
* Facilities management: Responsible for developing and coordinating all facility management strategies and activities resulting from a business disruption. This function works closely with the HR and health/safety/medical functions.
* Physical security: Responsible for developing and coordinating all security strategies and activities resulting from a business disruption.
* General staff: All staff of ***<Agency>*** are expected to recognize the importance of DR, to be familiar with the policy requirements, and to support the implementation of DR processes and procedures at the time of a business disruption. This awareness can be built through an employee awareness program given to new employees, temporary workers and reinforced on an annual basis.

Employee job descriptions, performance agreements, and contractor and partner statements of work will document the nature and extent of key recovery roles and responsibilities in order to create the incentive and recognition for coordinating and maintaining DR program.

|  |  |
| --- | --- |
| ICT DR Program | The ICT program framework has the following components: |
| Framework |  | DR methodology to be followed ***< ISO 27031: Information technology*** ***–*** ***Security*** |
|  |
|  |  | ***techniques: guidelines for ICT readiness for business continuity>*** |
|  |  DR roles and responsibilities assignment |
|  |  | DR budgeting process |
|  |  risk assessment for DR process |
|  |  business impact analysis process |
|  |  plan development and maintenance process |
|  |  | o suite of plans, including: |
|  |  |  | DR Plan |
|  |  |  | DR Application Plans |
|  |  |  ICT System Recovery Plans |
|  |  | plan testing process |
|  |  | plan audit process |
|  |  | DR program assessment process |
|  |  ICT program reporting process |
|  |  DR program and plan communications process. |
|  |  |
| Monitoring and | Any person covered by this policy is obligated to report apparent non-compliance to the |
| Compliance | responsible ***<Agency>*** manager, as well as to the DR office/ team. Any non-compliance of |
|  | this policy may result in disciplinary action, up to and including the termination of |
|  | employment. |  |
|  | Periodic auditing of the DR program implementation against the BCM program framework |
|  | provides insight and guidance on general and selected aspects of <***Enterprise Name***>'s |
|  | BCM activities. The scope of each audit will be decided from year to year by the audit |
|  | committee. |  |
|  |  |
| Review and | To ensure that the importance of this policy is communicated uniformly throughout the |
| Ratification | agency, all members of agencies (DR governance group) will review, update and ratify, at |
|  | least annually, this DR policy. |
|  |  |
| Sources and | ***<Insert a list of references and other organizational policies that complement the DR*** |
| References | ***program policy. Examples include risk management, legal/compliance, facilities*** |
|  | ***management, HR, emergency management, health/safety and so forth. Examples*** |
|  | ***follow.>*** |  |
|  | Agency policies: |  |
|  |  | risk management policy |
|  |  business continuity management policy |
|  |  business continuity management plan |
|  |  | information security policy |
|  |  information security incident response plan |
|  | Frameworks and standards: |
|  |  International Organisation for Standardization (ISO) — 27001:2005, 27002:2005, |
|  |  | PAS 22399:2007, and 24762:2008 |
|  |  |  |  |

* Business Continuity Institute (BCI) — The BCI Good Practice Guidelines (international)
* Federal Emergency Management Agency (FEMA) — National Incident Management System (NIMS)/Incident Command System (ICS)
* HB 221:2004 Business Continuity Management (Australia)
* HB 292-2006 A Practitioners Guide to Business Continuity Management (Australia)
* ISO 22301 — Societal security — Business continuity management systems — Requirements
* ITIL v.3 (international) — "IT Service Continuity Management" is part of the "Service Design" book in ITIL v.3

Revision History

Next Review Date:

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Approver | Summary of Change |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**ICT disaster recovery strategy and management: Classifying ICT systems recovery tiers**

This document illustrates as an example by using the tiering model as the disaster recovery strategy for planning and developing DR plans and conducting DR tests. Once the DR strategy is developed with all the parameters filled, as in an example table below, DR Management in turn scopes the required disaster recovery investment, provides a platform to validate recovery priorities and clarifies terminology thus accelerating business unit buy in.

DR strategy includes formalisation of recovery strategy using tiering scheme/model and formalisation of recovery levels for all ICT system and services. The ICT tiers should be classified according to the importance of the ICT system and services to the agency, to the importance being driven by the time critical or otherwise essential services for which ICT is a critical enabler. Agencies may choose to associate the lower tiers with lower outage tolerance or vice versa. Virtualization and storage technology can also be used to bundle different tiers together for DR Recovery and DR testing.

Recovery tiering would identify and document recovery targets (RTO and RPO); it would extend the work of the BIA into an action oriented disaster recovery strategy. Establishing tiering will help manage business service level expectations. Although agencies often want to believe all of their systems are mission critical, they need to understand the cost trade off of faster recovery times versus minimised data loss. The goal of DR Strategy and Management is to communicate the trade-offs and help agencies to find the proper balance.

Any DR strategy and management should be developed to reflect the needs of the agency. Consider the following while using the tiering model:

* + aligning DR tiers or levels to business priorities (critical business functions supported by ICT are derived from the agencies BIA)
	+ classifying business critical applications and services into logical recovery tiers
	+ tiering or levels would indicate frequency of testing and exercising; % of applications per tier or level; % of DR Management (DRM) budget
* system redundancy, high available clusters, virtualisation replication and SRM, fail-over technology capability.

EXAMPLE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | Classification |  |  |  |  |  |  |  |  | Processing / Standby |  |  | Data/ DR |  |  |  |  |  |  |  |  |  |  |  | % of Solutions |  |  | % of |  |  | Testing & |  |  | Agency specific |  |
|  | Tier |  |  |  |  | Business Process |  |  | Business Criticality Measure |  |  |  |  |  |  | Availability |  |  | RTO |  |  | RPO |  |  | / applications |  |  | DRM |  |  | exercising |  |  | systems |  |
|  |  |  | level |  |  |  |  |  |  | Approaches |  |  | Protection |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | per Tier |  |  | budget |  |  | can be up to |  |  | /applications |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Must be |  |  |  |  |  |  |  |  |  |  |  |  |  | Domain Name |
|  |  |  |  |  |  |  |  |  |  | Critical systems dependent on |  |  |  |  |  |  |  |  |  |  | recovered |  | Must be recovered |  |  |  |  |  |  |  |  |  |  | System (DNS) |
|  |  |  |  |  |  |  |  |  |  | infrastructure — for example, |  |  |  |  |  |  |  |  |  |  | with or |  |  |  |  |  |  |  |  |  |  |  | LAN - |
|  |  |  |  |  |  |  | Support infrastructure for critical |  |  | Active / Active, |  |  |  |  | 24x7 scheduled |  |  | with or prior to |  |  |  |  |  |  |  |  |  |  |
| 1 |  | Foundational |  |  | networking, connectivity, DNS, |  |  | Replication |  |  | prior to |  |  |  |  |  |  |  |  |  |  |  | WAN - |
|  |  | business systems |  |  | Primary / Secondary |  | 99.99+% |  |  |  | mission-critical |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | enterprise directory and access |  |  |  |  |  |  | mission- |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | services |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | controls |  |  |  |  |  |  |  |  |  |  | critical |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | Critical services impacted |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 20-40% |  | 40-70% |  | Quarterly |  | Email |
|  |  |  |  |  |  |  | Critical business function and/or |  |  | Active / Active, |  |  |  |  | 24/7 scheduled |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | and/or revenue stops if |  |  | Database Logs, |  |  | 2 to 8 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  | Mission Critical |  | revenue impacting — generally |  | systems are lost — customer |  | Parallel or Stretched |  | Replication | 99.9% |  |  | hours |  | ≤ 2 hours |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | customer facing |  |  | HA |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | <45min/mo |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | interactions are interrupted |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 10-30% |  | 15-30% |  | Semi-annual |  |  |  |
|  |  |  |  |  |  |  |  |  |  | Services continue though data |  |  |  |  | CDP/ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Internal operations and/or |  | collection and transaction |  | Active / Passive, |  |  |  |  |  | 8 to 24 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 |  | Critical |  |  |  |  | Replication/ |  | 24/6 ¾ scheduled |  |  | ≤ 4 hours |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | customer relationship focused |  | processing may be delayed. |  | Warm Standby |  |  |  | hours |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | Snapshots |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | Operational workarounds exist |  |  |  |  |  | 99.5%<3.5hrs/mo |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Internal — with alternative |  | Support services that can fail- |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 10-30% |  | 5-10% |  |  | Annual |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | operations model |  | back to manual execution — |  | Active/Passive, Cold/ |  | Daily |  |  |  |  | 1 to 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 |  | Important |  |  | system loss may slow but will |  |  | Replication / |  |  |  |  |  | ≤ 24 hours |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Shared Standby |  |  | 18/7 scheduled |  | days |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | not stop business-critical |  |  | Backup |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | activities |  |  |  |  |  |  |  | 99% <5.5hr/Mo |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 10% +/- |  |  | 5% +/- | At least every |  |  |  |
|  |  |  |  |  |  |  |  |  |  | Systems of automation, |  |  |  |  | Periodic |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 18 months |  |  |  |
|  |  |  |  |  |  |  | Internal — departmental |  |  | Active/Passive, |  |  | 24/6 ½ Scheduled |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  | Noncritical |  |  | experimentation and |  |  | Replication / |  |  | > 3 days |  | 24- 48 hours |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | systems, experimentation |  |  | Shared Standby |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | promotion (marketing) |  |  | Backup | 98% |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | <413.5hrs/mo |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Appendix C –Test Plan Example**

****

DRP TEST DESCRIPTION

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | COMPONENT |  |  |  | MODULE | System XXX |
|  |  |  |  |  |  |  |
|  | TEST MANAGER |  |  | ALTERNATE |  |  |
|  |  |  |  |  |  |
|  | OBJECTIVE |  | 1. To test the technical recovery procedures outlined in the Disaster |  |
|  |  |  | Recovery Plan updated July 2014. |  |
|  |  |  | 2. To validate that the recovery procedures required to activate the |  |
|  |  |  | system at the Recovery Site are not dependent in any manner upon |  |
|  |  |  | the availability of primary site resources. System, People, |  |
|  |  |  | Workstations, Equipment, Documentation. |  |
|  |  |  | 3. To validate that the system is recovered meeting both the Recovery |  |
|  |  |  | Time and Recovery Point Objectives as stated in the plan. |  |
|  |  |  |  |  |  |
|  | SCENARIO |  | Site loss has occurred at the Primary Site (assume an outage of 3 |  |
|  |  |  | months). |  |  |  |  |
|  |  |  |  |  |
|  | ASSUMPTIONS |  | All technical information documented in the Disaster Recovery Plan, is |  |
|  |  |  | complete and accurate. |  |  |
|  |  |  | There are no backup tapes that can be recalled from off-site. |  |
|  |  |  |  |
|  | TEAMS INVOLVED | Component System Recovery Team. |  |
|  |  |  |  |  |  |  |  |
|  | LOCATION OF TEST TEAMS | DR Data Centre. |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | EQUIPMENT STATUS | Recovery Site hardware available. Primary Site hardware unavailable. |  |
|  |  |  |  |  |  |  |  |
|  | OFFSITE TAPES |  | Not available. |  |  |  |  |
|  |  |  |  |  |
|  | PERSONNEL STATUS | BEST CASE – All staff are available |  |  |
|  |  |  |  |  |  |
|  | TIME/DAY OF DISASTER | Time: 10:00 | Day: Tuesday | Date: 15 July 2014 |  |
|  |  |  |  |  |  |
|  | RECOVERY POINT | Time: 11:30 | Day: Tuesday | Date: 15 July 2014 |  |
|  |  |  |  |  |  |  |  |
|  | PRE-REQUISITES | Current Component Disaster Recovery Plan. |  |
|  |  |  |  |  |  |  |  |
|  | APPLICATIONS/SYSTEMS | Component ID platform. |  |  |
|  | TO RECOVER |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | TEST START: | 10:00 15.07.14 |  | SET UP BY: |  |  |
|  | TEST END: | 11.30 15.07.14 |  | DATE: | 15.07.14 |  |
|  |  |  |  |  |  |  |  |

Planned log of events

TEST EXERCISE: RESTORE COMPONENT ID SYSTEM TO DR SITE & TEST APPLICATION

FUNCTIONALITY

|  |  |  |  |
| --- | --- | --- | --- |
|  | Attendees | DR Data Centre – |  |
|  |  |  |  |  |
|  | Estimated | Estimated |  |  |
|  | Actual Time | Elapsed time | Activity |  |
|  | HH:MM | H:MM |  |  |
|  |  |  |  |  |
|  | Tuesday 15 July | -1:00 | Component Disaster Recovery Team meet (Level 7) |  |
|  |  |  | START DRP TEST (Level 1) |  |
|  | 10:00 | 0:00 | Step 1 – (DR Simulation task) |  |
|  |  |  | Step 2 – Shut down (DR Simulation only) |  |
|  |  |  | Step 3 – Update the DNS Alias entries. |  |
|  |  |  | Step 4 – A02 - Failover System XXX to DR Site - (All steps) |  |
|  |  |  | Step 5 –Step 7 – Conduct Validity Test |  |
|  |  |  | A03 - Validity Test Procedure |  |
|  |  |  | Step 8 – Brief Recovery coordinator of status and request |  |
|  |  |  | approval to commence operations at DR Site |  |
|  |  |  | Step 9 – Release to commence operations at BBB |  |
|  |  |  | Step 10 - Debrief Recovery team on recovery process |  |
|  |  |  | DRP Test Complete |  |
|  |  |  | Test cutoff Point - Absolute |  |
|  |  |  | Commence Failback |  |
|  |  |  | Composite ID back in production at AAA |  |
|  |  |  |  |  |

**Appendix D – Resources**

****

The following table provides a list of other resources which support Disaster Recovery development.

|  |  |  |
| --- | --- | --- |
| Description |  | references |
|  |  |  |
| Related international |  | ISO 22301 – Societal security – Business continuity management |
| standards and guidelines |  | systems - Requirements |
|  |  |  |
|  |  | ISO 27031 – Information technology – Security techniques – Guidelines |
|  |  | for information and communication technology readiness for business |
|  |  | continuity |
|  |  |  |
|  |  | ISO 24762 – Guidelines for information and communication technology |
|  |  | disaster recovery services |
|  |  |  |
|  |  | ISO 31000 – Risk management principles and guidelines |
|  |  |  |
|  |  | ISO 20000.1 – Service management system requirements |
|  |  |  |
|  |  | [Good Practice Guidelines 2013 - Business Continuity Institute](https://govdex.gov.au/confluence/download/attachments/282013071/BCI%20Good%20Practice%20Guidelines%202013%20WEBSITE%20copy%20%283%29.pdf?version=1&modificationDate=1406160773054&api=v2) |
|  |  |  |
| Definition and glossary |  |
|  |  |  |
| Disaster Recovery glossary |  | Disaster Recovery Journal, downloadable glossary list: drj\_glossary.doc |
|  |  | http://www.drj.com/resources/tools/glossary-2.html |
|  |  |  |
| Disaster Recovery planning |  | [Business Continuity and Disaster Recovery Planning Definition and](http://www.cio.com/article/2439506/security0/business-continuity-and-disaster-recovery-planning-definition-and-solutions.html) |
| definition and solutions |  | [Solutions, CIO, Mar 6 2007](http://www.cio.com/article/2439506/security0/business-continuity-and-disaster-recovery-planning-definition-and-solutions.html) |
|  |  |  |
| Agency materials and examples |  |
|  |  |
| Frequently Asked Questions |  | [https://govdex.gov.au/confluence/display/NSWIS/Working+Group+-](https://govdex.gov.au/confluence/display/NSWIS/Working%2BGroup%2B-%2BDisaster%2BRecovery%2Band%2BBusiness%2BContinuity) |
|  |  | [+Disaster+Recovery+and+Business+Continuity](https://govdex.gov.au/confluence/display/NSWIS/Working%2BGroup%2B-%2BDisaster%2BRecovery%2Band%2BBusiness%2BContinuity) |
| Disaster Recovery and |  |
|  |  |
| Business Continuity Working |  | Information security community of practice Govdex space. |
| Group |  | (Membership required for access, please send inquiries to |
|  |  | informationsecurity@finance.nsw.gov.au) |
|  |  |  |

**Appendix E – Glossary**

****

The following glossary provides definitions for terms that are not otherwise explained in the guidelines.

|  |  |
| --- | --- |
| **Term** | **Definition** |
|  |  |
| Alternate site | A site held in readiness for use during/following an invocation of business |
|  | or disaster recovery plans to continue urgent and important activities of |
|  | an organisation. |
|  |  |
| Application recovery | The component of Disaster Recovery that deals specifically with the |
|  | restoration of business system software and data after the processing |
|  | platform has been restored or replaced. |
|  |  |
| Asset | Anything that an organisation signifies as important or valuable. This |
|  | could include technology equipment, real estate, operating equipment, |
|  | intellectual property, reputation, and financial resources. |
|  |  |
| Backup (Data) | A process by which data (electronic or paper-based) and programs are |
|  | copied in some form so as to be available and used if the original data |
|  | from which it originated is lost, destroyed or corrupted. |
|  |  |
| Business continuity | The strategic and tactical capability of the organisation to plan for and |
|  | respond to incidents and business disruptions in order to continue |
|  | business operations at an acceptable predefined level. |
|  |  |
| Business continuity | Ongoing management and governance process supported by top |
| management (BCM) program | management and appropriately resourced to implement and maintain |
|  | business continuity management (Source: ISO 22301:2012) |
|  |  |
| Business Continuity Plan | Documented procedures that guide organizations to respond, recover, |
| (BCP) | resume and restore to a pre-defined level of operation following |
|  | disruption. |
|  | Note: Typically this covers resources, services and activities required to |
|  | ensure the continuity of critical business functions. (Source= ISO |
|  | 22301:2012) |
|  |  |
| Business impact analysis | A process designed to assess the potential quantitative (financial) and |
|  | qualitative (non-financial) impacts that might result if an organisation was |
|  | to experience a business disruption. |
|  |  |
| Business disruption | Any event, whether anticipated (i.e., public service strike) or |
|  | unanticipated (i.e., blackout) which disrupts the normal course of |
|  | business operations at an organization’s location. Similar terms: outage, |
|  | service interruption. |
|  |  |
| Contact List | A list of key people to be notified at the time of disruption or as needed. |
|  |  |
| Critical business functions | The critical operational and/or business support functions that could not |
|  | be interrupted or unavailable for more than a mandated or |
|  | predetermined timeframe without significantly jeopardizing the |
|  | organisation. |
|  |  |
| Data centre recovery | The component of Disaster Recovery which deals with the restoration of |
|  | data centre services and computer processing capabilities at an alternate |
|  | location and the migration back to the production site. |
|  |  |

|  |  |
| --- | --- |
| Disaster | Situation where widespread human, material, economic or |
|  | environmental losses have occurred which exceeded the ability of the |
|  | affected organization, community or society to respond and recover |
|  | using its own resources. |
|  |  |
| Disaster recovery | The process, policies and procedures related to preparing for recovery or |
|  | continuation of technology infrastructure, systems and applications |
|  | which are vital to an organisation after a disaster or outage. *Note:* |
|  | *Disaster Recovery focuses on the information or technology systems that* |
|  | *support business functions, as opposed to Business Continuity which* |
|  | *involves planning for keeping all aspects of a business functioning in the* |
|  | *midst of disruptive events. Disaster recovery is a subset of Business* |
|  | *Continuity.* |
|  |  |
| Disaster recovery plan | The management approved document that defines the resources, |
|  | actions, tasks and data required to manage the technology recovery |
|  | effort. Usually refers to the technology recovery effort. This is a |
|  | component of the Business Continuity Management Program. |
|  |  |
| Disaster Recovery planning | The process of developing and maintaining recovery strategies for |
|  | information technology (IT) systems, applications and data. This includes |
|  | networks, servers, desktops, laptops, wireless devices, data and |
|  | connectivity. |
|  | Note: Priorities for IT recovery should be consistent with the priorities |
|  | for recovery of business functions and processes that were developed |
|  | during the business impact analysis (BIA) process. IT resources required |
|  | to support time-sensitive business functions and processes should also be |
|  | identified. |
|  |  |
| Exercise | A people focused activity designed to execute business continuity plans |
|  | and evaluate the individual and/or organisation performance against |
|  | approved standards or objectives. Exercises can be announced or |
|  | unannounced, and are performed for the purpose of training and |
|  | conditioning team members, and validating the business continuity plan. |
|  | Exercise results identify plan gaps and limitations and are used to |
|  | improve and revise the Business Continuity Plans. Types of exercises |
|  | include: table top exercise, simulation exercise, operational exercise, |
|  | mock disaster, desktop exercise, full rehearsal. |
|  |  |
| Impact | The effect, acceptable or unacceptable, of an event on an organisation. |
|  | The types of business impact are usually described as financial and non- |
|  | financial and are further divided into specific types of impact. |
|  |  |
| Incident | An event which is not part of standard business operations which may |
|  | impact or interrupt services and, in some cases, may lead to disaster. |
|  |  |
| Incident command system | A standardized on-scene emergency management construct specifically |
| (ICS) | designed to provide for the adoption of an integrated organisational |
|  | structure that reflects the complexity and demands of single or multiple |
|  | incidents, without being hindered by jurisdictional boundaries. ICS is the |
|  | combination of facilities, equipment, personnel, procedures, and |
|  | communications operating within a common organisational structure, |
|  | designed to aid in the management of resources during incidents. It is |
|  | used for all kinds of emergencies and is applicable to small as well as |
|  | large and complex incidents. ICS is used by various jurisdictions and |
|  | functional agencies, both public and private, to organize field-level |

|  |  |
| --- | --- |
|  | incident management operations. |
|  |  |
| Incident management | The process by which an organisation responds to and controls an |
|  | incident using emergency response procedures or plans. |
|  |  |
| Incident management plan | A clearly defined and documented plan of action for use at the time of an |
|  | incident, typically covering the key personnel, resources, services and |
|  | actions needed to implement the incident management process. |
|  |  |
| Incident response | The response of an organisation to a disaster or other significant event |
|  | that may significantly impact the organization, its people, or its ability to |
|  | function productively. An incident response may include evacuation of a |
|  | facility, initiating a disaster recovery plan, performing damage |
|  | assessment, and any other measures necessary to bring an organisation |
|  | to a more stable status. |
|  |  |
| Information security | The securing or safeguarding of all information, electronic or otherwise, |
|  | which is owned by an organisation. |
|  |  |
| Loss | Unrecoverable resources that are redirected or removed as a result of a |
|  | Business Continuity event. Such losses may be loss of life, revenue, |
|  | market share, competitive stature, public image, facilities, or operational |
|  | capability. |
|  |  |
| Operational risk | The risk of loss resulting from inadequate or failed procedures and |
|  | controls. This includes loss from events related to technology and |
|  | infrastructure, failure, business interruptions, staff related problems, and |
|  | from external events such as regulatory changes. |
|  |  |
| Outage | The interruption of automated processing systems, infrastructure, |
|  | support services, or essential business operations, which may result, in |
|  | the organizations inability to provide services for some period of time. |
|  |  |
| Recovery | Implementing the prioritized actions required to return the processes and |
|  | support functions to operational stability following an interruption or |
|  | disaster. |
|  |  |
| Recovery Point Objective | The point in time to which data is restored and/or systems are recovered |
| (RPO) | after an outage. |
|  | Note: RPO is often used as the basis for developing backup strategies and |
|  | determining the amount of data that may require recreation after |
|  | systems have been recovered. RPO for applications can be enumerated in |
|  | business time (i.e., “8 business hours” after a Sunday disaster restores to |
|  | close of business Thursday) or elapsed time, but is always measured in |
|  | terms of time before a disaster. RPO for systems typically must be |
|  | established at time of disaster as a specific point in time (e.g., end of |
|  | previous day’s processing) or software version/release. |
|  |  |
| Recovery site | A designated site for the recovery of business unit, technology, or other |
|  | operations, which are critical to the enterprise. |
|  |  |
| Recovery strategy | See business continuity strategy. |
|  |  |
| Recovery Time Objective | The period of time within which systems, applications, or functions must |
| (RTO) | be recovered after an outage. RTO includes the time required for: |
|  | assessment, execution and verification. RTO may be enumerated in |
|  | business time (e.g. one business day) or elapsed time (e.g. 24 elapsed |
|  | hours). *Notes: Assessment includes the activities which occur before or* |

|  |  |
| --- | --- |
|  | *after an initiating event, and lead to confirmation of the execution* |
|  | *priorities, time line and responsibilities, and a decision regarding when to* |
|  | *execute.* |
|  | Execution includes the activities related to accomplishing the pre-planned |
|  | steps required within the phase to deliver a function, system or |
|  | application in a new location to its owner. |
|  | Verification includes steps taken by a function, system or application |
|  | owner to ensure everything is in readiness to proceed to live operations. |
|  |  |
| Response | The reaction to an incident or emergency to assess the damage or impact |
|  | and to ascertain the level of containment and control activity required. In |
|  | addition to addressing matters of life safety and evacuation, response |
|  | also addresses the policies, procedures and actions to be followed in the |
|  | event of an emergency. |
|  |  |
| Restoration | Process of planning for and/or implementing procedures for the repair of |
|  | hardware, relocation of the primary site and its contents, and returning |
|  | to normal operations at the permanent operational location. |
|  |  |
| Resumption | The process of planning for and/or implementing the restarting of |
|  | defined business processes and operations following a disaster. This |
|  | process commonly addresses the most critical business functions within |
|  | BIA specified timeframes. |
|  |  |
| Risk controls | All methods of reducing the frequency and/or severity of losses including |
|  | exposure avoidance, loss prevention, loss reduction, segregation of |
|  | exposure units and non-insurance transfer of risk |
|  |  |
| Scenario | A pre-defined set of Business Continuity events and conditions that |
|  | describe, for planning purposes, an interruption, disruption, or loss |
|  | related to some aspect(s) of an organization’s business operations to |
|  | support conducting a BIA, developing a continuity strategy, and |
|  | developing continuity and exercise plans. |
|  | Note: Scenarios are neither predictions nor forecasts. |
|  |  |
| Service continuity | The process and procedures required to maintain or recover critical |
|  | services such as “remote access” or “end-user support” during a business |
|  | interruption. |
|  |  |
| Service continuity planning | A process used to mitigate, develop, and document procedures that |
|  | enable an organisation to recover critical services after a business |
|  | interruption. |

Service Level Agreement (SLA) A formal agreement between a service provider (whether internal or external) and their client (whether internal or external), which covers the nature, quality, availability, scope and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as the need for the service may vary in a disaster.

|  |  |
| --- | --- |
| System recovery | The procedures for rebuilding a computer system and network to the |
|  | condition where it is ready to accept data and applications, and facilitate |
|  | network communications. |
|  |  |
| Test | A pass/fail evaluation of infrastructure (example-computers, cabling, |
|  | devices, hardware) and\or physical plant infrastructure (example-building |
|  | systems, generators, utilities) to demonstrate the anticipated operation |
|  | of the components and system. Tests are often performed as part of |

|  |  |  |
| --- | --- | --- |
|  |  | normal operations and maintenance. Tests are often included within |
|  |  | exercises. (See Exercise). |
|  |  |  |
|  | Threat | A combination of the risk, the consequence of that risk, and the |
|  |  | likelihood that the negative event will take place. |
|  |  |  |
|  | Vital records | Records essential to the continued functioning or reconstitution of an |
|  |  | organisation during and after an emergency and also those records |
|  |  | essential to protecting the legal and financial rights of that organisation |
|  |  | and of the individuals directly affected by its activities. |
|  |  |  |
|  |  |  |