

# **ABCD Data Centres**

## *Process Guide*

# *IT Service Continuity Management*

---

## TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>4</b>
<b>2.</b>	<b>MISSION .....</b>	<b>4</b>
<b>3.</b>	<b>SCOPE .....</b>	<b>4</b>
<b>4.</b>	<b>GOALS.....</b>	<b>5</b>
<b>5.</b>	<b>KEY PERFORMANCE INDICATORS AND MEASUREMENTS.....</b>	<b>6</b>
<b>6.</b>	<b>GUIDING PRINCIPLES .....</b>	<b>7</b>
6.1.	ROLE OF GUIDING PRINCIPLES .....	7
6.2.	ABCD GUIDING PRINCIPLES.....	7
6.2.1.	Control .....	7
6.2.2.	Value add .....	8
6.2.3.	Base Level of IT Continuity Service .....	8
6.2.4.	IT Continuity Testing.....	8
6.2.5.	Automation .....	9
6.2.6.	Responsibility .....	9
6.2.7.	Proactive Management.....	10
6.2.8.	Support of ABCD IT Continuity.....	10
<b>7.</b>	<b>PROCESS INTERFACES .....</b>	<b>11</b>
7.1.	HIGH LEVEL PROCESS INTERFACES.....	11
7.2.	PROCESS INTERFACES .....	12
<b>8.</b>	<b>HIGH-LEVEL PROCESS FLOW .....</b>	<b>14</b>
<b>9.</b>	<b>DETAILED PROCESS FLOW.....</b>	<b>15</b>
9.1.	ESTABLISH THE PROCESS FOUNDATION: FLOW .....	15
9.2.	ESTABLISH THE PROCESS FOUNDATION: DESCRIPTION .....	16
9.3.	CREATE AND MAINTAIN IT CONTINUITY READINESS: FLOW .....	18
9.4.	CREATE AND MAINTAIN IT CONTINUITY READINESS: DESCRIPTION.....	19
9.5.	PERFORM IT CONTINUITY PLAN TEST: FLOW .....	21
9.6.	PERFORM IT CONTINUITY PLAN TEST: DESCRIPTION.....	22
9.7.	EXECUTE IT CONTINUITY PLAN: FLOW.....	24
9.8.	EXECUTE IT CONTINUITY PLAN: DESCRIPTION.....	25
9.9.	PERFORM TRANSITION FROM CONTINUITY TO OPERATIONAL: FLOW .....	27
9.10.	PERFORM TRANSITION FROM CONTINUITY TO OPERATIONAL: DESCRIPTION ....	28
<b>10.</b>	<b>POLICIES AND STANDARDS .....</b>	<b>30</b>
<b>11.</b>	<b>EXPECTED PROCESS BENEFITS.....</b>	<b>30</b>

---

---

<b>12. ROLES AND RESPONSIBILITIES.....</b>	<b>31</b>
12.1. IT CONTINUITY PROCESS OWNER .....	31
12.2. IT CONTINUITY CO-ORDINATOR.....	32
12.3. IT CONTINUITY TEAM LEADER .....	33
12.4. IT CONTINUITY TEAM MEMBER.....	34
<b>13. APPENDIX A – MANAGE IT CONTINUITY TASKS .....</b>	<b>35</b>
13.1. ESTABLISH THE PROCESS FOUNDATION .....	35
13.2. CREATE AND MAINTAIN IT CONTINUITY READINESS.....	36
13.3. PERFORM IT CONTINUITY PLAN TEST .....	38
13.4. EXECUTE IT CONTINUITY PLAN .....	39
13.5. PERFORM TRANSITION FROM CONTINUITY TO OPERATIONAL .....	40
<b>14. APPENDIX B - DOCUMENT CONTROL.....</b>	<b>41</b>
14.1. SUMMARY OF CHANGES .....	41
14.2. DOCUMENT CHANGE APPROVERS .....	41
14.3. DOCUMENT REVIEW PLANS .....	41
14.4. DOCUMENT DISTRIBUTION.....	41
14.5. SECURITY CLASSIFICATION.....	41

---

---

## 1. INTRODUCTION

Manage IT Continuity is the process of planning, establishing, testing and implementing the strategies, processes and procedures imperative to minimise the impact of service unavailability on customers, according to service level agreements in the event of failure or outage. The intent is to anticipate and minimise the impact of extended system unavailability through the development of predefined, documented and tested continuity procedures that take software, data, applications hardware and facility continuity into account. The actions involved in this process include restoring information technology systems to its normal operating conditions or taking alternate actions to support critical applications.

Developing the process starts by taking the customer's requirements as input to design, build, test and implement a solution that will meet those requirements. Each request will be verified against the existing capabilities of the organisation, allowing current strategies, policies and other controls to be used in generating and evaluating potential solutions. After the required continuity capability is implemented, it should be monitored on a continuous basis to ensure that the detection of any problems or deficiencies with the execution thereof, renders the process to future modifications and enhancements as deemed necessary.

## 2. MISSION

To provide a service to minimise the business impact of an extended system outage, on both ABCD and ABCD's customers, by minimising risks and ensuring adequate resources to provide system availability and data integrity.

## 3. SCOPE

The process begins with:

- Identification of the applications, data and services in the ABCD Data Centres, and the identification of potential catastrophic outages.

The process ends with:

- Readiness for disaster, a working contingency plan, and a scenario for return to normal operations.

The process includes:

- The definition of system recovery timeframes
  - Planning and preparation for any anticipated major disasters – for example, total loss of processing capability and facilities which makes business-critical processing unavailable for an extended period
  - Risk Management, to identify and eliminate or contain risks
  - Restoration from major failures of facilities, environment, and technology
  - Method for returning to normal operations
-

---

The following Data Centre technology environments are to be addressed by the Manage IT Continuity process and will each have its' own IT Continuity Plan:

- IBM mainframes
- UNISYS mainframes
  - UNISYS IX
  - UNISYS NX
- UNIX servers
- Printers – laser and impact

The process excludes the following area of ABCD:

- Non-IT components of business continuity
- Routine operational recoveries
- Help Desk
- Distributed Support Services
- Networks

## 4. GOALS

The goals of the Manage IT Continuity process are:

- Enable continued delivery of IT services deemed essential to ABCD and ABCD's customers in the event of extended system unavailability.
  - Maintain consistency with the ABCD business plan.
  - Maintain proven readiness for information technology recovery.
  - Establish the recovery infrastructure to cater for the largest production platforms in ABCD.
  - Reduce recovery times.
  - Practice disaster avoidance by minimising risks.
  - Ensure that backup requirements defined in ABCD-customer Service Level Agreements are met.
  - Establish a base level of IT Continuity, which will be the default for all ABCD customers.
  - Implement remote mirroring wherever possible.
  - Effect smooth transition to post-disaster operational status when such environment and infrastructure is ready.
-

---

## 5. KEY PERFORMANCE INDICATORS AND MEASUREMENTS

A combination of the following will provide the basis for assessing the success of the Manage IT Continuity process, and to help identify areas of potential process improvement:

- The degree to which customer continuity requirements are documented in Service Level Agreements
  - Time to recover, as per test evaluation reports
  - Time to recover from an actual outage
  - The value and role of continuity plans and procedures in outages experienced
  - Bi-annual Continuity plan maintenance
  - Bi-annual tests per platform
  - Successful results from internal and external audits
  - Integration of IT Continuity into the day-to-day activities of the organisation:
    - Capacity planning
    - Staff job contracts
    - Daily production activities
-

---

## 6. GUIDING PRINCIPLES

### 6.1. *Role of Guiding Principles*

A set of principles can be defined in advance that will help describe how IT continuity will be provided. Principles allow a general statement to be made about how things should operate, independent of the changing technology platforms but accommodating the fast changing business environment in which service delivery operates. They help provide a framework within which more detailed strategies can be developed.

Every principle can be justified by an underlying rationale that explains why the principle should be adopted to guide strategy formulation at ABCD. Every principle spawns a related set of implications. Implications are the ramifications and side effects of following the principle. In effect, the implications are a discussion of just what the principle means.

### 6.2. *ABCD Guiding Principles*

#### 6.2.1. Control

##### **Principle**

- Disaster Recovery Planning process will be centrally managed.

##### **Rationale**

- Supports the Data Centre requirements
- Flexibility
- Control close to the customer
- Consistent adherence provides enterprise wide benefit
- Allows central control of all resources
- Provides total service orientation
- Develops and takes advantage of core competencies

##### **Implication**

- Need to manage performance and capacity that have a broad effect over the business environment
  - Consistent tracking of data for all appropriate components
  - Common rules
  - Information needs to be available across control boundaries
  - Well defined interfaces among processes
-

---

## 6.2.2. Value add

### **Principle**

- IT continuity activities and costs must prove clear value add to ABCD customers.

### **Rationale**

- Support ABCD business objectives
- Maintain focus on budgetary constraints
- Enhance ABCD image among customers

### **Implication**

- Must be a mechanism to provide guidance and direction on proposed activities
- Information needs to be available across control boundaries
- Well defined interfaces among processes

## 6.2.3. Base Level of IT Continuity Service

### **Principle**

- A base level of IT continuity will be included in the recoverable services offered to ABCD customers.

### **Rationale**

- Funds will be generated to finance continuity expenses

### **Implication**

- A base level of IT continuity must be established
- The infrastructure and capability to deliver this base level must be implemented
- Once this minimum level of service is contracted with customers ABCD will be legally liable for non-compliance

## 6.2.4. IT Continuity Testing

### **Principle**

- There will be an annual test of the recovery process

### **Rationale**

- Data and systems will need to be quickly recovered in the event of extended system unavailability

### **Implication**

- Management commitment to annual test
  - Expense of maintaining and using the backup and recovery infrastructure
-

---

### 6.2.5. Automation

#### **Principle**

- Disaster Recovery Planning will be automated with commercially available products wherever possible

#### **Rationale**

- Speed
- Cost reduction
- Consistency
- Robustness
- Reliability
- Accuracy
- Efficiency
- Reduce dependency on specific staff members

#### **Implications**

- Define gaps in automation
- Determine how to justify and eliminate the gaps
- Define policies and procedures to enable automation
- Tool investment
- Increased skill requirements

### 6.2.6. Responsibility

#### **Principle**

- The IT Continuity process will have a single identified process owner within Data Centres.

#### **Rationale**

- Keep the process discrete and bounded
- Avoids responsibility conflict or uncertainty
- Promotes responsibility, continuous improvement

#### **Implications**

- Ensure the process owner is at the right level in the organisation
  - The process owner will help define the process ownership role
  - Appropriate sponsorship is key
-

---

## **6.2.7. Proactive Management**

### **Principle**

- IT Continuity will be proactive rather than reactive whenever possible

### **Rationale**

- Will promote highest possible service levels
- Will allow ABCD reaction before customers are involved in many cases
- Will enable ABCD to advise non-contracted customers on Continuity issues

### **Implications**

- Availability of tools
- Requirement for a “service” orientation
- Commitment to an investment in infrastructure – prior to contract agreement with customers

## **6.2.8. Support of ABCD IT Continuity**

### **Principle**

- The ABCD Data Centre IT Continuity process must support the holistic ABCD IT Continuity process and objectives.

### **Rationale**

- In accordance with ABCD objectives and planning

### **Implications**

- Process to establish ABCD IT Continuity must be initiated.
  - Must be reviewed by relevant ABCD forum/mechanism.
-

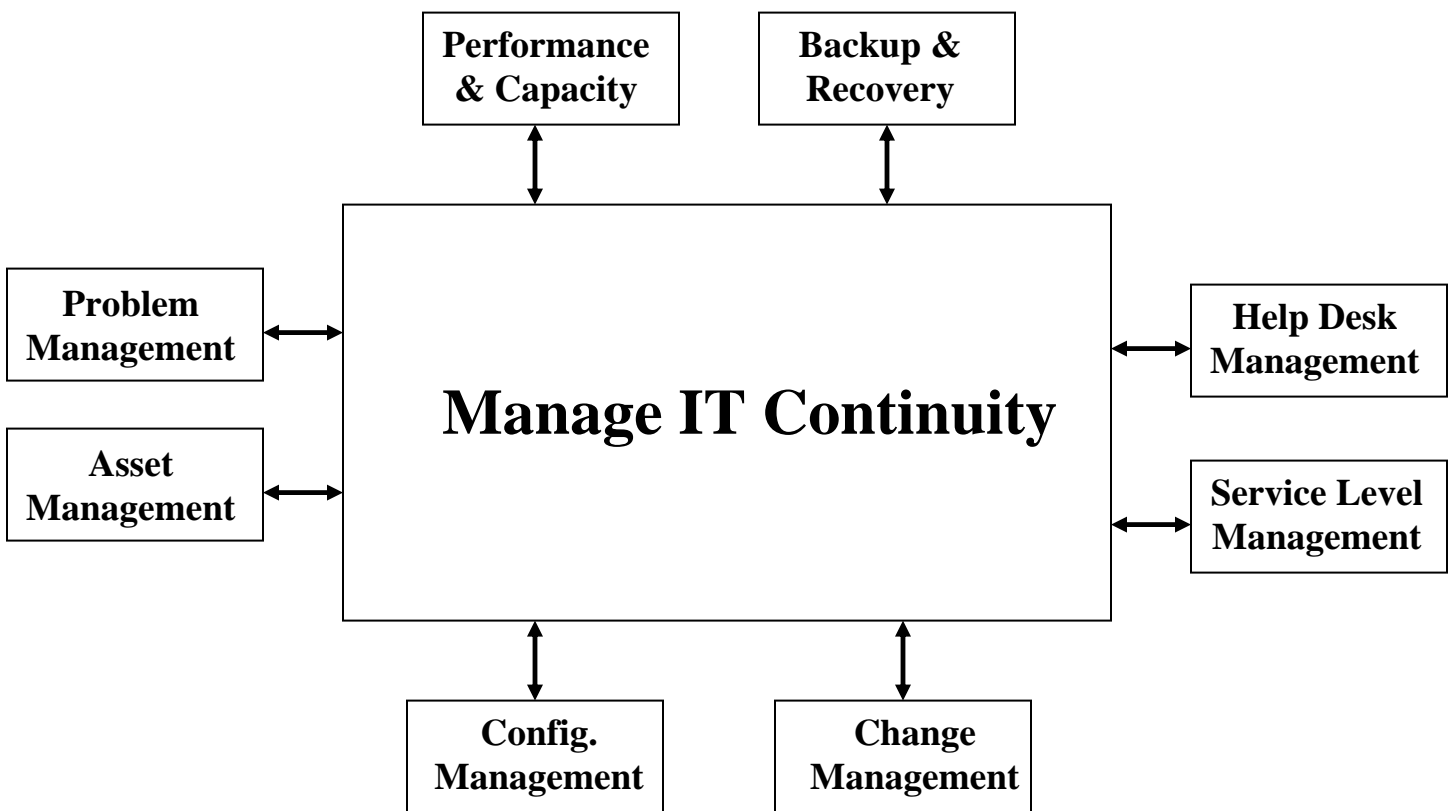
---

## 7. PROCESS INTERFACES

With the definition of any process, the interaction of that process with other processes in the organisation is of critical importance. This is due to the impact on the effectiveness and maintenance of the processes. The high level interfaces are graphically depicted below, while the detailed description of the interfaces is provided below.

### 7.1. High Level Process Interfaces

The various links between the Manage IT Continuity process and the other processes it interfaces with are depicted at a high level as follows:



## 7.2. Process Interfaces

The following table depicts the interfaces between IT Continuity and the other key Systems Management processes. Note that the “Outputs from IT Continuity” column indicates the outputs from IT Continuity to another process, and not general IT Continuity outputs such as plans or procedures.

<b>Interaction of Change Management with IT Continuity</b>		
<b>Potential Triggers</b>	<b>Inputs to IT Continuity</b>	<b>Outputs from IT Continuity</b>
<ul style="list-style-type: none"> <li>➤ Request for a new IT Continuity service</li> <li>➤ Change to an existing IT Continuity service</li> <li>➤ Changes to the production environment</li> </ul>	IT Continuity requirements.	Accepted/Rejected Change request.
<ul style="list-style-type: none"> <li>➤ Changes to the recovery environment</li> </ul>	New environment description	Impact on existing services.

<b>Interaction of Problem Management with IT Continuity</b>		
<b>Potential Triggers</b>	<b>Inputs to IT Continuity</b>	<b>Outputs from IT Continuity</b>
<ul style="list-style-type: none"> <li>➤ Service unavailability</li> <li>➤ Escalation process for rolling outage</li> </ul>	Damage assessment process will be initiated via a Problem Record.	Successful service recovery identified in the Problem Record.

<b>Interaction of Asset &amp; Inventory Management with IT Continuity</b>		
<b>Potential Triggers</b>	<b>Inputs to IT Continuity</b>	<b>Outputs from IT Continuity</b>
<ul style="list-style-type: none"> <li>➤ Production environment details</li> <li>➤ Recovery environment details</li> </ul>	Information pertaining to individual assets.	

<b>Interaction of Configuration Management with IT Continuity</b>		
<b>Potential Triggers</b>	<b>Inputs to IT Continuity</b>	<b>Outputs from IT Continuity</b>
<ul style="list-style-type: none"> <li>➤ Production environment details</li> <li>➤ Recovery environment details</li> </ul>	Information pertaining to the relationship between assets will be supplied.	Changes to recovery site infrastructure.

---

<b>Interaction of Performance and Capacity Management with IT Continuity</b>		
<b>Potential Triggers</b>	<b>Inputs to IT Continuity</b>	<b>Outputs from IT Continuity</b>
<ul style="list-style-type: none"> <li>➤ Production environment details</li> <li>➤ Recovery environment details</li> </ul>	Information regarding the performance and capacity.	Changes to recovery site infrastructure.
		Capacity requirements for the implementation of customer requests will be supplied to the Performance and Capacity Management process.

<b>Interaction of Service Level Management with IT Continuity</b>		
<b>Potential Triggers</b>	<b>Inputs to IT Continuity</b>	<b>Outputs from IT Continuity</b>
<ul style="list-style-type: none"> <li>➤ Request for a new IT Continuity service</li> <li>➤ Change to an existing IT Continuity service</li> </ul>	Updates to SLA's will initiate the Create and Maintain IT Continuity Readiness sub-process.	Implemented service or rejected service request.

<b>Interaction of Backup &amp; Recovery Management with IT Continuity</b>		
<b>Potential Triggers</b>	<b>Inputs to IT Continuity</b>	<b>Outputs from IT Continuity</b>
<ul style="list-style-type: none"> <li>➤ Information on the current Backup and Recovery process</li> </ul>	Current recovery capability will influence the Create and Maintain IT Continuity Readiness sub-process.	Request for modification to the Backup and Recovery process.

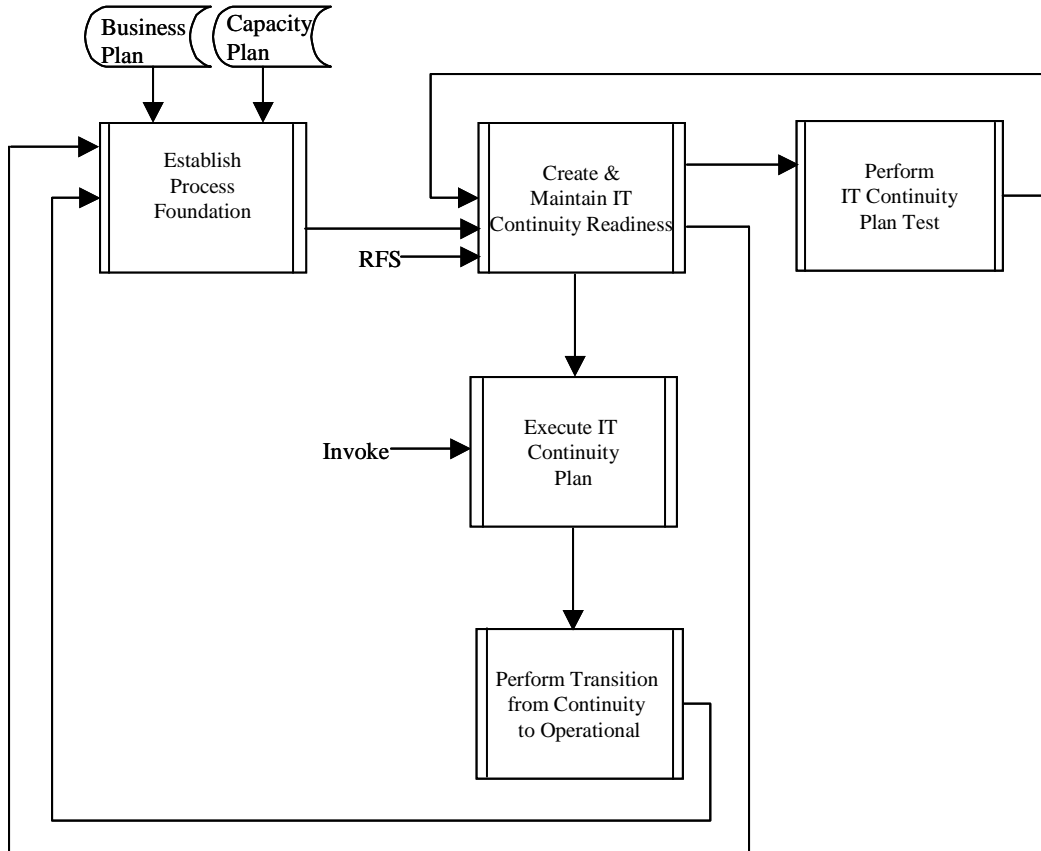
---

---

## 8. HIGH-LEVEL PROCESS FLOW

This section describes the high-level process flow of the Manage IT Continuity process. This is an overview of the sub-processes that make up the Manage IT Continuity process. Each sub-process is defined in terms of the inputs to the sub-process, the controls to which the sub-process is subject, the activities that make up the sub-process, and finally the output produced by the sub-process.

Below is a high-level overview of the Manage IT Continuity Process flow.



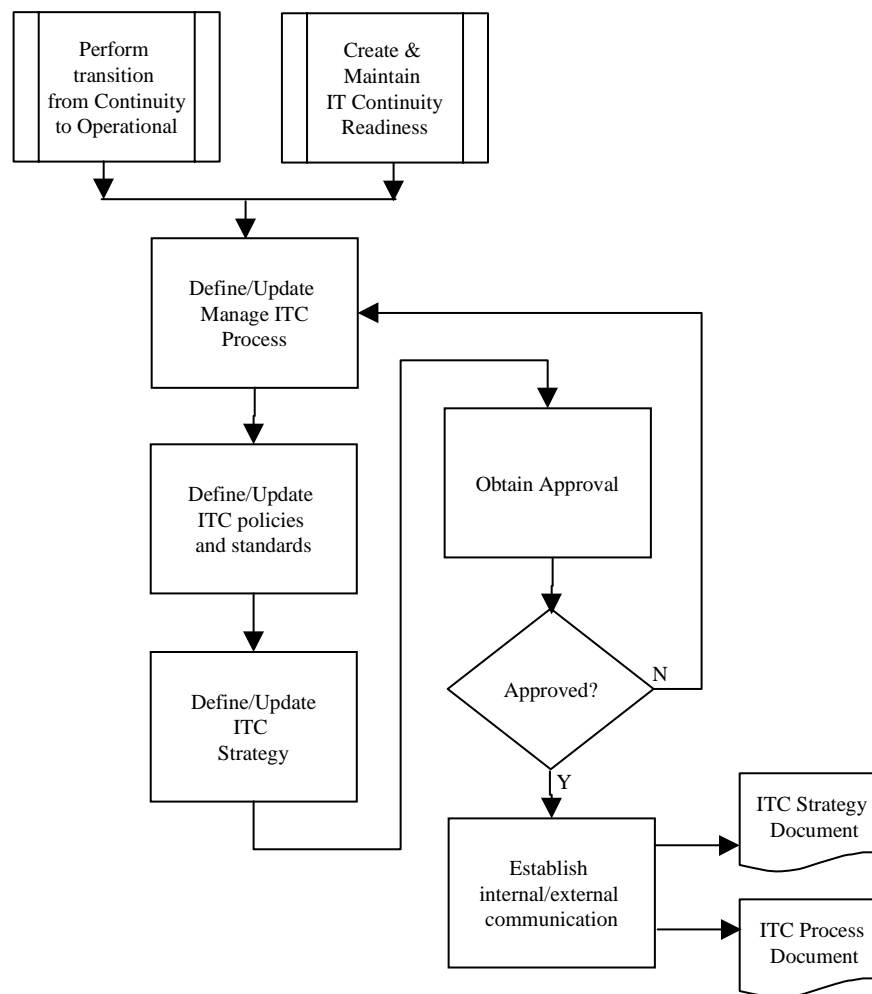
---

## 9. DETAILED PROCESS FLOW

The detailed description of the sub processes used within the Manage IT Continuity process is described in this section of the document. A detailed explanation of each of the sub processes is contained within in the following pages and is meant to provide an understanding of the general functional flow of the generic process.

Each of the sub-processes defined in the Manage IT Continuity process high level flow under the previous heading will be detailed in this section.

### 9.1. *Establish the Process Foundation: Flow*



## 9.2. **Establish the Process Foundation: Description**

**Description** This sub-process defines and updates how Manage IT Continuity process is to function, how the overall health of the process is to be monitored and defines the roles and responsibilities within the service delivery organisation for the elements of the process.

The sub-process is responsible for the enforcement of corporate policies, and the identification of additional policies support the process.

**Controls** ABCD Contingency Policy  
 ABCD Security Policy  
 Customer Service Level Agreements  
 Data Centre Business Plan  
 Data Centre Capacity Plan

**Goal** The goal of this sub-process is to:

- To establish a management framework that will govern the implementation and running of the process.
- To update the process as and when required based on the results of the measurements identified for each sub-process.
- Fully document the IT Continuity Strategy and all identified supporting policy documents.
- Ensure the IT Continuity Strategy & Policies are aligned with ABCD and customer business requirements.

**Inputs** The “Perform Transition from Continuity to Operational” sub-process  
 Customer requirements  
 The “Create and Maintain IT Continuity Readiness” sub-process

Activities	Who
Define/Update IT Continuity process. This activity is responsible for the definition of the ITC process and updating the process based on evaluation of process efficiency and effectiveness as defined for each sub-process.	ITC Process Owner
Define/Update IT Continuity policies and standards This activity is responsible for defining and updating the IT Continuity and related policies, and ensuring that these policies are adhered to.	ITC Process Owner
Define/Update IT Continuity Strategy This activity is responsible for ensuring that there is a formal strategy in place for each component of the Data Centre infrastructure, and it is well communicated.	ITC Process Owner
Obtain approval This activity relates to obtaining approval for the ITC Process document, Strategy and/or policies.	ITC Process Owner
Establish internal/external communication This activity is responsible for ensuring the IT Continuity Policies and Process are communicated and marketed to the customers and IT staff.	ITC Process Owner

---

**Outputs**

Updated IT Continuity Process  
Documented IT Continuity policies  
Updated IT Continuity Strategy

**Measurements**

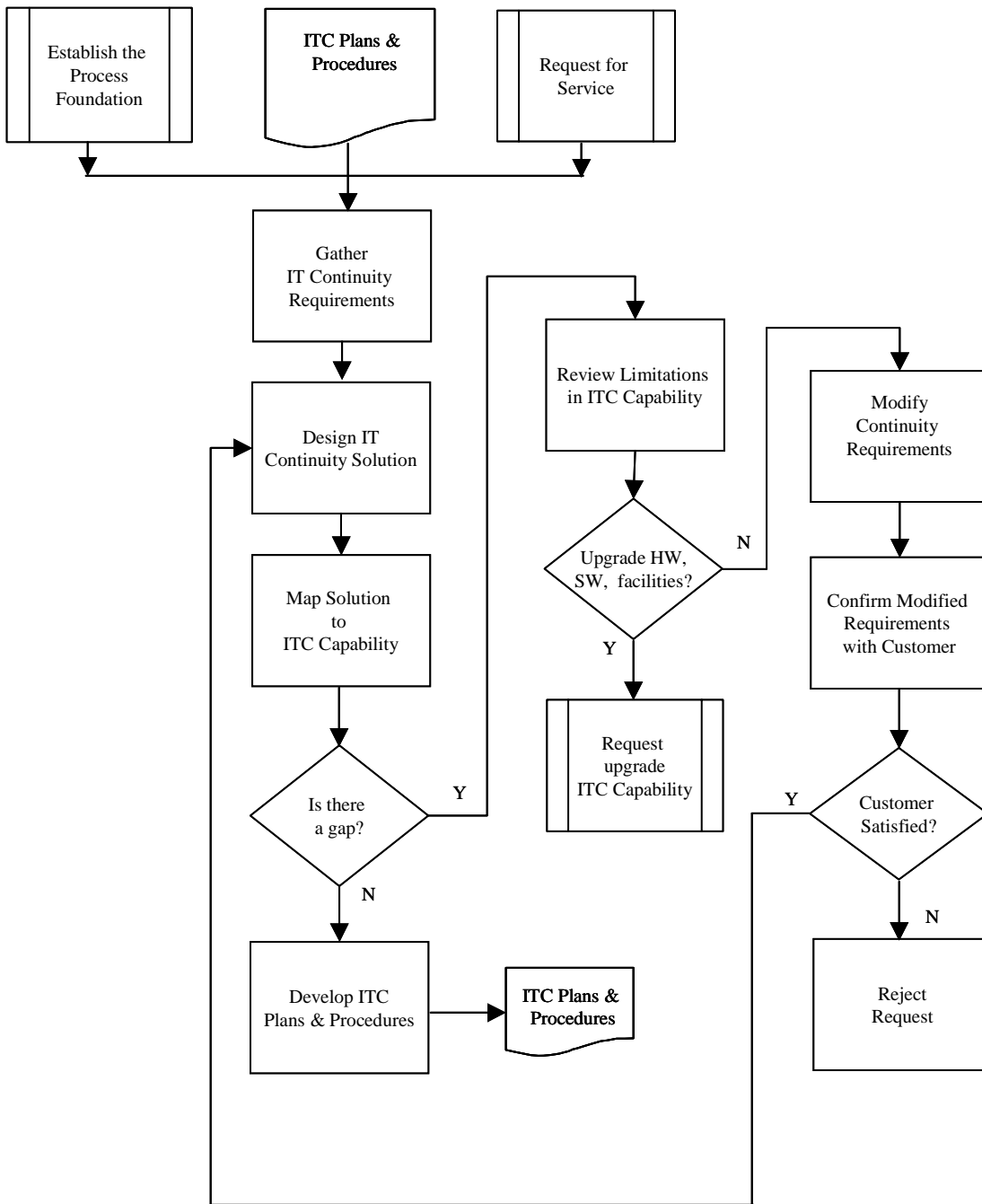
Process Effectiveness  
Turn around time for recovery requests  
Established focal point for IT Continuity investment and benefits  
Level of integration with other processes  
IT Continuity awareness within ABCD Data Centres and the customer base

Process Efficiency  
Signed-off documents within 2 weeks of publication

IT Continuity Process Audits  
Review IT Continuity plans/procedures to ensure compliance of standards

---

### 9.3. Create and Maintain IT Continuity Readiness: Flow



## 9.4. Create and Maintain IT Continuity Readiness: Description

<b>Description</b>	<p>This sub-process is responsible for creating and maintaining the IT Continuity infrastructure, plan and procedures.</p> <p>The sub-process is responsible for the implementation of policies in support of the process, as identified by the ITC Process Owner.</p>
<b>Controls</b>	<p>Capacity Planning          Customer Service Level Agreements          Data Centre IT Continuity Strategy          Audit requirements including Risk Management          Change Management          Configuration Management          Asset Management</p>
<b>Goal</b>	<p>The goal of this sub-process is to:</p> <ul style="list-style-type: none"> <li>➤ To develop and maintain an IT Continuity Plan and procedures for each platform in support of customer Service Level Agreements.</li> <li>➤ To update ABCD strategies, policies and standards while implementing continuity solutions, as necessitated by new Requests for Service.</li> <li>➤ To incorporate IT Continuity Planning into the daily fabric of Data Centre operations.</li> <li>➤ Ensure compliance with all required policies and standards.</li> </ul>
<b>Inputs</b>	<p>Request for Service          The “Establish the Process Foundation” sub-process          Perform “IT Continuity Plan Test” sub-process</p>

<b>Activities</b>	<b>Who</b>
Gather IT Continuity requirements This activity formalises customer requirements from Requests For Service.	ITC Manager
Design IT Continuity solution This involves translating the requirement into a holistic continuity solution, including the technology, process and organisation dimensions.	ITC Manager / ITC Process Owner
Map solution to ITC capability This activity compares the current IT Continuity capability and controls to the solution requirements. This includes interfacing with the Change Management process.	ITC Manager
Review limitations in ITC capability This activity examines all internal and external alternatives to determine the optimal solution to meet the requirements.	ITC Manager
Request upgrade IT Continuity capability This is the process of requesting additional resources to implement a solution to meet the customer requirements.	ITC Manager
Modify Continuity requirements If the feasibility of upgrading the IT environment is turned down then the original requirements are reviewed and modified to cater for the existing	ITC Manager

---

IT environment.	ITC Manager
Confirm modified requirements with customer During this activity the suggested changes to the request for service are discussed with the customer to determine if the altered solution criteria are acceptable.	ITC Manager
Reject request This activity is responsible for handling the rejection of the request for service by either the customer or ABCD.	ITC Manager
Develop ITC plans and procedures This activity develops the plans and procedures required to test, maintain and execute the continuity solution implemented.	ITC Manager

**Outputs**

IT Continuity Plans and procedures  
Feedback to the “Create and Maintain IT Continuity Readiness” sub-process (regarding IT Continuity-related controls, such as Strategy, Policy etc.)

**Measurements**

Process Effectiveness  
Acceptance of proposed solution by customer  
Percentage of production environment protected by either the default level of IT Continuity or the SLA-stipulated level of IT Continuity  
Established focal point for IT Continuity investment and benefits  
Level of solution integration into daily production environment  
Maintenance of IT Continuity documentation  
Staff awareness and understanding of the IT Continuity documentation

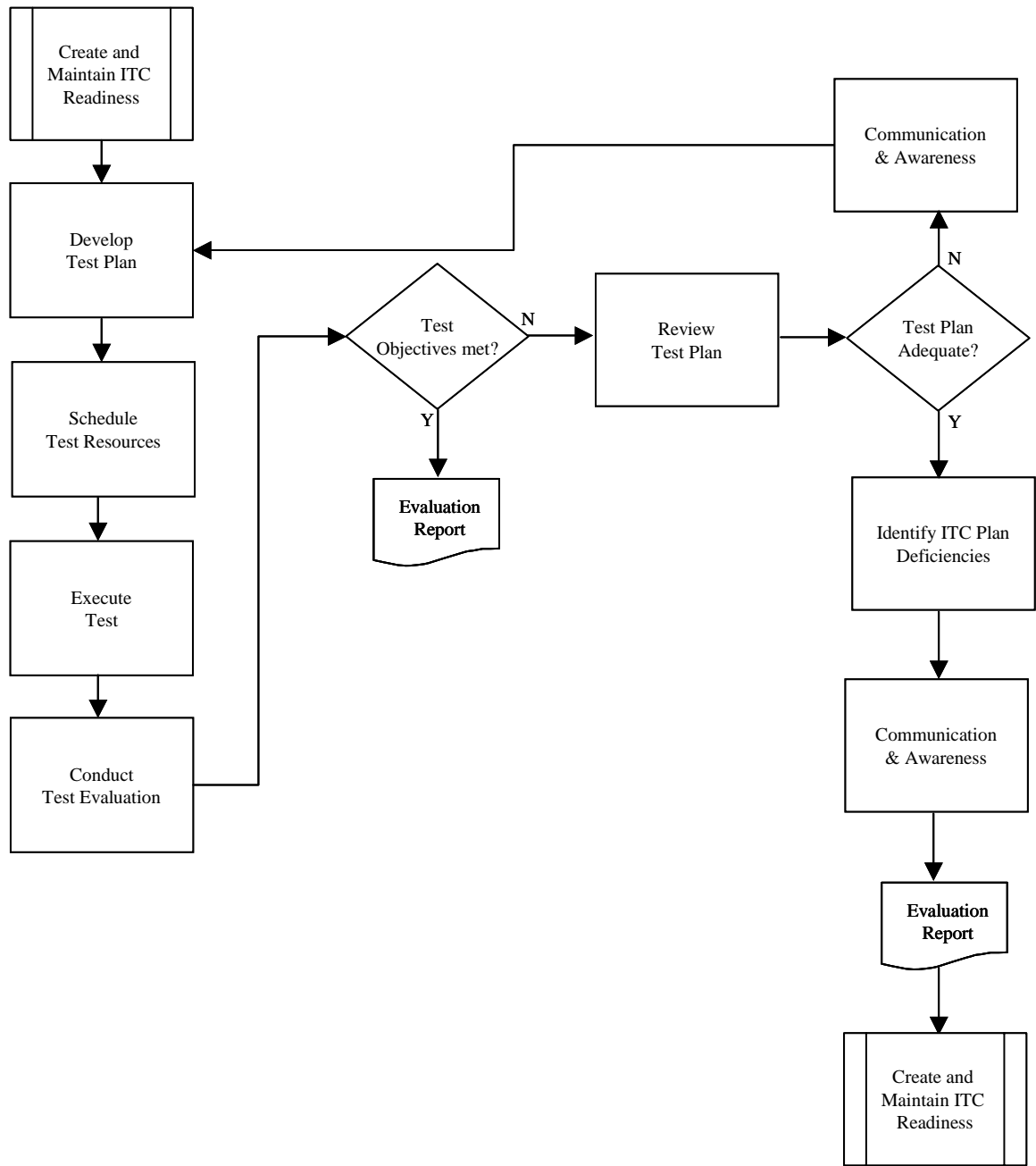
Process Efficiency  
Turn around time for recovery requests  
Turn around time for solution implementation  
IT Continuity Plan and procedures signed-off by ABCD within 2 weeks of publication

IT Continuity Process Audits  
Customer review of IT Continuity capability  
Internal audit of IT Continuity capability  
External audit of IT Continuity capability

---

---

**9.5. Perform IT Continuity Plan Test: Flow**



---

## 9.6. Perform IT Continuity Plan Test: Description

<b>Description</b>	This sub-process is responsible for testing the IT Continuity process defined in the previous sub-process (Create & Maintain IT Continuity Readiness) to ensure the validity of those plans and procedures, in accordance with the IT Continuity Strategy.
<b>Goals</b>	Adopt and follow a structured approach for IT Continuity testing Define test objectives and parameters based on customer requirements Utilise the test process as a marketing opportunity Verify Data Centre IT Continuity capability
<b>Controls</b>	Testing Policies Customer Service Level Agreements IT Continuity plans and procedures
<b>Inputs</b>	Create and Maintain IT Continuity Readiness (test requirements)

Activities	Who
Develop test plan This activity defines test objectives and guidelines.	ITC Manager
Schedule test resources This activity ensures the availability of the continuity infrastructure and resources for each test.	ITC Manager
Execute test During this activity the IT Continuity plans and procedures are tested, as defined in the test plan.	ITC Manager
Conduct test evaluation This activity develops a report explaining test performance and results against the defined test plan.	ITC Manager
Communication and awareness This activity involves creating awareness of the test and the result to the customer involved, and all other relevant stakeholders.	ITC Manager
Update and awareness This activity involves creating awareness of the test and the result to the customer involved, and all other relevant stakeholders.	ITC Manager

<b>Outputs</b>	Test Evaluation Report Feedback to the “Create and Maintain IT Continuity Readiness” sub-process (in the event of test failure as a result of inadequate plans and procedures)
<b>Measurements</b>	Process Effectiveness All primary test objectives met Extent to which secondary test objectives were met Repeated testing in the event of unsatisfactory performance Increased staff understanding of the IT Continuity documentation for execution in the event of an extended outage

---

---

Process Efficiency

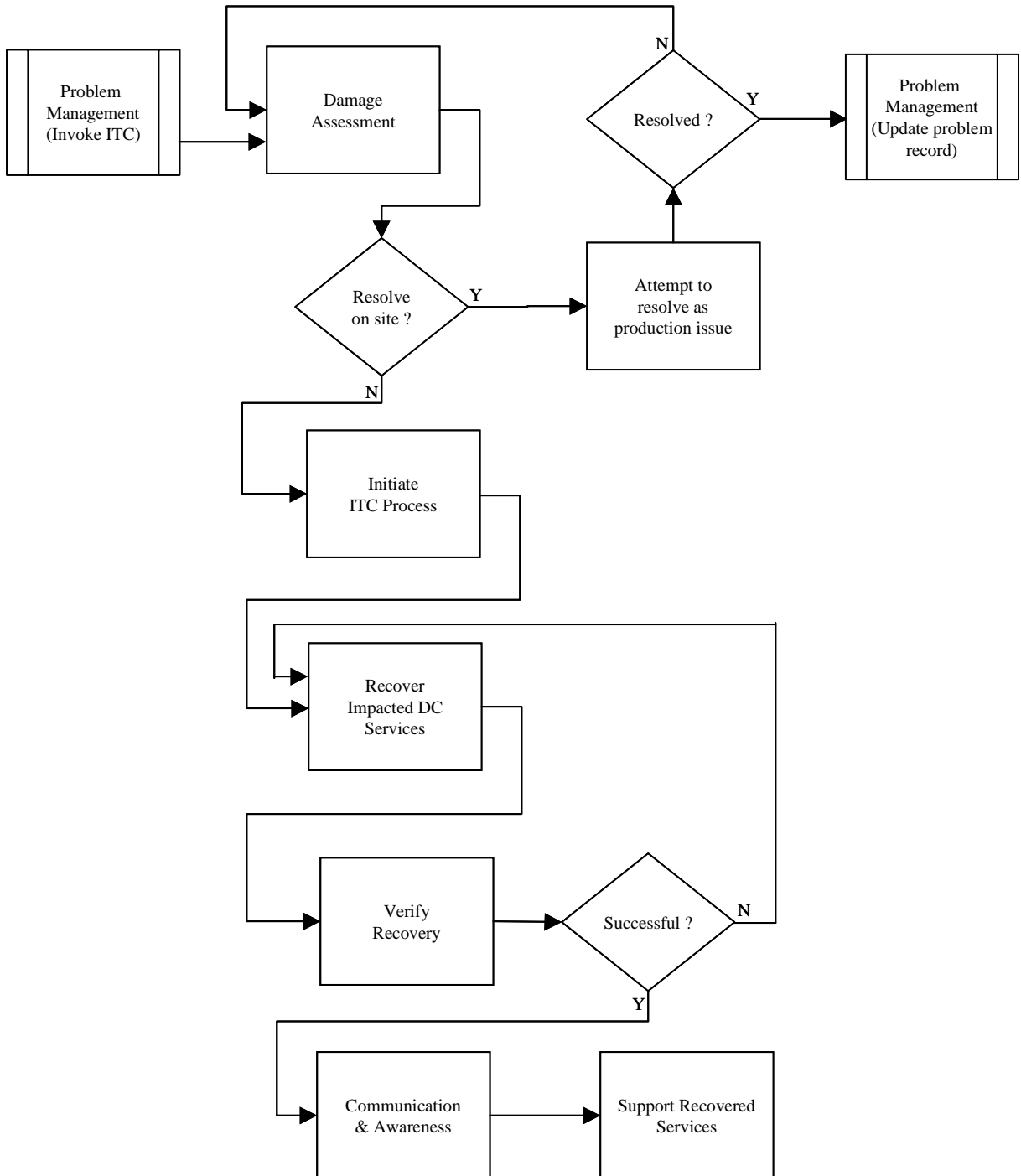
- Established test schedule for the year is met
- Availability and accuracy of process and procedure documentation
- Feedback to the “Create and Maintain IT Continuity” sub-process within a week after testing (if required)
- Continual improvement in test performance (e.g. reduced recovery time etc.)

IT Continuity Test Audit

- Customer review of IT Continuity test process
  - Customer participation in verification testing
-

---

### 9.7. Execute IT Continuity Plan: Flow



## 9.8. *Execute IT Continuity Plan: Description*

<b>Description</b>	This sub-process is responsible for execution of the IT Continuity Plan in the event of an extended system outage, to ensure that normal operations can be resumed with minimal impact to ABCD and it's customers.
<b>Controls</b>	ABCD Corporate Marketing and Communication Client Services IT Continuity plans and procedures Customer priorities (for recovery sequence) if all customers cannot be recovered simultaneously due to infrastructure constraints) Service Level Agreements, if inclusive of disaster recovery
<b>Goal</b>	The goal of this sub-process is to: <ul style="list-style-type: none"> <li>➤ Minimise the impact of an extended outage on ABCD and it's customers</li> <li>➤ To provide system availability within predefined limits</li> <li>➤ To reduce data loss to predefined limits</li> <li>➤ Ensure compliance with the relevant ABCD policies and standards</li> </ul>
<b>Inputs</b>	Problem Management To provide the details of the incident, and accept the results of the IT Continuity process to update the problem record with the status of the incident.

<b>Activities</b>	<b>Who</b>
Damage assessment This activity assesses the problem to determine if the IT Continuity process should be invoked to deal with the situation.	ITC Manager / ITC Process Owner
Attempt to resolve as a production issue This activity addresses the problem as a production issue, and uses the standard problem resolution process.	ITC Manager
Initiate IT Continuity process This activity authorises the use of continuity facilities and initiates the process.	DC Executive
Recover impacted Data Centre services This activity involves the execution of the instructions contained in the IT Continuity plans and procedures.	ITC Manager
Verify recovery During this activity the status of recovered services is verified before allowing all users access.	ITC Manager / Customer
Communication and awareness This activity alerts the ABCD staff and clients that recovery was successful, and system usage may resume.	ITC Manager / ITC Process Owner / Marketing / Client Services
Support recovered services This activity supports and maintains the recovered services at the recovery location.	ITC Team Leader

---

**Output**

Service resumption  
Problem Management  
Problem Management update of the problem record created in response to the emergency situation.

**Measurements**

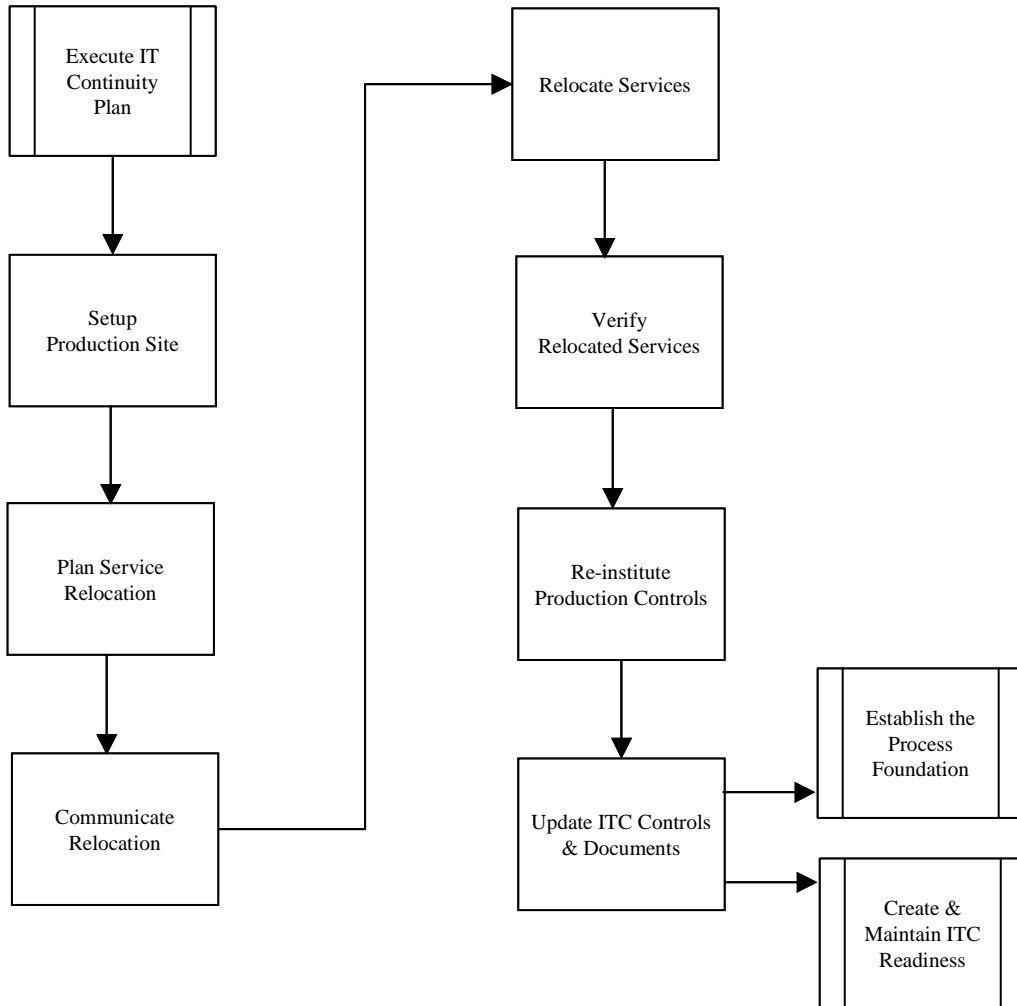
Process Effectiveness  
Successful recovery of impacted services  
Effective internal and external communication throughout

Process Efficiency  
Recovery time as expected (test results)  
Data loss within defined parameters

---

---

**9.9. Perform Transition from Continuity to Operational: Flow**



## 9.10. Perform Transition from Continuity to Operational: Description

<b>Description</b>	This sub-process is responsible for the return to normal operation. This involves preparing a new primary and backup site configuration and getting them up and running in those capacities.
<b>Controls</b>	Data Centre Executive ABCD Corporate Marketing and Communication
<b>Goal</b>	The goal of this sub-process is: <ul style="list-style-type: none"> <li>➤ The efficient relocation of services to the target production environment (ie. from continuity mode to operational mode)</li> <li>➤ Ensure compliance with the relevant ABCD policies and standards</li> </ul>
<b>Inputs</b>	The “Execute IT Continuity Plan” sub-process Capacity Planning Client Services

Activities	Who
Setup production site This activity involves preparing the production site and installing and configuring the required equipment.	ITC Manager / Capacity Planning
Plan service relocation Once the site has been setup, this activity plans and schedules the move from the continuity site back to the production site.	ITC Manager / ITC Team Leader
Communicate relocation The relocation is communicated with all IT staff and affected users during this activity.	ITC Manager / ABCD Corporate Communications
Relocate services This activity actually moves the recovered services from the continuity site to the production site, in accordance with the Service Relocation Plan.	ITC Manager
Verify relocated services Once the services have been relocated, this activity verifies that these services are fully recovered and available.	ITC Manager / Customer
Re-instate standard production controls As soon as the relocated services are made available to the users, this activity re-institutes standard production controls, such as user support, off-site backups, security regulations etc.	ITC Manager
Update ITC controls and documents This activity provides feedback to update the IT Continuity Strategy, Plans and Procedures, based on the role and accuracy of these plans during the exercise. Changes may also be required due to changes to the newly restored production environment.	ITC Manager / IT Continuity Team Leader

---

**Output**

Relocated services (transparent to customer)  
Feedback to the “Establish the Process Foundation” and “Create and Maintain IT Continuity” sub-processes to make the relevant modifications.

**Measurements**

Process Effectiveness  
    Successful service relocation  
    Effective internal and external communication throughout

Process Efficiency  
    Relocation time as scheduled  
    No data loss and/or user downtime

---

---

## 10. POLICIES AND STANDARDS

Policies and standards must be in place to allow ABCD to implement IT Continuity as efficiently and effectively as possible. By adhering to the following policies and standards, ABCD Data Centres will enjoy a higher probability of accomplishing the IT Continuity process goals and objectives previously stated, and establish synergy across functional areas.

Policies are management directives, which significantly influence the way processes and procedures are executed. Standards are rules and conventions that help implement policies and enforce required conventions.

The following is a list of potential policies and standards that should be defined and adhered to facilitate the definition and implementation of the Manage IT Continuity process. Note that the identification of further policies and standards, as well as the revision of existing policies and standards is an ongoing activity.

- Backup and Recovery
- Security
- Media Management
- Maintenance
- Testing
- Risk Management
- Audit and Verification
- Naming Convention

## 11. EXPECTED PROCESS BENEFITS

There are several benefits that ABCD Data Centres intends to achieve through the definition and implementation of the Manage IT Continuity process. These are listed below:

- Reduce business cost (avoid lost revenue, penalties etc.)
  - Maintain image and customer confidence
  - Minimise the impact and duration of extended system unavailability in the event of a catastrophic outage
  - Assign clearly defined roles and responsibilities to the accountable individuals
  - The process document will become the basis for customer negotiations regarding IT Continuity
  - Provide a framework for common understanding of IT Continuity with Data Centres
  - Facilitate communication across functional areas of ABCD
  - Provide a communication vehicle for relevant client discussions
-

---

## 12. ROLES AND RESPONSIBILITIES

### 12.1. *IT Continuity Process Owner*

The **IT Continuity Process Owner** is the individual who oversees the implementation of the IT Continuity process across all areas of ABCD Data Centres. This role assumes responsibility for monitoring and control of the process, and effectively acts as champion and focal point for the organisation.

- Manages the overall process and maintains its quality and effectiveness
- Develops and maintains the Manage IT Continuity Process document
- Ensures the development of IT Continuity Plans and procedures for each area
- Gives direction regarding business requirements/guidelines for disaster recovery
- If appropriate, establishes vendor relationships for disaster recovery operations
- Monitors and measures the quality and effectiveness of the process
- Ensures process education is available and up-to-date
- Continually identifies and initiates activities for improving and updating the process
- Markets the IT Continuity process to all areas of ABCD
- Gathers requirements for improving the process
- Represents the IT Continuity process at all Management meetings
- Implements and maintains a Risk Management Programme for Data Centres
- Approves or rejects process deviation requests
- Ensures the definition of an IT Continuity Strategy for each environment
- Ensures implementation of corporate policies
- Identifies Data Centre policies and procedures required to support the process
- Facilitates, resolves or escalates cross-functional issues
- Oversees the test process, schedule, execution and reports on test success

This role has been assigned to:

- Senior Production Planner, responsible for IT Continuity – xxx
-

---

## 12.2. *IT Continuity Co-ordinator*

The **IT Continuity Manager** must ensure the implementation of the IT Continuity process within that manager's area of responsibility. This role assumes responsibility for implementing, documenting, testing and maintaining recovery solutions for the existing infrastructure, and in response to new requests for service. The responsibility includes a management role in the execution of the adopted recovery solutions as required.

- Implements customer disaster recovery requirements
- Acts as focal point for IT Continuity planning for that area
- Ensures the creation/maintenance of IT Continuity plans for each environment considering:
  - Customer requirements
  - Business/management requirements and guidelines
- As appropriate, manages and works with vendors for disaster planning, testing, execution and the return to an operational state
- Communicates with customers and management the results and status of IT Continuity activities
- Identifies process improvement opportunities and communicates them to the process owner
- Defines measurements to determine the efficiency and effectiveness of the process, and acts on poor results
- Identifies and communicates the tool and training requirements to support the process
- Oversees the execution of the IT Continuity Plan in the event of an extended outage
- Ensures that adequate backups are in place for that area
- Defines and implements requests for new services, and communicates with the Process Owner and Team Leader(s)
- Complies with the test objectives set out by the Process Owner

This role has been assigned to the following managers:

- Numerus, including regions – xxx
  - UNIX – xxx
  - Centurion/Beta - xxx
-

---

### 12.3. *IT Continuity Team Leader*

The **IT Continuity Team Leader** is the individual who implements and executes the IT Continuity process for the platform(s) within that team leader's area of responsibility. This role assumes responsibility for developing plans and procedures, as well as testing and maintaining this documentation. The role also involves influencing management decisions with input from the Team Leader's perspective.

- Ensure that you and your alternate are familiar with the IT Continuity Plan for your area
- Ensure that all documentation required for effective recovery in the event of a disaster is in place, current and stored off-site, (configuration information, contact details, procedures etc.)
- Ensure that the recovery team members are familiar with their responsibilities and that the alternate team members are also familiar with these responsibilities
- Ensure that the backup process agreed to for recovery purposes is being followed
- Implement modifications to the relevant documentation, based on test performance
- Respond immediately to a disaster alert
- Participate in damage assessment should you be asked to help determine if a disaster should be declared
- Keep the relevant ABCD officials informed of the situation at all times
- Co-ordinate the work of the recovery team and provide the required support
- Ensure recovery teams are carrying out their responsibilities
- Involve internal and external entities as required, via the IT Continuity Manager
- Oversee the distribution/recovery of the workload to other centres if appropriate, via the IT Continuity Manager
- Assess the overall performance of teams and effectiveness of the IT Continuity Plan during the recovery process in the event of an outage, and act on the results
- Provide the IT Continuity Manager with input to improve the overall process

This role has been assigned to the following co-ordinators:

- Centurion
    - UNISYS NX Support Specialist – xxx
    - IBM Support Specialist – xxx
    - UNIX Support Specialist – xxx
  - Numerus
    - IBM Support Specialist – xxx
    - UNIX Support Specialist – xxx
  - Bloemfontein Data Centre Manager – xxx
  - Pietermaritzburg Data Centre Manager – xxx
  - Eastern Cape Data Centre Manager – xxx
  - Western Cape
    - Data Centre Manager - xxx
    - UNISYS IX Support Specialist – xxx
    - UNIX Support Specialist – xxx
  - Beta Data Centre Manager – xxx
-

---

## **12.4. IT Continuity Team Member**

An **IT Continuity Team Member** is an individual that belongs to a continuity team(s), and has the responsibility of executing the instructions in the IT Continuity plans and procedures to recover affected services. This individual is involved in the process of implementing, testing and maintaining the relevant solutions, so that s/he can recover affected services when requested to do so by the relevant **IT Continuity Manager**.

- Ensure that you and your backup are familiar with the IT Continuity Plan for your area
- Ensure that all documentation required for effective recovery in the event of a disaster is in place, current and stored off-site, (configuration information, contact details, procedures etc.)
- Ensure that the backup process agreed to for recovery purposes is being followed
- Implement modifications to the relevant documentation, based on test performance
- Respond immediately to a disaster alert
- Participate in damage assessment should you be asked to help determine if a disaster should be declared
- Keep the IT Continuity Team Leader informed of the situation at all times
- Assess the overall performance of teams and effectiveness of the IT Continuity Plan during the recovery process in the event of an outage, and act on the results

This role will be assigned to various individuals by the IT Continuity Team Leader as plans are developed.

---

## 13. APPENDIX A – MANAGE IT CONTINUITY TASKS

A task breakdown is provided for each activity identified within the Manage IT Continuity sub-processes.

### 13.1. *Establish the Process Foundation*

Activity	Tasks	Role
Define/Update IT Continuity process.	<ul style="list-style-type: none"> <li>➤ Define and update process scope and objectives</li> <li>➤ Define and update Roles and Responsibilities</li> <li>➤ Define and update process flow</li> <li>➤ Determine process measurements</li> <li>➤ Determine audit requirements</li> <li>➤ Publish process definition document</li> <li>➤ Ensure adherence to Quality Control standards</li> <li>➤ Establish Risk Management process</li> </ul>	ITC Process Owner
Define/Update IT Continuity policies and standards	<ul style="list-style-type: none"> <li>➤ Review existing IT Continuity policies and standards</li> <li>➤ Identify new policies, or update requirements for the policies</li> <li>➤ Develop/Update policies as required, with ITC Manager</li> <li>➤ Ensure policy adherence</li> </ul>	ITC Process Owner
Define/Update IT Continuity Strategy	<ul style="list-style-type: none"> <li>➤ Verify current capability per platform</li> <li>➤ Determine continuity requirements per services per platform</li> <li>➤ Determine gap between current and required capability</li> <li>➤ Examine alternatives and recommend optimal strategy</li> <li>➤ Define Strategy per platform</li> <li>➤ Provide future infrastructure requirements to Capacity Planning</li> </ul>	ITC Process Owner / ITC Co-ordinator
Obtain approval	<ul style="list-style-type: none"> <li>➤ Distribute the document to relevant parties</li> <li>➤ Conduct orientation or awareness sessions as required</li> <li>➤ Obtain formal sign-off</li> <li>➤ File document</li> </ul>	ITC Process Owner
Establish internal/external communication	<ul style="list-style-type: none"> <li>➤ Conduct orientation or awareness sessions</li> <li>➤ Create awareness within Data Centres and within the broader ABCD context (Client Services etc.)</li> </ul>	ITC Process Owner

## 13.2. Create and Maintain IT Continuity Readiness

Activity	Tasks	Role
Gather IT Continuity requirements	<ul style="list-style-type: none"> <li>➤ Define customer availability and data loss requirements</li> <li>➤ Verify and formalise these requirements</li> </ul>	ITC Co-ordinator / Customer Account Managers
Design IT Continuity solution	<ul style="list-style-type: none"> <li>➤ Translate the requirements into a technology solution</li> <li>➤ Determine the organisational impact and requirements (skills, staff levels etc.)</li> <li>➤ Determine the continuity solution that must be designed to implement and support the customer requirement</li> </ul>	ITC Process Owner / ITC Co-ordinator
Map solution to IT Continuity capability	<p>Determine if the current organisational capability is sufficient for solution implementation, maintenance and execution</p> <ul style="list-style-type: none"> <li>➤ Determine if the current technology infrastructure is adequate</li> <li>➤ Determine the effort to implement and document the solution</li> <li>➤ Determine if current IT Continuity-related controls support the proposed solution (IT Continuity Strategy, policies, standards, technical plans etc.)</li> </ul>	ITC Process Owner / ITC Co-ordinator
Review limitations in ITC capability	<ul style="list-style-type: none"> <li>➤ Determine the effort and cost to provide an internal solution</li> <li>➤ Determine the effort and cost to provide an external solution (partnership, service provider etc.), if applicable</li> <li>➤ Determine implementation and maintenance cost, complexity, scalability, risks and benefits</li> <li>➤ Determine if current IT Continuity-related controls support the proposed solution (IT Continuity Strategy, policies, standards, technical plans etc.)</li> <li>➤ Examine alternatives and recommend optimal solution</li> <li>➤ Prepare business case for proposed solution</li> </ul>	ITC Process Owner / ITC Co-ordinator
Request to upgrade IT Continuity capability	<ul style="list-style-type: none"> <li>➤ Submit business case for proposed solution to management for approval</li> <li>➤ Determine if interim solution is required, and implement accordingly</li> </ul>	ITC Co-ordinator

Modify Continuity requirements	<ul style="list-style-type: none"> <li>➤ Examine the results of “Map solution to ITC capability” to determine current capability</li> <li>➤ Examine possible alterations to the service request to improve feasibility</li> <li>➤ Prepare motivation for the change including cost, benefits and risks</li> </ul>	ITC Co-ordinator / Customer Account Manager
Confirm modified requirements with customer	<ul style="list-style-type: none"> <li>➤ Submit motivation from “Modify Continuity requirements”</li> <li>➤ Obtain formal sign-off for modified service request</li> </ul>	ITC Co-ordinator / Customer Account Manager
Reject request	<ul style="list-style-type: none"> <li>➤ Notify customer of decision to reject request, and attach motivation from “Modify Continuity requirements”</li> </ul>	Customer Account Manager
Develop IT Continuity Plans and Procedures	<ul style="list-style-type: none"> <li>➤ Provide feedback to update IT Continuity Strategy if required</li> <li>➤ Define recovery objectives</li> <li>➤ Define escalation process</li> <li>➤ Provide backup requirements to Backup process, and review once implemented</li> <li>➤ Clarify roles and responsibilities</li> <li>➤ List production and continuity resources</li> <li>➤ Describe damage assessment process</li> <li>➤ Describe invocation procedure</li> <li>➤ Describe continuity process</li> <li>➤ Define continuity procedures</li> <li>➤ Define verification procedures</li> <li>➤ Define test and maintenance objectives and processes</li> <li>➤ Compile continuity plan according to ABCD format</li> </ul>	ITC Process Owner / ITC Co-ordinator

---

### 13.3. Perform IT Continuity Plan Test

Activity	Tasks	Role
Develop test plan	<ul style="list-style-type: none"><li>➤ Define primary and secondary test objectives</li><li>➤ Define test guidelines, including aspects of IT Continuity plans and procedures to be tested</li><li>➤ Define roles and responsibilities</li><li>➤ Communicate the test to the relevant people</li><li>➤ Develop estimated time line</li></ul>	ITC Process Owner / ITC Co-ordinator
Schedule test resources	<ul style="list-style-type: none"><li>➤ Ensure the availability of the continuity infrastructure</li><li>➤ Assign primary and alternate names to each role</li><li>➤ Verify that all required documentation is available</li><li>➤ Verify availability of resources external to Data Centres</li></ul>	ITC Process Owner / ITC Co-ordinator / Customer Account Manager
Execute test	<ul style="list-style-type: none"><li>➤ Execute test according to test plan</li><li>➤ Verify results</li></ul>	ITC Co-ordinator / Customer
Conduct test evaluation	<ul style="list-style-type: none"><li>➤ Monitor test effectiveness and efficiency against the test plan</li><li>➤ Monitor the relevance and accuracy of documentation</li><li>➤ Record actual time taken</li><li>➤ Document verification testing performed and results</li></ul>	ITC Process Owner
Communication and awareness	<ul style="list-style-type: none"><li>➤ Publish executive summary of test evaluation report</li><li>➤ Inform the Customer Account Manager</li><li>➤ Discuss test result with customer</li></ul>	ITC Process Owner / ITC Co-ordinator / Customer Account Manager

---

### 13.4. Execute IT Continuity Plan

Activity	Tasks	Role
Damage assessment	<ul style="list-style-type: none"> <li>➤ Initiate damage assessment by appropriate resources</li> <li>➤ Conduct damage assessment meeting</li> <li>➤ Provide motivation based on:               <ul style="list-style-type: none"> <li>➤ Nature and extent of damage</li> <li>➤ Impact on production</li> <li>➤ Effort and time to replace/restore/repair</li> </ul> </li> <li>➤ Take a decision to resolve as operational issue or to recommend IT Continuity invocation to Executive</li> </ul>	Emergency Management Team
Attempt to resolve as a production issue	<ul style="list-style-type: none"> <li>➤ Mobilise internal and external resources to solve problem</li> <li>➤ Issue communication as appropriate</li> <li>➤ Monitor progress against agreed timeframes</li> <li>➤ Convene damage assessment meeting if required</li> </ul>	ITC Co-ordinator
Initiate IT Continuity process	<ul style="list-style-type: none"> <li>➤ Submit recommendation from damage assessment to Executive to motivate the request for invocation</li> <li>➤ Initiate continuity process once approved</li> <li>➤ Issue communication as appropriate</li> </ul>	ITC Process Owner / ITC Co-ordinator / DC Executive
Recover impacted Data Centre services	<ul style="list-style-type: none"> <li>➤ Define recovery priority if applicable</li> <li>➤ Execute IT Continuity process for affected services</li> <li>➤ Ensure continual status updates</li> </ul>	ITC Co-ordinator / ITC Team Leader
Verify recovery	<ul style="list-style-type: none"> <li>➤ Involve all require resources (staff, users, vendors etc.)</li> <li>➤ Once the services have been recovered conduct verification testing</li> <li>➤ Document the results of the verification tests before declaring the services available to all users</li> <li>➤ Issue communication as appropriate</li> </ul>	Process Owner / ITC Co-ordinator / Customer Account Manager / Customer
Communication and awareness	<ul style="list-style-type: none"> <li>➤ Issue communication as appropriate via ABCD HO</li> <li>➤ Obtain management approval for all releases</li> <li>➤ Define audience for communication</li> </ul>	ABCD Public Relations / DC Executive / Customer Account Manager
Support recovered services	Once impacted services are recovered, all standard production availability and support services must be resumed	ITC Co-ordinator / ITC Team Leader / ITC Team Members

### 13.5. *Perform Transition from Continuity to Operational*

<b>Activity</b>	<b>Tasks</b>	<b>Role</b>
Setup production site	<ul style="list-style-type: none"> <li>➤ Restore facility</li> <li>➤ Replace/repair infrastructure</li> <li>➤ Configure equipment</li> </ul>	Emergency Management Team
Plan service relocation	<ul style="list-style-type: none"> <li>➤ Develop plan to relocate affected services</li> <li>➤ Schedule resources</li> <li>➤ Define roles and responsibilities</li> <li>➤ Assign primary and alternate names to roles</li> <li>➤ Determine if IT Continuity plans and procedures need to be modified to relocate services</li> </ul>	Emergency Management Team
Communicate relocation	<ul style="list-style-type: none"> <li>➤ Distribute schedule of system unavailability to Client Services, users and IT staff</li> <li>➤ Establish focal point for queries</li> </ul>	Emergency Management Team / Customer Account Managers
Relocate services	<ul style="list-style-type: none"> <li>➤ Execute relocation as per relocation plan</li> <li>➤ Ensure continual status updates</li> </ul>	ITC Co-ordinator / ITC Team Leader(s) / ITC Members
Verify relocated services	<ul style="list-style-type: none"> <li>➤ Involve all require resources (users, vendors etc.)</li> <li>➤ Once the services have been relocated conduct verification testing</li> <li>➤ Document the results of the verification tests before declaring the services available to all users</li> <li>➤ Issue communication as appropriate</li> </ul>	ITC Co-ordinator / ITC Team Leaders / Customers
Re-instate standard production controls	<ul style="list-style-type: none"> <li>➤ Re-instate standard production controls (user support, backups, security etc.)</li> <li>➤ Ensure compliance with all ABCD policies and standards</li> </ul>	ITC Co-ordinator / ITC Team Leader(s) / ITC Team Members
Update ITC controls and documents	<ul style="list-style-type: none"> <li>➤ Provide feedback to update the IT Continuity Process (if required)</li> <li>➤ Provide feedback to review the IT Continuity Strategy, Plans and Procedures (if required)</li> </ul>	ITC Process Owner / ITC Co-ordinator / ITC Team Leader(s) / ITC Team Members

---

## 14. APPENDIX B - DOCUMENT CONTROL

### 14.1. *Summary of Changes*

<i>Version Number</i>	<i>Date Released</i>	<i>Nature of Change</i>	<i>Date Approved</i>

### 14.2. *Document Change Approvers*

To be determined by ABCD Data Centres.

### 14.3. *Document Review Plans*

To be determined by ABCD Data Centres.

### 14.4. *Document Distribution*

The document will be distributed to those with the following areas of responsibility:

- Executive: Data Centres
- Disaster Recovery Manager and team
- Technical Manager: UNIX
- Technical Manager: Database Administration
- Senior Manager: Software Support Services
- Senior Manager: Capacity Planning
- Senior Manager: Hardware
- Disaster Recovery Co-ordinator: Department of Defence

This list will be used during the development of this document, and will be finalised by the working group.

### 14.5. *Security Classification*

To be determined by ABCD Data Centres.

---