the dpsa

Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

DETERMINATION AND DIRECTIVE ON ICT SERVICE CONTINUITY IN THE PUBLIC SERVICE

MONITORING PLAN

APRIL 2025

CONTENT

1. BACKGROUND

The Minister for Public Service and Administration (MPSA) is responsible for establishing uniform norms and standards to improve the effectiveness and efficiency of the public service and its service delivery to the public in line with Section 3(1)(f) and (i) of the Public Service Act, 1994 as amended.

The 2019/20 and 2020/21 AG reports identify the ICT Service Continuity focus area as one of the areas with fundamental challenges. The current statistics on the AG reports have proven that the controls put in place are not adequate for sustaining ICT Services during a disaster. The lack of ICT system/services resilience impedes ICT adoption as a tool of choice for service delivery.

The Public Service ICT Service Continuity Determination and Directive was published in November 2022 and seeks to guide departments on minimum requirements to consider when developing the ICT Service Continuity Plan. The minimum requirements contained in the Determination and Directive aim to ensure resiliency before, during, and after an ICT Disaster.

2. PURPOSE

The purpose of the plan is to outline the strategic intent of the Determination and Directive into measurable criteria that will be used by the DPSA to monitor and evaluate the implementation of the Determination and Directive by departments. Furthermore, the plan articulates the requirements of the Determination and Directive on the implementation of ICT Service Continuity into measurable criteria against which the departments can measure ICT compliance and performance.

3. OBJECTIVES

The objectives of the compliance monitoring process are as follows:

- Track the progress departments are making in implementing the determination and directive.
- Identify challenges encountered during the implementation phase and provide remedial action.
- Determine lessons learned as a baseline for improvement.
- Determine the effectiveness of the determinations and directives and identify areas of improvement.

4. SUMMARY OF MONITORING INDICATORS AND EVIDENCE (ICT SERVICE CONTINUITY)

The DPSA will use monitoring indicators to measure departments' progress in implementing the determinations and directives. The tables below provide a high-level overview of the monitoring indicators that will be used to measure compliance with the determinations and directives.

4.1. SUMMARY OF MONITORING INDICATORS (KEY PERFORMANCE AREAS)

Indicator 1.	**ICT SERVICE CONTINUITY PLAN**
Indicator 2.	**ESTABLISHMENT OF AN ICT DISASTER RECOVERY TEAM**
Indicator 3.	**IDENTIFICATION OF ALL DEPARTMENTAL CRITICAL INFORMATION SYSTEMS/ ICT SERVICES**
Indicator 4.	**DISASTER RECOVERY RELATED DOCUMENTATION**
Indicator 5.	**ALTERNATIVE ICT DR SITE/ ENVIRONMENT**
Indicator 6.	**BACKUP AND RECOVERY**
Indicator 7.	**TESTING AND MAINTENANCE OF THE ICT SERVICE CONTINUITY PLAN**
Indicator 8.	**INVENTORY OF THE DEPARTMENT'S ICT INFRASTRUCTURE**

4.2. SUMMARY OF EVIDENCE

ICT SERVICE CONTINUITY DETERMINATION AND DIRECTIVE	
1	Approved ICT service continuity plan
2	Evidence that demonstrates that disaster recovery testing is performed in the environment
3	Evidence that demonstrates that there is efficient operational backups in the department

5. ASSESSMENT CRITERIA

5.1. PURPOSE OF ASSESSMENT CRITERIA

The assessment criteria will be used to measure whether the departments comply with the requirements set in the determinations and directives.

5.1.1. NON-COMPLIANT

Non-compliant refers to a department that has not fully implemented the requirements of the determinations and directives.

5.1.2. FULLY COMPLIANT

Fully compliant refers to a department that has fully implemented the requirements of the determinations and directives.

6. DATA COLLECTION

Departments will be required to upload their compliance information on the online DPSA compliance portal.

7. DPSA ICT SERVICE CONTINUITY DETERMINATION AND DIRECTIVE MONITORING PROCESS

The DPSA will conduct an annual assessment using the criteria mentioned above through the assessment process indicated in the figure below:

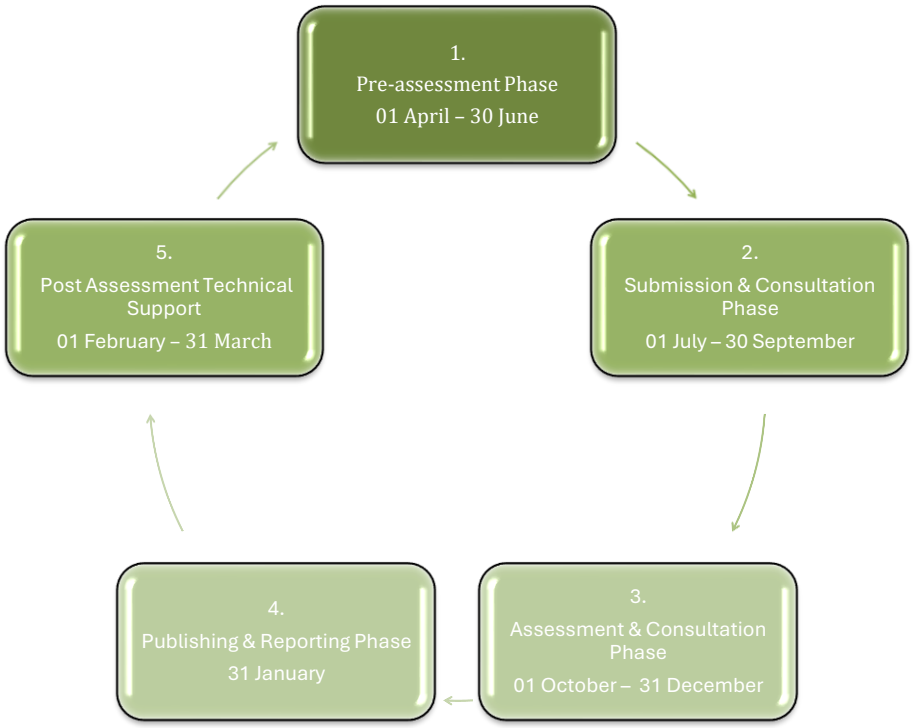

Figure 1: DPSA ICT Service Continuity ICT assessment process

DPSA ICT Service Continuity assessment process

NO	ASSESSMENT PHASE / ACTIVITY	TIME-FRAME	RESPONSIBLE
1. PRE-ASSESSMENT PHASE *(Preparation for submission as per the requirements of the assessment standard)*		1 April – 30 June	DPSA
1.1	Publishing of the self-assessment toolkits *(e.g. assessment standard, guidelines, and reporting templates).*		
1.2	Provide technical support to departments on self-assessment.		
2. SUBMISSION & CONSULTATION PHASE *(capturing, validation and approval of the submitted evidence)*		1 July - 30 September	DPSA All departments
2.1	Submit self-assessment reports & evidence by departments.		
2.2	Capture & validate the submitted self-assessment reports & evidence in line with assessment standard		
2.3	Approve the validated assessment evidence in line with assessment standards.		
2.4	Conduct consultations with departments on submission of self-assessment reports & uploading of evidence submission.		
2.5	Send confirmation / submission acknowledgement to departments.		

NO	ASSESSMENT PHASE / ACTIVITY	TIME-FRAME	RESPONSIBLE
3. ASSESSMENT AND POST SUBMISSION CONSULTATION *(assessing the reports and evidence submitted by departments)*		01 October – 31 December	DPSA
3.1	Moderate the submitted information and evidence submitted by departments in line with assessment standards.		
3.2	Consult departments-based assessment outcome. *(e.g. opportunity for departments to consult the DPSA on areas for clarity or dispute)*		
3.2.1	Provide support by responding to clarity seeking questions / disputes		
3.2.2	Resolve disputes		
4. PUBLISHING & REPORTING TO DEPARTMENTS *(publishing of final assessment results for departments to implement)*		01 January – 31 January	DPSA
4.1	Report on assessment outcome and provide comments to departments		
4.2	Publish final assessment results for departments to implement		
5. POST ASSESSMENT TECHNICAL SUPPORT *(providing support to departments with unsatisfactory assessment outcomes)*		1 February – 31 March	DPSA All Departments
5.1	Support departments on implementing remedial actions emanating from the assessment		

8. TECHNICAL INDICATOR DESCRIPTORS

INDICATOR 1. ICT SERVICE CONTINUITY PLAN	
Definition	An ICT Service Continuity Plan is a comprehensive plan that outlines the procedures and strategies a department will follow to ensure that its critical ICT services can continue or be restored in the event of a disruption. The plan is a vital component of a department's overall business continuity management (BCM) framework and aims to minimize the impact of incidents, maintain essential functions, and ensure a swift return to normal operations. Key components of an ICT Service Continuity Plan are: 1. Risk Assessment and Business Impact Analysis (BIA) 2. Recovery Objectives 3. Continuity and Recovery Strategies 4. Emergency Response and Crisis Management: 5. Testing 6. Communication Plan 7. Maintenance and Review 8. Documentation Departments must develop an ICT continuity plan aligned with and informed by the departmental business continuity plan, which is the responsibility of Enterprise Risk Management.
Source of Data	ICT Service Continuity Plan
Means of Verification	Verify that the ICT Service Continuity plan is approved
Assumptions	Departments are aligned to CGICTPF V2 which has a requirement on ICT Service Continuity Plan.
Indicator Responsibility	All departments

INDICATOR 2. ESTABLISHMENT OF AN ICT DISASTER RECOVERY TEAM	
Definition	The Head of department must establish an ICT Disaster Recovery Team for the department. The ICT Disaster Recovery Team led by the GITO will develop, document, and execute processes for a department's data recovery for business continuity, and IT infrastructure in the event of a disaster (ICT service/system) disruption.
Source of Data	ICT Service Continuity Plan
Means of Verification	Verify /check in the plan that there is a disaster recovery team in the department
Assumptions	Departments are aligned to CGICTPF V2 which has a requirement on ICT Service Continuity Plan.
Indicator Responsibility	All departments

INDICATOR 3. IDENTIFICATION OF ALL DEPARTMENTAL CRITICAL INFORMATION SYSTEMS/ ICT SERVICES	
Definition	The Head of Department, through the GITO must ensure that the department conducts a Business Impact Analysis (BIA) internally and the minimum critical ICT services that must be provided by the department even during the disruption/disaster are identified. Determination of system availability/capacity requirements of the department informed by the BIA or their criticality. The Head of Department must determine the duration within which critical ICT services Recovery Time Objectives (RTO) must be recovered should a disaster/disruption occur, this must be expressed in minutes, hours, or days. The Head of Department must determine the recovery point and the associated data/information that must be retrieved during the disaster. The Recovery Point Objectives (RPO) after the disaster/disruption must be expressed in minutes, hour and days in case of future disruptions.
Source of Data	ICT Service Continuity Plan
Means of Verification	Verify /check in the plan that critical systems and services have been defined and classified
Assumptions	Departments are aligned to CGICTPF V2 which has a requirement on ICT Service Continuity Plan.
Indicator Responsibility	All departments

INDICATOR 4. DISASTER RECOVERY RELATED DOCUMENTATION	
Definition	The Head of Department must ensure the existence and safekeeping of all relevant documentation that will support disaster recovery efforts by the department. Such documents must include but are not limited to the design and configuration of the system documents primarily for critical and other systems, systems recovery procedures, contact details of staff (including 3rd party contractors) to assist/conduct recovery, relevant 3rd party suppliers, etc.
Source of Data	ICT Service Continuity Plan
Means of Verification	Verify /check in the plan that DR related documents are kept secure
Assumptions	Departments are aligned to CGICTPF V2 which has a requirement on ICT Service Continuity Plan.
Indicator Responsibility	All departments

INDICATOR 5. ALTERNATIVE ICT DR SITE/ ENVIRONMENT	
Definition	The Head of Department must ensure provision of an alternative disaster recovery site. Alternative disaster recovery (DR) sites are critical components of a business continuity plan. These sites serve as backup locations where businesses can continue operations in the event that the primary site is unavailable due to a disaster such as a natural calamity, cyberattack, or any other disruptive event.
Source of Data	ICT Service Continuity Plan
Means of Verification	Verify /check the plan that there is an alternative recovery site
Assumptions	Departments are aligned to CGICTPF V2 which has a requirement on ICT Service Continuity Plan.
Indicator Responsibility	All departments

INDICATOR 6. BACKUP AND RECOVERY	
Definition	The GITO must establish a process of creating and storing copies of data that can be used to protect the department against data loss.
Source of Data	Backup evidence (snapshot of the backup environment with backup jobs)
Means of Verification	Verify /check that the submitted evidence adequately demonstrates that backups are performed
Assumptions	Departments are aligned to the Public Service Information Security Directive
Indicator Responsibility	All departments

INDICATOR 7. TESTING AND MAINTENANCE OF THE ICT SERVICE CONTINUITY PLAN	
Definition	The GITO must identify and prioritize the business functions, maintaining the ICT systems that support their operations. The recovery arrangements must also be established to preserve the continuity of ICT services. The GITO must ensure that the ICT Service Continuity Plan is tested and maintained regularly for effectiveness.
Source of Data	Close out reports or any evidence of tests conducted
Means of Verification	Verify or check that the evidence adequately demonstrates that tests are conducted
Assumptions	Departments are aligned to CGICTPF V2 which has a requirement on ICT Service Continuity Plan.
Indicator Responsibility	All departments

INDICATOR 8. INVENTORY OF DEPARTMENT'S ICT INFRASTRUCTURE	
Definition	The GITO must establish an inventory of the environmental ICT infrastructure. This inventory list must include: - Hardware - Software (Including Applications) - Network information assets (i.e., Servers, Switches, Firewalls, Routers, Virtual Machines) - Network Diagram/Blueprint of the department.
Assumptions	Departments are aligned to CGICTPF V2 which has a requirement on ICT Service Continuity Plan.
Indicator Responsibility	All departments