FINALISED 24/07

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

DBAC SUBMISSION

RECEIVED
CENTRAL POINT
08:18
2023 -07- 21
OFFICE OF THE DG

Tracking no D35086

ROUTE FORM

BRANCH: FINANCE

Reference No: WD418

SUBJECT: **WD418:** DEVIATION AND TO APPOINT SITA TO PROVIDE SECURITY OPERATIONS CENTRE (SOC) SERVICES TO DWS FOR A PERIOD OF THREE (3) YEARS

DBAC SECRETARIAT		SUPERVISOR	
Name: Ms Hester van der Merwe Ms Marshia Batayi Ext : 7725/ 7474 Office :522 ZWA		Name: Ms N Khubana Extension: 8926 Office No.: ZWA	
Rank: SPAO	Date:	Rank: Director	Date:

Rank	Date	Name and Surname	Signature	Office No
CFO (CHAIRPERSON OF DBAC)		Frans Moatshe		0709

24/07/23 DG

INSTRUCTIONS/REMARKS TO AUTHOR BY ACTING DIRECTOR-GENERAL

DEPARTMENT OF WATER AND SANITATION
OFFICE OF THE DG
RECEIVED
PM
11H30
2023 -07- 21
185 FRANCIS BAARD STREET
PRETORIA 0001
DEPARTMENT OF WATER AND SANITATION

Rec: 24.07.2023

21/7/2023

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

ENQUIRIES: A Kitchen
TELEPHONE: 012-336-8157
REFERENCE: 4/8/3/6/4/1

DEPARTMENTAL BID ADJUCICATION COMMITTEE

REQUEST TO DEVIATE AND APPOINT SITA TO PROVIDE SECURITY OPERATIONS CENTRE TO THE DEPARTMENT OF WATER AND SANITATION OVER A PERIOD OF THREE (3) YEARS

1. PURPOSE

1.1. To obtain approval to deviate and appoint SITA to provide Security Operations Centre (SOC) services in the Department for a period of three (3) years.

2. BACKGROUND AND DISCUSSION

2.1 The Information Security Strategy was developed and approved in June 2022. One of the initiatives highlighted in this strategy is the need for ensuring better detection capabilities regarding security event monitoring, cyber analytics, cyber threat intelligence, vulnerability scanning and more frequent penetration testing.

2.2 To achieve this initiative, DWS developed technical specifications for the Security Operations Centre (SOC) services, with the aim of publishing these in the open market to source a suitable service provider.

2.3 SITA indicated to the Department that they are putting in place a SOC services contract that will be used by government departments and the DWS specifications are aligned with this contract based on the discussion held between DWS and SITA for the IT outsourcing services. The tasking letter is attached as **Annexure A.**

2.4 In October 2022, the DWS issued a tasking letter to SITA to provide a proposal to the Department to render these services. SITA is mandated through the SITA Act, to provide security related services to all government departments. The proposal is attached **(Annexure B).**

2.5 SITA's objective as stated in the SITA Act No. 38 of 2002 is to "(a) to improve service delivery to the public through the provision of information technology, information systems and related services in a maintained information systems security environment to departments and public bodies; and (b) to promote the efficiency of departments and public bodies through the use of information technology". Below is the extract from the act for ease of reference.

REQUEST TO DEVIATE AND APPOINT SITA TO PROVIDE SECURITY OPERATIONS CENTRE TO THE DEPARTMENT OF WATER AND SANITATION OVER A PERIOD OF THREE (3) YEARS

Act No. 38, 2002 STATE INFORMATION TECHNOLOGY AGENCY AMENDMENT ACT, 2002

Amendment of section 6 of Act 88 of 1998

4. The following section is hereby substituted for section 6 of the principal Act:

"Objects of Agency

6. The objects of the Agency are—

(a) to improve service delivery to the public through the provision of information technology, information systems and related services in a maintained information systems security environment to departments and public bodies; and

(b) to promote the efficiency of departments and public bodies through the use of information technology.".

2.6 Section 7(3) and 7(4.b.ii) of the SITA Act further states that:

(3) Despite any other law to the contrary, every department must, subject to subsection (4), procure all information technology goods or services through the Agency.

(4) A department that wishes to acquire a service contemplated in—

(a) subsection (1)*(a)*, must—

(i) acquire that service from the Agency in accordance with business and service level agreements concluded in terms of section 20; or

(ii) procure that service through the Agency in terms of subsection (3) if the Agency indicates in writing that it is unable to provide the service itself;

(b) subsection (1)*(b)*, must either—

(i) acquire that service from the Agency in accordance with business and service level agreements concluded in terms of section 20; or

(ii) procure that service through the Agency in terms of subsection (3).

2.7 Furthermore, as per PFMA SCM Instruction Note No. 3 of 2021/22 number 4.1 states:

4. DEVIATIONS FROM NORMAL BIDDING PROCESS

4.1 If in a specific case it is impractical to invite competitive bids, the AO/AA may procure the required goods or services by other means, provided that the reasons for deviating from inviting competitive bids must be recorded and approved by the AO/AA.

2.8 The SOC service will be an independent assurance of the security state within the DWS by providing a 24X7 monitoring, prevention, detection, investigation, and response for day-to-day security events. SITA will also provide supporting services such as remediation, threat intelligence (TI) and TI integration, hunts, and device management.

2.9 Documents attached to this submission are:

Annexure A	Technical specifications
Annexure B	SITA Proposal
Annexure C	Demand Plan
Annexure D	BAS Report

3. IMPLICATIONS

3.1 Personnel

None

3.2 Financial

The financial implication is estimated at R6 000 000.00 per year.

3.2.2 The Chief Directorate: Information Services budget will be utilized for payment.

SCOA SEGMENT	ALLOCATION DESCRIPTION	ALLOCATION CODES
FUND :	VOTED FUNDS	341222
RESPONSIBILITY :	DIR:ICT GOV COMP RISK & INFO SEC	30586906
OBJECTIVE :	INFORMATION & COMM TECHNOLOGY	30027906
PROJECT :	NO PROJECTS	18906
ITEM :	SITA SPECIALISE COMPT SER	1346906
ASSET INDICATOR:	NON-ASSETS RELATED	22906
INFRASTRUCTURE :	NON INFRA/ST ALONE:CURRENT	49906
REGION IDENTIFIER:	NAT FUNCTION:WHOLE COUNTRY DOM	30002906

3.3 Legal

None

3.4 Regulatory Compliance

SITA Act No. 38 of 2002.
PFMA SCM Instruction Note No. 3 of 2021/22 (4.1).
Financial delegation of 2021, item 2.17.

3.5 Communication

None

4. OTHER COMPONENTS CONSULTED

4.1 None

REQUEST TO DEVIATE AND APPOINT SITA TO PROVIDE SECURITY OPERATIONS CENTRE TO THE DEPARTMENT OF WATER AND SANITATION OVER A PERIOD OF THREE (3) YEARS

5. RECOMMENDATION

It is recommended that you approve:

5.1 the deviation and appointment of SITA as a service provider to Security Operations Centre (SOC) services in the Department for a period of three years.

INFORMATION SECURITY AND RISK MANAGER

NAME: Anette Kitchen

DATE: 19 June 2023

RECOMMENDATION IN PAR 5.1 SUPPORTED / ~~NOT SUPPORTED~~

DIRECTOR: ICT GOVERNANCE, RISK AND SECURITY

NAME: Monelisi Njeza

DATE: 19/06/2023

RECOMMENDATION IN PAR 5.1 SUPPORTED / NOT SUPPORTED

CHIEF INFORMATION OFFICER

NAME: A.Kekana

DATE: 22/06/2023

RECOMMENDATION IN PAR 5.1 SUPPORTED / ~~NOT SUPPORTED~~

ON CONDITION THAT:
1. INDEED IT IS IMPRACTICAL TO INVITE THE COMPETITIVE BIDS AS PER THE DEVIATION REGULATIONS
2. INDEED IT IS WITHIN THE REGULATIONS THAT SITA COULD BE THE ONLY SERVICE PROVIDER TO RENDER THE SERVICES IN TERMS OF SITA ACT WITHOUT GOING OUT TO THE MARKET TO SOURCE THE SERVICES FROM THE COMPETITIVE BIDS

DEPUTY DIRECTOR-GENERAL: CORPORATE SERVICES

NAME: ONV FUNDAKUBI

DATE: 2023/06/23

REQUEST TO DEVIATE AND APPOINT SITA TO PROVIDE SECURITY OPERATIONS CENTRE TO THE DEPARTMENT OF WATER AND SANITATION OVER A PERIOD OF THREE (3) YEARS

FUNDS AVAILABLE / ~~FUNDS NOT AVAILABLE~~

CHIEF FINANCIAL OFFICER

NAME: F Mogotsi

DATE: 2023/08/26

RECOMMENDATION IN PAR 5.1 SUPPORTED / NOT SUPPORTED

RECOMMENDED
BID ADJUDICATION COMMITTEE
DATE: 26/07/23

CHAIRPERSON: DEPARTMENTAL BID ADJUDICATION COMMITTEE

NAME:

DATE:

RECOMMENDATION IN PAR 5.1 APPROVED / ~~NOT APPROVED~~

DIRECTOR-GENERAL

NAME: DR SEAN PHILLIPS

DATE: 24/07/23

SITA SOC Ltd, 459 Tsitsa Street, Erasmuskloof, Pretoria, South Africa • PO Box 26100, Monument Park, 0105, South Africa
Tel: +27 12 482 3000 • Fax +27 12 367 5151 • Reg. No 1999/001899/30 • www.sita.co.za

Our Ref: **Procurement**
Enquiries: Unathi Thoka
Tel: +27 12 482-2238
Date: 04 July 2023

NATIONAL DEPARTMENT OF WATER AND SANITATION (DWS)
185 Francis Baard Street
Pretoria
0001

Dear Mr. Arthur Kekana

Chief Information Officer

RE: PROCUREMENT OF IT INFORMATION SECURITY GOODS AND SERVICES

This letter seeks to clarify the query of the National Department of Water and Sanitation whether IT information Security Goods and Services are mandatory services or not and further which process the department must follow when it requires to source those services.

In terms of Section 7(3) of the SITA Act (Act 88 of 1988), every department must procure all information technology goods or services through or from SITA. A "department" is defined in section 1 of the SITA Act as a national department, provincial administration, provincial department or organisational component listed in schedules 1, 2 and 3 to the Public Service Act, 1994.

Even though section 7 (1) of the SITA Act makes a distinction between the "may" and "must" services ,all these services have to be procured through or from SITA, in terms of Section 7 (3).

The **IT Information Security goods or services** is a mandatory service in terms of s.7(1)(a)(ii) of the SITA Act.
For ease of reference, please see attached **SITA Act.**

The department when it needs to source Information Security Goods and Services, the department must formally send SITA a tasking letter that is signed by the Accounting Office or a person who has delegation to source such services. Upon receiving the tasking letter , SITA will have a meeting with the department technical team to understand the User Requirements Specification (URS) and finalise it together with the department. Both SITA and DWS will then signoff the URS and after that SITA will furnish the department with a proposal. After the department have accepted and issued the government order, SITA will then start with the implementation of the required solution.

Non-Executive Directors:
Ms M Mosidi (Chairperson), Ms S Bvuma (Dr) (Deputy Chairperson), Ms S Moonsamy, Ms N Pietersen, Ms Z Hill, Ms O Ketsekile, Mr T Ratshitanga (Dr), Mr R Ramabulana, Mr W Vukela, Ms L Mseme, Ms J Morwane, Mr M Ratshimbilani
Executive Directors:
Dr BA Mabaso (Managing Director) Mr MK Kgauwe (Chief Financial Officer),
Mr TV Mphaphuli (Company Secretary: Acting)

SITA remains committed to our ongoing service delivery and support to the National Department of Water and Sanitation as a valued client. Please do not hesitate to contact your Client Relationship Manager(CRM) , Ms. Unathi Thoka on **074 605 0473** should you need more clarity.

Yours sincerely.

.....

Stephen Motlhaoleng
SPCHD Cluster Advocate

Non-Executive Directors:
Ms M Mosidi (Chairperson), Ms S Bvuma (Dr) (Deputy Chairperson), Ms S Moonsamy, Ms N Pietersen, Ms Z Hill, Ms O Ketsekile, Mr T Ratshitanga (Dr), Mr R Ramabulana, Mr W Vukela, Ms L Mseme, Ms J Morwane, Mr M Ratshimbilani
Executive Directors:
Dr BA Mabaso (Managing Director) Mr MK Kgauwe (Chief Financial Officer),
Mr TV Mphaphuli (Company Secretary: Acting)

Security Operation Centre Services (SOC) roles and responsibilities		
Provision and operation of a SIEM service	X	
Security Orchestration, Automation and Response (SOAR)	X	
Vulnerability Management service including external penetration testing twice a year.	X	
Threat Intelligence (TI) (open and commercial)	X	
Threat hunting (manual and machine-assisted methods)	X	
Intrusion detection	X	
Incident response	X	
First Expert Verdict (FEV) for incident response	X	
Monitor and analyse day-to-day security events	X	
User Behaviour Analytics (UBA)	X	
24/7/365 monitoring and management	X	
Alert triage process	X	
Incident playbooks	X	
Alert prioritization matrix	X	
Incident categorization	X	
Incident security process	X	
Reporting matrix and KPIs	X	
Cyber threats countermeasures planning through research and development	X	
Practical recommendations for remediation and prevention of threats and other related matters	X	
Provide same visibility as the SOC has to the DWS security management	X	
Perform Cybersecurity forensic investigation services	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	
Manage capacity	X	
Develop and implement application security standards	X	
Develop and implement cloud security standards	X	

MARKET ANALYSIS REPORT TO REQUEST TO DEVIATE AND APPOINT SITA TO PROVIDE SECURITY OPERATIONS CENTRE TO THE DEPARTMENT OF WATER AND SANITATION OVER THE PERIOD OF THREE YEARS

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

MARKET ANALYSIS REPORT

PURPOSE

The aim of this exercise is to determine the number of suppliers available on the market, credibility to deviate and appoint SITA to provide security operations centre (SOC) to the Department.

BACKGROUND

The information Security Strategy was developed and approved in June 2022. One of the initiatives highlighted in this strategy was the need ensuring better detection capabilities regarding security event monitoring, cyber analytics, cyber threat intelligence, vulnerability scanning and more frequent penetration testing.

COMMODITY AND SUPPLIER ANALYSIS / ENGAGEMENT

To achieve this initiative, the department developed technical specification for the SOC, with the aim of publishing these in the open market to source for a suitable service provider.

SITA indicated to the Department that they are putting in place a SOC service contract that will be used by government departments and the DWS specifications are aligned with this contract based on the discussion held between the DWS and SITA for the IT outsourcing services.

In October 2022, the DWS issued a tasking letter to SITA to provide a proposal to the Department to render these services. SITA is

mandated through the SITA act, to provide security related services to all government departments.

It should be noted that there are other suppliers in the market who can provide the service for SOC (**Cyber Africa, Dimension Data, Phakamo Tech, Sizwe Technologies and etc**).

In terms of SITA act, section 7(3) and 7(4.b.ii) states that despite any other law to the contrary, every department must procure all information technology goods or services through SITA. A department that wishes to acquire a service planned for must acquire that service from the Agency in accordance with business and service level agreement concluded in terms of section 20.

DEVIATION FROM NORMAL BIDDING PROCESS

Public Finance Management Act, Supply Chain Management instruction note no. 3 of 2021/22 states that Accounting officer may procure the goods / services by other means, provided that the reasons for deviating from inviting competitive bids must be recorded and approved by the Accounting Officer.

RECOMMENDATION

Based on the analysis, it is recommended that the request to deviate and appoint SITA to provide SCO services be considered.

Compiler: Siphiwe Nxumalo

ASD: Demand Management

Date: 29/06/2023

MARKET ANALYSIS REPORT TO REQUEST TO DEVIATE AND APPOINT SITA TO PROVIDE SECURITY OPERATIONS CENTRE TO THE DEPARTMENT OF WATER AND SANITATION OVER THE PERIOD OF THREE YEARS

RECOMMENDATION SUPPORTED/NOT SUPPORTED

DD: Demand Management

Date: 29/06/2023

CONFIDENTIAL

DWS Information Security services Requirements

DWS requires security services with the aim of implementing and improving technical and information security controls that will ensure the protection of enterprise information against illegal intrusion by unauthorized users. These services include:

1. Security operations
2. Remote access
3. End-point protection
4. Perimeter security
5. Logical access control
6. Patch management
7. Security awareness and training
8. Data backup and disaster recovery

1. Services, Roles and Responsibilities

1.1. Security Operations

Security operations are the activities associated with the day-to-day management of the information security environment, providing and supporting a stable security posture and effectively and efficiently performing operational procedures to ensure the services meet Service Level Requirement (SLR) targets and requirements. The following table identifies the Operations roles and responsibilities to be performed.

Security Operations Roles and Responsibilities	Provider	DWS
Planning and prevention roles and responsibilities		
Define planning and prevention requirements and policies		X
Define and implement and configure appropriate tools and security metrics	X	
Define and implement methodologies to be used in detection response and monitoring	X	
Define and implement key performance indicators for cyber security	X	
Perform research and development to implement countermeasures against cyber threats	X	
Security Operation Centre Services (SOC) roles and responsibilities		
Provision and operation of a SIEM service	X	
Security Orchestration, Automation and Response (SOAR)	X	
Vulnerability Management service including external penetration testing twice a year.	X	
Threat Intelligence (TI) (open and commercial)	X	
Threat hunting (manual and machine-assisted methods)	X	
Intrusion detection	X	
Incident response	X	

First Expert Verdict (FEV) for incident response	X	
Monitor and analyse day-to-day security events	X	
User Behaviour Analytics (UBA)	X	
24/7/365 monitoring and management	X	
Alert triage process	X	
Incident playbooks	X	
Alert prioritization matrix	X	
Incident categorization	X	
Incident security process	X	
Reporting matrix and KPIs	X	
Cyber threats countermeasures planning through research and development	X	
Practical recommendations for remediation and prevention of threats and other related matters	X	
Provide same visibility as the SOC has to the DWS security management	X	
Perform Cybersecurity forensic investigation services	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	
Monitoring and management roles and responsibilities		
Perform 24/7/365 monitoring and management	X	
Conduct Root Cause Analysis (RCA) and submit recommendations for remediation and prevention of threats and other related matters	X	
Provide reporting against KPIs	X	
Provide proactive and scheduled console monitoring of security across the network, respond to messages and take corrective action as required	X	
Provide preventative measures for proactive monitoring and self-healing capabilities to limit threats that impact service delivery	X	
Review and approve monitoring procedures	X	
Develop and maintain standard automated scripts to perform monitoring on systems software	X	
Provide daily, weekly and monthly reports as set out in the SLR	X	
System Administration Roles and Responsibilities		
Define system administration requirements and policies		X
Develop and document in the Standards and Procedures Manual procedures for performing system administration that meet requirements and adhere to defined policies	X	
Review and approve systems administration procedures		X

Set up and manage End-User accounts, perform access control, manage files and disk space and manage transaction definitions in accordance with information security guidelines	X	
Perform system or component configuration Changes necessary to support computing services in conformance with Change Management requirements	X	
Provide usage statistics reports that will be used to support chargeback and other reporting requirements	X	
Implement system administration polices and standards	X	
Manage capacity	X	
Develop and implement application security standards	X	
Develop and implement cloud security standards	X	

1.2. Remote Access

Remote Access Services are the activities associated with the installation, management, operations, administration and support of the hardware and software that support Remote Access and connectivity to all systems (e.g., VPN, Citrix Metaframe via dialup and Internet, Web-based e-mail). The following table identifies the Remote Access roles and responsibilities that the provider and DWS will perform.

Remote Access Roles and Responsibilities	Provider	DWS
Define Remote Access standards and procedures		X
Define requirements and standard for remote access management		X
Develop and document the Standards and Procedures that meet requirements and adhere to defined policies	X	
Review and approve Remote Access standards and procedures		X
Install, test, provide technical support, administration and security administration for remote access hardware and software	X	
Provide testing support for defined DWS applications that will be made available via remote access	X	
Provide technical assistance and subject matter expertise as required by DWS infrastructure staff and third-party solution providers for remote access products and solutions	X	
Perform system or component configuration changes necessary to support remote access services	X	
Provide troubleshooting, repair and escalation of problems in the remote access management solution(s) environment	X	
Provide proactive and scheduled management of the remote access management solution(s) (e.g., hardware, middleware, network, interfaces, versions of software and/or solution(s) (major and minor upgrades), respond to messages and take corrective action as required	X	
Maintain the version of the solution(s) to ensure the latest approved version is installed including middleware where required	X	
Provide advice in terms of the capabilities of the Remote Access Management Solution(s) where required	X	

Remote Access Roles and Responsibilities	Provider	DWS
Respond to all requests and perform the necessary tasks to ensure that the environment is not vulnerable	X	
Ensure that the logs for the operating system(s) as well as the solution(s) is stored securely and being backed up	X	
Provide detailed analysis of the remote access management solution(s) logs	X	
Provide input into the relevant policy, standard, etc. documents when required	X	
Ensure remediation of audit findings and vulnerability assessments and any other findings that might be received	X	
Identify and report problems including hardware, system, file, disk and solution(s)problems proactively	X	
Resolve or assist in resolving solution(s) problems in accordance with SLRs and escalate as required	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	
Provide monthly reports on the details around remote access management as set out in the SLR.	X	

1.3. Endpoint Protection

Endpoint Protection Services are the activities associated with the day-to-day management of the endpoint protection environment, providing and supporting a secure environment and effectively and efficiently performing operational and processing procedures to ensure services meet SLR targets and requirements. The following table identifies the Endpoint Protection Solution Management roles and responsibilities that the provider and DWS will perform.

Endpoint Protection Roles and Responsibilities	Provider	DWS
Define requirements and standard for endpoint protection		X
Develop and document the procedures document for managing the endpoint protection solution that meet requirements and adhere to defined policies and standards	X	
Review and approve the endpoint protection solution management procedures		X
Provide proactive and scheduled management of the endpoint protection solution (e.g., hardware, network, scheduled scans, interfaces, versions of software on workstations/servers (major and minor upgrades), outdated updates on workstations/servers, etc.), respond to messages and take corrective action as required	X	
Ensure availability of latest end-point protection licenses		X
Maintain the latest approved solution versions on all workstations/servers	X	
Develop and maintain standard automated scripts to perform management of the endpoint protection solution	X	

Ensure that patches of the endpoint protection solution are tested and installed in conjunction with the responsible parties for patch management	X	
Perform scheduled/immediate deployment of the endpoint protection solution to all DWS equipment	X	
Confirm and ensure that the endpoint protection solution for clients and servers is fully operational (including the latest definition file is installed) and being monitored once deployed	X	
Ensure that the features of the Endpoint Protection Solution are implemented to offer the optimal level of protection against threats while ensuring effectiveness and efficiency of the IT environment	X	
Provide advice in terms of the endpoint protection solution's capabilities when required	X	
Perform necessary interventions at desktop/server level where problems/issues are experienced	X	
Respond to all threats & vulnerabilities and perform the necessary tasks to ensure workstations/servers are not vulnerable	X	
Ensure that the logs for the operating system(s) as well as the solution(s) is stored securely and being backed up	X	
Respond and provide information for audit purposes	X	
Provide input into the relevant policy, standard, etc documents when required	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	
Monitoring Endpoint Protection Roles and Responsibilities		
Define monitoring requirements and standard for endpoint protection		X
Develop and document the procedures document for the monitoring of the end point protection environment.	X	
Review and approve monitoring procedures		X
Provide proactive and scheduled console monitoring of endpoint protection solution (e.g., hardware, network, scheduled scans, interfaces, versions of software on workstations/servers, outdated updates on workstations/servers, etc.), and respond to messages and take corrective action as required	X	
Develop and maintain standard automated scripts to perform monitoring of endpoint protection solution	X	
Proactively, troubleshoot, repair and report incidents relating to Endpoint Protection solution including zero-day attacks/outbreaks	X	
Perform 24/7/365 monitoring and management	X	
Provide weekly and monthly reporting on Logical Access Control as set out in the SLR	X	

1.4. Perimeter security Services

Perimeter Security Services are the activities associated with the day-to-day management of the Firewall(s) and Proxy devices that provide a stable and secure environment. The Provider must perform support effectively and efficiently to ensure services meet SLR targets and requirements.

The following table identifies the Perimeter Security Services roles and responsibilities that the Provider and DWS will perform.

Firewall(s) and Proxy Management Roles and Responsibilities	Provider	DWS
Define requirements and standard for firewall(s) and proxies		X
Develop and document the procedures for managing the firewall(s) and proxies that meet requirements and adhere to defined policies and standards	X	
Review and approve the firewall(s) and proxies procedures		X
Ensure that the firewall(s) and proxies solution(s) are backed up as required (e.g. configurations, etc)	X	
Ensure proper configuration management and reporting thereof	X	
Provide proactive and scheduled management of the firewall(s) and proxies (e.g., hardware, middleware, network, interfaces, versions of software and/or devices (solution(s)) (major and minor upgrades), respond to alerts and take corrective action as required	X	
Ensure availability of licenses for the solution(s)		X
Maintain the version of the solution(s) to ensure the latest approved version is installed including middleware where required	X	
Develop and maintain standard automated scripts to perform management of the solution(s)	X	
Ensure that patches of the firewall(s) and proxies solution(s) are tested and installed in conjunction with the responsible parties for patch management where relevant	X	
Ensure that the features of the Firewall(s) and Proxies solution are implemented to offer the optimal level of protection against threats while ensuring effectiveness and efficiency of the IT environment	X	
Provide advice in terms of the capabilities of the Firewall(s) and Proxies solution(s) where required	X	
Respond to all requests and perform the necessary tasks to ensure that the environment is not vulnerable	X	
Manage the opening and closing of ports for specific services per DWS approved processes	X	
Provide security impact assessment of opening and closing of ports	X	
Map and maintain the perimeter policy as defined by DWS to the firewall(s) and proxies according to the approved DWS processes	X	
Perform maintenance of users and user groups accessing the Internet	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	
Monitoring Firewall(s) and Proxy Roles and Responsibilities		
Define monitoring requirements and standard for firewall(s) and proxies		X
Develop and document the procedures for the monitoring	X	
Review and approve monitoring procedures		X

Provide proactive and scheduled monitoring of the firewall(s) and proxies (e.g., hardware, middleware, network, interfaces, versions of software and/or devices (solution(s)) (major and minor upgrades), respond to messages and take corrective action as required	X	
Develop and maintain standard automated scripts to perform monitoring of firewall(s) and proxies solution(s)	X	
Proactively, troubleshoot, repair and report incidents/problems relating to perimeter security (solution).	X	
Respond to alerts generated by the firewall(s) and proxies according to industry best practices and as per the SLR	X	
Perform 24/7/365 monitoring and management	X	
Provide weekly and monthly reporting on Perimeter Security as set out in the SLR	X	

1.5. Logical Access Control Management

Logical Access Control Management Services are the activities associated with the day-to-day management of the Logical Access Controls in the environment for providing a secure environment and effectively and efficiently performing procedures to ensure services meet SLR targets and requirements. The Logical Access Control Management Services includes tools and protocols for identification, authentication, authorization and accountability in information systems. The following table identifies the Logical Access Control Management roles and responsibilities that the provider and DWS will perform.

Logical Access Control Management Roles and Responsibilities	Provider	DWS
Define requirements and standard for logical access control		X
Develop and document the procedures document for managing the logical access control that meet requirements and adhere to defined policies and standards	X	
Review and approve the logical access control procedures		X
Provide proactive and scheduled management of the logical access control mechanisms and respond to alerts/messages and take corrective action as required	X	
Develop and maintain standard automated scripts to perform management of the logical access control	X	
Provide advice in terms of the capabilities of the Logical Access Control solution(s) where required	X	
Respond to all requests and perform the necessary tasks to ensure that the environment is not vulnerable	X	
Perform maintenance of users in terms of logical access control as per DWS processes	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	
Monitoring Logical Access Control Roles and Responsibilities		
Define monitoring requirements and standard for logical access control		X

Develop and document the procedures document for the monitoring procedures that meet requirements and adhere to defined policies and standards	X	
Review and approve monitoring procedures		X
Provide proactive and scheduled monitoring of the logical access control solution(s) and respond to messages and take corrective action as required	X	
Develop and maintain standard automated scripts to perform monitoring of logical access control	X	
Proactively troubleshoot, repair and report incidents in the logical access control solution(s) environment	X	
Provide preventative measures for proactive monitoring and self-healing capabilities to limit risks to the environment that will impact service delivery	X	
Perform weekly checks to ensure that only active users are registered in the various logical access control solution(s) (e.g. AD)	X	
Perform monthly user administration audits and report on findings	X	
Perform quarterly password vulnerability checks and report on findings	X	
Perform monthly checks to ensure that privileged accounts and report on findings	X	
Provide monthly reporting on Logical Access Control as set out in the SLR	X	

1.6. Patch Management Services

Patch Management Services are the activities associated with the day-to-day management of the Patch Management in the EUC and server environment for providing a secure environment and effectively and efficiently performing procedures to ensure services meet SLR targets and requirements. The following table identifies the Patch Management roles and responsibilities that the provider and DWS will perform.

Patch Management Roles and Responsibilities	Provider	DWS
Define requirements and standard for patch management		X
Develop and document the procedures document for managing the patches that meet requirements and adhere to defined policies and standards	X	
Review and approve the patch management procedures		X
Ensure that the patch management solution(s) are backed up (e.g. configurations, etc)	X	
Provide proactive and scheduled management of the patch management solution(s) (e.g., hardware, middleware, network, interfaces, versions of software and/or solution(s) (major and minor upgrades), respond to messages and take corrective action as required	X	
Ensure that the latest licenses of the solution(s) are available		X

Patch Management Roles and Responsibilities	Provider	DWS
Maintain the version of the solution(s) to ensure the latest approved version is installed including middleware where required	X	
Develop and maintain standard automated scripts to perform management of the solution(s)	X	
Analyse patches published before being tested	X	
Provide patch release notifications as received from the manufacturers	X	
Establish the vulnerability within the managed environment (workstation or server). Review and select from all published updates		X
Ensure that patches are tested and deployed in a controlled manner in conjunction with the responsible parties in the various environments which will include servers and workstations	X	
Ensure that notifications for hotfixes are circulated to all relevant parties immediately for discussions	X	
Ensure that hotfixes are tested and installed as per the SLR	X	
Ensure that the service packs are tested and installed as per the SLR	X	
Ensure that the Patch Management Solution(s) are used to its fullest capability and in relation to the environment in terms of network, etc.	X	
Provide advice in terms of the capabilities of the Patch Management Solution(s) where required	X	
Respond to all requests and perform the necessary tasks to ensure that the environment is not vulnerable	X	
Ensure that the logs for the operating system(s) as well as the solution(s) is stored securely and being backed up	X	
Provide detailed analysis of the patch management solution(s) logs	X	
Respond and provide information for audit purposes	X	
Provide input into the relevant policy, standard, etc documents when required	X	
Ensure that patches that cannot be deployed using a tool are deployed manually	X	
Ensure remediation of audit findings and vulnerability assessments and any other findings that might be received	X	
Ensure exceptions are document and provided for approval should such a requirement exist	X	
Monitoring Patch Management Roles and Responsibilities		
Define monitoring requirements and standard for patch management		X
Develop and document the procedures document for monitoring that meet requirements and adhere to defined policies and standards	X	
Review and approve monitoring procedures		X
Provide proactive and scheduled monitoring of the patch management solution(s) (e.g., hardware, middleware, network, interfaces, versions of solution(s) (major and minor upgrades), respond to messages and take corrective action as required	X	

Patch Management Roles and Responsibilities	Provider	DWS
Develop and maintain standard automated scripts to perform monitoring of the patch management solution(s)	X	
Identify and report problems including hardware, system, file, disk and solution(s)problems proactively	X	
Provide troubleshooting, repair and escalation of problems in the patch management solution(s) environment	X	
Provide preventative measures for proactive monitoring and self-healing capabilities to limit risks to the environment that will impact service delivery	X	
Identify and report solution(s)problems	X	
Resolve or assist in resolving solution(s) problems in accordance with SLRs and escalate as required	X	
Respond to alerts generated by the patch management solution(s) according to industry best practices and as per the SLR	X	
Provide monthly reports on the details around patch management as set out in the SLR.	X	

1.7. Data backup and disaster recovery

Data backup and disaster recovery are the activities associated with the day-to-day management of the data- backups, restores, archiving, and disaster recovery in the environment to ensure an environment that will be able to recover data from backups as and when required and to ensure this service meet SLR targets and requirements. This service will also include media management. The following table identifies the Data backup and disaster recovery roles and responsibilities that will be performed.

Data backup and disaster recovery Roles and Responsibilities	Provider	DWS
Define strategies, requirements and standard for backup and restore management		X
Provide input and recommendations on best practices into strategies, services, specifications and standards for supporting the data storage and backup environment to reduce total cost of ownership	X	
Develop and document the procedures document for managing the backups and restores that meet requirements and adhere to defined policies and standards	X	
Review and approve the backup- as well as restore procedures		X
Ensure that the backup solution(s) are backed up (e.g. configurations, etc)	X	
Ensure proper configuration management and reporting thereof	X	
Provide proactive and scheduled management of the backup and restore solution(s) (e.g., hardware, middleware, network, interfaces, versions of software and/or solution(s) (major and minor upgrades), respond to messages and take corrective action as required	X	

Data backup and disaster recovery Roles and Responsibilities	Provider	DWS
Maintain the version of the solution(s) to ensure the latest approved version is installed including middleware where required	X	
Develop and maintain standard automated scripts to perform backups of the solution(s)	X	
Ensure that backup integrity is tested through regular test **restores**	X	
Respond to all requests and perform the necessary tasks to ensure that the environment is not vulnerable, e.g. restores, etc.	X	
Ensure that the logs for the operating system(s) as well as the solution(s) is stored securely and being backed up	X	
Provide detailed analysis of the backup solution(s) logs	X	
Respond and provide information for audit purposes		
Provide input into the relevant strategy, policy, standard, process etc documents when required	X	
Ensure remediation of audit findings and vulnerability assessments and any other findings that might be received	X	
Setting up and testing of backup schedules and procedures as per the backup strategy and/or standard	X	
Ensure that backup schedules are communicated and agreed upon as per the request from the data owners	X	
Ensuring that backups are performed within the timeframe (window) provided	X	
Testing the recovery procedures as approved	X	
Daily, weekly and monthly reports on backups	X	
Monthly report on restores testing and/or performed	X	
Performing restores from backups as and when required	X	
Ensure the process to add and/or remove backup requirements are followed	X	
Management of backup tapes (ensure that the amount of tapes available and request tapes to be ordered according to the standard) (for all sites). This will also include cleaning tapes.	X	
Manageme and maintain backup tape management and inventory system as per DWS procedure	X	
Management of backup tapes in terms of mounting and dismounting of tapes	X	
Manage the media that is stored off-site as well as the recovery of the tapes from the off-site storage site	X	
Maintain the integrity of the media libraries	X	
Ensure remediation of audit findings and vulnerability assessments and any other findings that might be received	X	
Disaster recovery		
Define monitoring requirements for disaster recovery		X
Develop and document the recovery procedures and adhere to defined RTOs and RPOs	X	

Data backup and disaster recovery Roles and Responsibilities	Provider	DWS
Review IT DRP	X	X
Review and approve recovery procedures		X
Planning and coordination of DR tests	X	X
Identify and report potential recovery problems including hardware, system, file, disk, processes and solution(s)problems proactively	X	
Perform DR test and reports as per set timeframes	X	
Reporting on outcome of DR tests performed	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	

1.8. Security Awareness and Training

Security Awareness and Training Services are the activities associated with the awareness and training of security to all officials in the Department. The Provider must perform awareness and training to ensure services meet SLR targets and requirements. The following table identifies the Security Awareness and Training Services roles and responsibilities that the provider and DWS will perform.

Security Awareness and Training Roles and Responsibilities	Provider	DWS
Define requirements and standard for security awareness and training		X
Review and approve the logical access control procedures		X
Provide proactive and scheduled security awareness and training material	X	
Perform electronic security awareness and training using relevant tools	X	
Ensure remediation of audit findings and assessments and any other findings that might be received	X	
Monitoring Security Awareness and Training Roles and Responsibilities		
Define monitoring requirements and standard for logical access control		X
Develop and document the procedures document for the monitoring procedures that meet requirements and adhere to defined policies and standards	X	
Review and approve monitoring procedures		X

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

Enquiries: Mr LCS Manqele
Telephone: 012-336 8394
Reference: 4/8/3/1/4

DIRECTOR-GENERAL
CHAIRPERSON: DEPARTMENTAL BID ADJUDICATION COMMITTEE

REQUEST FOR APPROVAL FOR THE PROCUREMENT OF THE INFORMATION TECHNOLOGY OUTSOURCE SERVICES FOR THE DEPARTMENT OF WATER AND SANITATION (DWS) THROUGH THE STATE INFORMATION TECHNOLOGY AGENCY (SITA) FOR A PERIOD OF THREE YEARS

1. PURPOSE

1.1. To obtain Director-General's approval for the procurement of the Information Technology Outsource Services for the Department of Water and Sanitation through the State Information Technology Agency (SITA) for a period of three years.

1.2. To request the Director-General's signature on the attached Terms of Reference marked as **Annexure "A"**, should the Director-General agree with the content.

2. BACKGROUND AND DISCUSSION

2.1 The current IT outsourcing contract between EOH Mthombo (PTY) LTD and the department is coming to an end on the 31 March 2023. The contract is for the provisioning and management of IT services (i.e. End-User Support, Server Support service and Application development and maintenance to the department).

2.2 The 31st March 2023 deadline for the current contract requires that the Department undergo a process to appoint a new service provider through SITA in order to acquire a new contract.

2.3 In terms of the SITA Act 1998 and General Regulations under section 10, state that all Government Departments are prohibited to invite the bids for ICT goods and/or services that are the subject of SITA transversal contract. It is further state that an institution which resolved to procure such goods and/or services through SITA, may procure such goods and/or services only from the relevant supplier (s) under that contract (see attached as **Annexure "B"**). However, the instruction from the Chief Financial Officer, supported by Director-General, is that the request to appoint be done through an open tender process through SITA, and not via the transversal contract 1183.

2.3 The appointed Bid Specification Committee met on 31st of May 2021 to review the Terms of Reference. The committee recommended the reviewed Terms of Reference to Departmental Bid Adjudication Committee and to the Acting Director-General for approval (see appointed BSC member as **Annexure "C"**)

2.4 Part of the document is the Statement of Work (SOW) which defines the roles and responsibilities between DWS and the new contractor/incumbent (see SOW as **Annexure "D"**). The SOW will be part of scope when sourcing the IT Outsource Services through Supply Chain Management who must ensure compliance of the terms of reference with respect to the SCM related matters in the terms of reference.

2.5 The services that will form part of the tender are:
- 2.6.1 LAN and Desktop Support Services
- 2.6.2 Data Centre Support Services
- 2.6.3 Business Application development and maintenance
- 2.6.4 Enterprise Architecture Services
- 2.6.5 Information Security Services
- 2.6.6 Project Management Office Services

3. FINANCIAL IMPLICATIONS

3.1 The total cost for outsourcing the listed services for a period of three years is expected to be approximately R290 000 000-00 (VAT included) for the duration of the contract. The funds for this contract are shared between the following components:

- Water Services
- Water Resources Information Management
- Planning and Information
- Macro Planning
- Regulation
- Information Services

3.2 Regulatory Compliance

3.2.1 This request for the procurement is in terms of SITA Act 1998 and General Regulation as outlined in paragraph 2.3.

4. OTHER COMPONENT(S) CONSULTED

4.1 All DWS business portfolio units are affected by the IT contract were notified of this intention trough the Portfolio Managers Committee. Funds are available on the budgets of the different business units within DWS.

5. RECOMMENDATIONS

It is recommended that the Director-General:

5.1 Approves the procurement of the Information Technology Outsource Services for the Department of Water and Sanitation through the State Information Technology Agency (SITA) for a period of three years.

5.2 Signs the Terms of Reference attached as **Annexure "A"**.

DIRECTOR: IT OPERATIONS AND INFRASTRUCTURE
NAME: MR LUCKY CS MANQELE
DATE: 2022/07/05

5. RECOMMENDATIONS

It is recommended that the Director-General:

5.1 Approves the procurement of the Information Technology Outsource Services for the Department of Water and Sanitation through the State Information Technology Agency (SITA) for a period of three years.

5.2 Signs the Terms of Reference attached as **Annexure "A"**.

RECOMMENDATION IN SUB-PAR 5.1: SUPPORTED / ~~NOT SUPPORTED~~ XXXXXXXXXXXX
RECOMMENDATION IN SUB-PAR 5.2: SUPPORTED / ~~NOT SUPPORTED~~

CHIEF INFORMATION OFFICER
NAME: MR ARTHUR KEKANA
DATE: 5 July 2022

RECOMMENDATION IN SUB-PAR 5.1: SUPPORTED / ~~NOT SUPPORTED~~
RECOMMENDATION IN SUB-PAR 5.2: SUPPORTED / ~~NOT SUPPORTED~~

CHIEF DIRECTOR: LEGAL SERVICES(Acting)
NAME: ~~**MR MPHO RATSHISUSU**~~ M Khuduga
DATE: 06/07/2022

RECOMMENDATION IN SUB-PAR 5.1: SUPPORTED / ~~NOT SUPPORTED~~
RECOMMENDATION IN SUB-PAR 5.2: SUPPORTED / ~~NOT SUPPORTED~~

DEPUTY DIRECTOR-GENERAL: CORPORATE SERVICES
NAME: ONV FUNDAKUBI
DATE: 2022/07/06

RECOMMENDATION IN SUB-PAR 5.1: SUPPORTED / ~~NOT SUPPORTED~~
RECOMMENDATION IN SUB-PAR 5.2: SUPPORTED / ~~NOT SUPPORTED~~

CHIEF DIRECTOR: RISK MANAGEMENT
NAME:MR MANDLA MALINDISA
DATE: 2022/07/06

5. RECOMMENDATIONS

It is recommended that the Director-General:

5.1 Approves the procurement of the Information Technology Outsource Services for the Department of Water and Sanitation through the State Information Technology Agency (SITA) for a period of three years.

5.2 Signs the Terms of Reference attached as **Annexure "A"**.

RECOMMENDATION IN SUB-PAR 5.1: ~~FINDS~~ FUNDS AVAILABLE / ~~NOT AVAILABLE~~

CHIEF FINANCIAL OFFICER
NAME: MR FRANS MOATSHE
DATE: 2022/08/18

RECOMMENDATION IN SUB-PAR 5.1: RECOMMENDED / ~~NOT RECOMMENDED~~
RECOMMENDATION IN SUB-PAR 5.2: RECOMMENDED / ~~NOT RECOMMENDED~~

CHAIRPERSON: BID SPECIFICATION COMMITTEE
NAME: MR CONRAD GREVE
DATE: 2022/8/18

RECOMMENDATION IN SUB-PAR 5.1: RECOMMENDED / ~~NOT RECOMMENDED~~
RECOMMENDATION IN SUB-PAR 5.2: RECOMMENDED / ~~NOT RECOMMENDED~~

CHAIRPERSON: DEPARTMENTAL BID ADJUDICATION COMMITTEE
NAME: SD NDHLOVU
DATE: 05/09/2022

RECOMMENDATION IN SUB-PAR 5.1: APPROVED/ ~~NOT APPR~~OVED
RECOMMENDATION IN SUB-PAR 5.2: APPROVED/ ~~NOT APPR~~OVED

DIRECTOR-GENERAL
NAME: DR SEAN PHILLIPS
DATE: 07/09/22

For Supply Chain Management:

Contact Person: Ms Nokubonga Mkhize

Tel: (012) 336 7571

Email: MkhizeN6@dws.gov.za

9. TERMS OF REFERENCE APPROVAL

APPROVED/ ~~NOT APPROVED~~

NAME: DR S PHILLIPS

DIRECTOR-GENERAL

DATE: 07/09/22

CONFIDENTIAL

Annexure B

Proposal for Information Security Services for the Department of Water and Sanitation, by the State Information Technology Agency SOC Ltd

Document No:	1107 INC24157236
Revision:	1.0
Author	Kinny Mcaba
Effective Date:	On Date of Signature
Electronic File:	1107 INC24157236

Notice

Copyright © 2023, SITA SOC Ltd (Registration No: 1999/001899/30). All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without the express written permission of SITA SOC Ltd.

Document enquiries can be directed to:
Records Management Office
SITA SOC Ltd
PO Box 26100, Monument Park, 0105, South Africa
Tel: +27 12 482 3000
www.sita.co.za

Attention: Unathi.Thoka@sita.co.za
Telephone: +27 12 482 2238
Cell phone: +27 74 605 0473

Approval

The signatories hereof, being duly authorised thereto, by their signatures, hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

Sandra Herbst
Acting Head of Department: Products, Services and Solutions
SITA

12 June 2023
Date

Accepted On behalf of Department of Water and Sanitation and duly authorised thereto

Date

Foreword

This document contains information regarding SITA's security operation centre service offering to the Department of Water and Sanitation herein referred as DWS. It does not form part of any other document, nor does it replace or supersede any other document.

The document is applicable to the management of DWS who shall be required to, should they elect for SITA to continue with the project, sign their approval of this document and place a formal order on SITA who shall be responsible for executing the project.

The document has been drafted according to the conventions as stipulated in the formal SITA document layout, writing and typing standard.

References

1. SITA Amendment Act (Act number 38 of 2002).
2. Procurement Regulations for SITA and Government.
3. Request for Information Technology Outsourcing Services of a period of 3 years.
4. Service Requirement Specification for Security Operation Centre, SRS_SOC_v1.

Non-disclosure of information

(1) On receipt of a SITA proposal the DWS undertakes to:

(a) Keep confidential all information (written, including information contained in electronic format, or oral) concerning the business and affairs of SITA that it shall have obtained or received from SITA through the relevant document/agreement.

(b) Not disclose nor change the information in whole or in part to any other person save its employees involved in the implementation of this agreement, and who have a need to know the same without SITA's written consent.

(c) Use this information solely in connection with the implementation of this agreement/document and not for its own benefit or that of any third party.

(2) The provisions of paragraph 1 above shall not apply to the whole or any part information to the extent that it is:

(a) Already known to the recipient without obligation of confidence.

(b) Independently developed by the recipient.

(c) Publicly available without breach of this agreement.

(d) Rightfully received from a third party.

(e) Released for disclosure by the disclosing party with its written consent.

(f) Required to be disclosed in response to a valid order of court or other governmental agency or if disclosure is otherwise required by law.

Contents

Figures

Tables

Area	Business challenge	Value Statement
Service delivery	(a) Inadequate security controls to protect sensitive data. (b) Lack of specialised security skills and capacity. (c) Risk of compromised data integrity. (d) Loss of service provision due to unavailability of systems. (e) Loss of proprietary and confidential information, as a result of security breaches and incidents.	(a) Improve the quality of government services delivered to the public by ensuring that the business can rely on the confidentiality and integrity of the information stored on its databases. (b) Improve government security through leveraging security expertise from the SITA SOC.
Risk management, compliance and auditability	(a) Audit findings on inadequate security posture protection. (b) Legal and regulatory penalties as a result of non-compliance. (c) Audit findings on inadequate security posture protection.	(a) Maintain consistent compliance against international best practices, standards and security frameworks. (b) Enable the business to reduce risk of legal and regulatory penalties due to non-compliance.

3. Scope of work

A once off high-level breakdown of the services are as follows:

1. Managed Security Operation Centre services:
   - (a) Planning (Environment Preparation Assessment):
     - (i) Assess DWS ICT environment against SOC service requirement.
   - (b) SOC Solution Design:
     - (i) Analysis of business service requirements.
     - (ii) Security solution design and architecture.
   - (c) SOC Solution Implementation:
     - (i) Customise SOC infrastructure to meet DWS's requirements.
     - (ii) Deployment of data collectors.
     - (iii) Deployment of SOC Components (service correlation engine).
     - (iv) Customisation of SOC dashboards.
     - (v) Solution integration (such as Service Desk).
     - (vi) Initial testing of the SOC Plan.
   - (d) Conduct annual Penetration Test for a large size environment:
     - (i) Penetration testing planning and preparation.
     - (ii) Penetration testing.
     - (iii) Penetration test report with identified vulnerabilities and recommendations.
     - (iv) Presentation of results.
   - (e) Managed SOC (Service Level Agreement (SLA):

     Managed Detection and Response services offer turnkey threat monitoring, detection and response via SITA's remotely delivered, 24/7/365 security operations centre (SOC) capabilities and technologies to rapidly detect, analyse, investigate and actively respond to threats (e.g., containment or disruption). DWS has to note that the logs will be kept for a period of 12 months. High-level SOC breakdown services, which will be included in an SLA once activation is implemented will be detailed as follows:
     - (i) Security Event Monitoring and Threat Detection.
     - (ii) Remote Security Device Monitoring and Management (Data Collectors).
     - (iii) Vulnerability / Playbook Analysis.
     - (iv) Change - Move, Add, Change, or Delete (MACD) – Prioritisation.

(v) Incident and Request Management: Monitoring and escalation.
(vi) Security Dashboard / Portal and the portal that provide same visibility as the SOC has to the DWS security management.
(vii) Perform Threat Hunting (manual and machine assisted methods).
(viii) DWS define SOC Alert Triage process with the inputs of SITA.
(ix) DWS define Emergency incident response with the inputs of SITA
(x) DWS define SOC incident response plan with the inputs of SITA.
(xi) Research and development to implement countermeasures against cyber threats.
(xii) Ensure remediation of audit findings and assessments and any other findings that might be received.
(xiii) Provide practical recommendations for remediation and prevention of threats and other related matters.
(xiv) The below table are SOC consulting services which a quotation may be required. The services are based on **time and material** costing:

Table 2: Consulting Services:

Description	Costing method
Emergency security investigations.	Time-and-material
Perform digital forensic investigation.	

4. Exclusions

Table 3: Exclusions

Exclusion	Reason
1. Monitoring of systems and components not included in the scope of the approved Technical Solution Design (TSD).	The solution only covers the identified in-scope ICT environment for systems and servers and security agent deployment as defined in the proposed solution design/ approved TSD. Future additions to be managed through the formal SITA proposal, change management and/or request fulfilment processes.
2. This proposal does not include the acquisition of any infrastructure from SOC services.	Minimum required infrastructure (a) 1 Petabyte of storage. (b) 4 VM's.
3. Security Policy development.	The development of DWS security strategies, policies, planning and processes are excluded from this proposal. SITA can assist the Department by providing inputs into the documents, should the Department so require. The service can be addressed as an additional project.
4. Resolution of security incidents prior service activation.	SITA will not be held responsible for, or to manage, any security incidents that occurred prior SITA managed SOC service activation.
5. Post-Remediation Plan.	(a) Implementation of remediation recommendations and remediation will be remediated by EUC as per SLA with DWS.
6. IT Service Desk	Service Desk to be outlined and costed in the existing SLA (Annex N to SLA_1107_001: Service Management Service)

4.1 Assumptions

(a) The assumption is that, during the development of the security services design, the existing and future security landscape were considered, or that at least certain security measures were implemented.

(b) DWS will provide adequate infrastructure to implement the security products such as firewalls (see exclusions).

(c) The following are assumptions made concerning the implementation/take-on approach:

i) The project shall be a formal project, sponsored by top management, to ensure quality participation of all stakeholders.

ii) Access to and availability of identified representatives, according to the agreed schedule.

iii) Access to and availability of the required systems and information.

(d) Penetration test cost will be done annually and is based on a large environment size with more than 10 applications/ solution, more than 10 000 users, more than 5 sites and more than 200 servers.

4.2 Constraints/ Critical success factors

The following constraints have been identified:

(a) Availability of the architectures and/or design documentation that define the solutions in operation.

(b) Adequate storage capacity for SITA to accommodate the security logs that must be kept for a period of 12 months.

4.3 Dependencies

The following dependencies have been identified.

Table 4: Dependencies

No.	Category	Description	Impact Description	Mitigation	Responsible Party	Mitigation Owner
1.	Governance	Proper management and control.	No control in the event of a disaster, data loss or service interruption.	Ensure approved governance mechanisms are implemented.	DWS	DWS
2.	Network connectivity	Inter-VPN and network connectivity between the DWS site and the GPCE site. Internet gateway configuration	No access to servers and endpoints included in TDS.	Network connectivity to be addressed as part of solution design.	SITA is responsible for managing network connectivity to the SITA network.	DWS
3.	Bandwidth capacity	Last mile bandwidth must be sufficient to ensure acceptable levels of bandwidth utilisation and latency.	Insufficient bandwidth will impede response times.	Ensure sufficient bandwidth capacity.	SITA to report on network utilisation for DWS.	DWS
4.	DWS's ICT services support team	Configuration of ICT equipment for identified end	Incorrect ICT equipment configurations will affect the	Ensure ICT support team participation	EUC	DWS

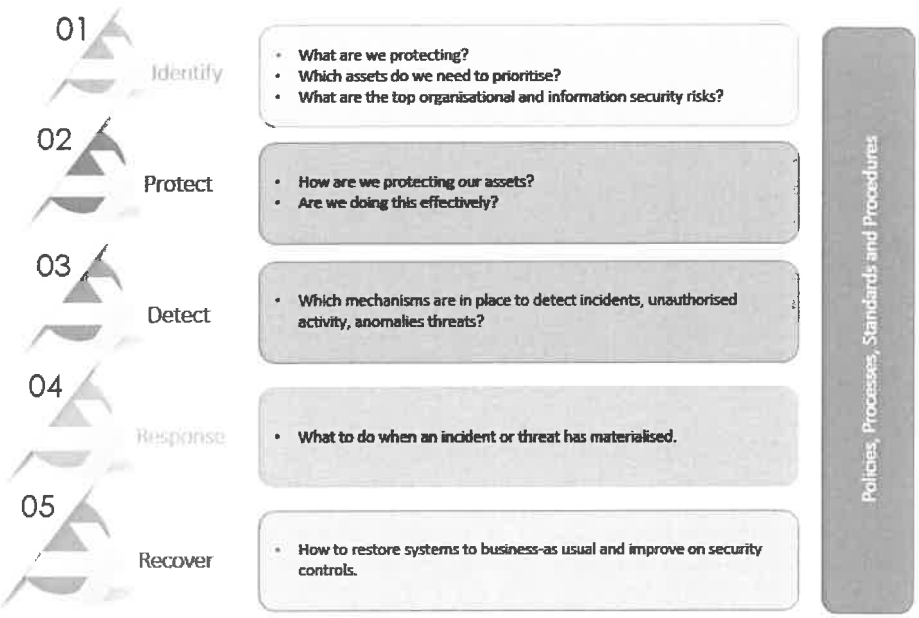

Figure 1: Five core functions of the SOC

The SITA SOC follows a structured security event and incident management process that comply with principles defined in the Information Security Forum, Standard of Good Practice. A high-level overview of the process and functionalities are described as follows:

5.1.1 Detect

SITA uses a tested detection framework paired with research and investigations capabilities to foster fast triage of alerts, applying contextual observation, threat intelligence, and observed kill chain behavior. These capabilities include the following:

(a) Monitoring and providing escalated security incident alerting systems for known and emerging attacks.
(b) Intelligence to help detect and predict threats.
(c) Adaptive defenses to detect non-standard attacks.
(d) Detecting suspicious and anomalous activities using cloud native security analytics.
(e) Using early detection to support accelerating security operations to stop, prevent or contain the threat or attack.

5.1.2 Analyse

(a) Tracking and analysis of tagged suspicious files on endpoints, as they traverse the network, and across email and web content.
(b) Monitoring for indicators of compromise on internal networks and cloud assets.
(c) SITA uses analysts and automation to investigate certain categories of anomalous events and traffic where there isn't a known cause and may pose a material threat.

5.1.3 Investigate

(a) SITA will Investigate threats on endpoints, user behaviours', applications, and the network elements protected by the SOC components.
(b) SITA uses threat intelligence to research indicators of compromise (IOCs) and attack (IOAs) to confirm threats, attacks, compromises or exploitation.

(c) SITA uses investigation methodology to add context from integrated security products and help identify impact, severity and scope of security Incident to the endpoint.

(d) Investigate the security Incident for impact and attacker attributes.

5.1.4 Respond

(a) Where applicable, perform changes to the SOC components defined within the SOC Response Plan with the intent to prevent, mitigate or stop malicious activity.

(b) Create and modify the detection and response playbooks based on new information and threats from security events detected from the SOC components and processes described above.

(c) Provide general (see below for details) guidance on how to mitigate, stop, or prevent a Security Incident based on the intelligence and advisories provided above, as relevant to DWS's environment.

5.2 SOC Planning and Design

SITA and DWS will work together to provide details on the SOC service scope, and to define the plan for establishing connectivity between the SITA SOC and the SOC components to be deployed in the DWS environment. Planning deliverables include:

(a) **Environment Preparation Assessment** – Planning to gather and confirm the business requirements and details of the scope of the services. The purpose of the assessment is to:
   i) Define the SOC service scope and components.
   ii) Cover all access points, critical systems, and segmentation methodologies.
   iii) Confirm which security controls are in place.
   iv) Develop and authorise the Service Requirement Specifications.

(b) **Solution Design** – The Technical Solution Design (TSD) document will include compute specifications, storage requirements, network connectivity and security requirements. Deliverables are:
   i) Security solution design.
   ii) Network connectivity design.
   iii) Technical solution design.

(c) **Review of the Information Security Incident Response Plan** – SITA will ensure that the SITA/DWS Incident Response Plan meet the DWS's requirements. The ISIR-Plan is a key deliverable to enable DWS to recover from information security incidents and safeguard Government data in the event of an attack.

5.3 Managed Security Operation Centre Components

The framework for enabling, installing, configuring and maintaining the SOC components (using SITA configuration guides) to allow for Service Activation by the requested Service Activation date and ongoing performance of the Services.

The SOC service will only be deployed and activated for the SOC components (or its covered endpoints) as specified in the approved Technical Solution Design.

The successful delivery of the service depends on the DWS cooperation and assistance to SITA (e.g., making changes to SOC Components that cannot be done remotely, locally running tests, or diagnostics on SOC Components, enabling or updating APIs or configurations, etc.).

5.4 SOC Component Deployment and Activation

SITA will connect the SOC components, with the assistance of the DWS's technical team, via APIs to the SITA SOC. SITA will perform tests to confirm that the SOC components meet technical readiness requirements and activate the SOC components onto the SOC Platform (SOCP).

SITA Deployment activities include:

(a) Deployment of identified in-scope SOC components.
(b) Customisation of SOC infrastructure.
(c) Configuration of the SOC Platform.
(d) Customisation of dashboards.
(e) Vulnerability pre-scanning of the DWS in-scope environment at the time of implementation.
(f) Testing and quality assurance.
(g) Initial testing of SITA SOC Incident Response Plan.
(a) Configuration of APIs and SOC components on DWS devices and infrastructure.
(b) Unless SITA is performing installation services at the DWS site, the DWS is responsible to perform any required hardware or software installations, configuration changes and other activities as may be required to enable connectivity and communication between the SOC Components and SOCP.

SITA Deliverables are:

(a) User acceptance testing report to confirm service deployment and activation.
(b) SITA SOC IR test report.

6. ISIR-Plan

The SITA will manage the DWS 's security incidents based on the SITA default Information Security Incident Response Plan (ISIR-Plan).

or

SITA will develop an ISIR Plan in collaboration with DWS to meet the business requirements for RPO and RTO.

The Information Security Incident Response Plan (ISIR Plan) ensures that:

(a) All information security incidents (including information security) are managed quickly and efficiently.
(b) A consistent approach is implemented to manage information security incidents.
(c) The damage caused by an information security incident is minimised.
(d) The likelihood of recurrence of the information security incident is reduced by the review and implementation of appropriate measures.

6.1 ISIR-Plan Testing

(a) Testing of the ISIR-Plan will ensure that the DWS can recover data, restore business critical applications and continue operations after a service interruption, critical IT failure or complete disruption.
(b) Two ISIR-Plan tests per annum for 2 SOC components only will be provided.
(c) SITA will schedule the tests.
(d) There will be additional charges for any additional SOC components to be tested.

6.2 ISIR-Plan Activation

The ISIR-Plan may only be invoked by the SITA ISIR ISS HOD or the SITA Executive Service Management.

6.3 Recovery objectives

The DWS's information security incident response recovery point objectives (RPO) and the recovery time objectives (RTO) are documented in the SOC incident response plan.

7. Operations and Support

Once the SOC components were successfully deployed and the service is activated, SITA provide the following services, which will be based on a Service Level Agreement (SLA):

7.1 Service Delivery Management

The SOC service delivery management will be executed based on ITIL principles and practices, and include:

(a) **Service Desk:** SITA will provide a 24/7 SITA Service Desk for DWS to report all service related incidents.
(b) **Incident Management:** SITA will manage all service incidents, including service interruptions, or reduction in the quality of service.
(c) **User Service Request Management:** Support to fulfil user service requests. This includes requests for access to a service, request for information etc.
(d) **Service Delivery Manager:** Service delivery management services by a Security Delivery Manager. SITA will conduct monthly service meetings to discuss security incident and related information.
(e) **Change enablement:** Management of IT changes to ensure that risks have been properly measured, changes are authorised and managed according to a change schedule.

7.2 Security Monitoring

(a) SITA will centrally monitor security alerts from the SOC components 24/7/365 for potential Security Incidents.
(b) Alerts will be correlated against configured use cases, Threat Intelligence and available third-party threat intelligence using analytics, SIEM and security orchestration and automation response (SOAR) systems.

7.3 Security Incident Response

When a Security Incident has been found, SITA will recommend responses to help contain, mitigate, remediate, or eradicate the threat. SITA's SOC remote response actions are limited to actions defined within the SOC Incident Response Plan.

In the event of a security incident, SITA will:

(a) Recommend the appropriate response based on the nature of the Security Incident.
(b) Provide recommendations to resolve, mitigate or eradicate security incidents.
(c) Where the Security Incident is a known attack, recommend response to mitigate or stop attack.

SITA	DWS
4. Monitoring of events and alerts within DWS ICT environment for security threats and risks to determine the adequacy of security measures and identify security deficiencies. 5. Manage events and alerts based on incident response processes, automated cross-data correlation and alerting. 6. Provide guidance to DWS on mitigation control. 7. Design, setup and configure SITA approved security policies. 8. Notify SITA SOC customers of confirmed or "real" security incidents, and identified threats and risk. 9. Recommend response to mitigate risk or stop attack. In cases of cost implications, provide a quotation. 10. Provide a Security Dashboard / Portal for DWS to view and download reports. 11. SITA and any of its subcontractors will be subject to confidential vetting process. 12. SITA will be responsible for the analysis, evaluation and reporting to DWS SLA owner of a Security Breach, and to notify DWS SLA owner.	4. Assist SITA to install, configure and maintain the SOC Components (data collectors and correlation engine) in the DWS ICT environment. 5. Assist SITA in establishing and validating bidirectional management connectivity between the SOC Components and SOC Platform. 6. Authorise resolution actions (when applicable, or in case of cost implications). 7. Act on and implement SITA recommendations. 8. DWS remains responsible for backups of the DWS ICT environment and Disaster Recovery to protect its data against loss, damage, theft or destruction. 9. Provide SITA timely with remote (logical) access to the SOC Components. 10. Identify, together with SITA, the possible service limitations as a result of SOC Component type and configuration. 11. Management of the third parties currently providing maintenance and support in the DWS ICT environment. 12. DWS will be accountable to communicate the Security Breach internally and externally, and notify the governing body.

Detailed roles and responsibilities per service component will be described in and governed by the SITA/DWS SLA.

10. Critical success factors

In order for the SOC services to be rendered successfully the following are the required minimum critical success factors:

(a) Executive support
  i) Executive support of SOC services is the number one success factor, since executives are responsible for providing, among other things, funding, human resources, and political guidance. The availability of senior management further reflects this commitment.

(b) Support by other stakeholders
  i) SITA needs to work closely with all the stakeholders of the department in order to conduct a successful project. The commitment by all identified participants is critical.

(c) Access to required documentation
  i) Access to the documentation about ICT systems, policies, and business processes form a crucial initial step towards the achievement of the SOC services.

11. Financial Implications

11.1 Once-Off Pricing

Find below pricing for the once-off services to deliver the SOC Set-up.

11.2 Planning and Solution Design

Table 6: Planning and Solution Design

Description	Total
Client Environment assessment	R 52 450.80
TSD including Network and Security requirements	R 104 218.80
Infrastructure configuration	R 40 432.00
Data Collectors Deployment	R 34 739.60
SOC components deployment	R 104 218.80
SOC Dashboard configuration	R 104 218.80
Solution Integration	R 104 218.80
Quality Assurance	R 34 739.60
User Acceptance Testing	R 34 739.60
Event, alert and response planning	R 26 940.80
Initial SOC plan Testing	R 34 739.60
Professional services	R 26 940.80
Total (Excl. VAT	**R 702 598.00**
Plus 15% VAT	R 105 389.70
Total amount (Incl. VAT)	**R 807 987.70**

Table 7: Penetration test Charges

Description	Once Per Annum
Client Environment assessment requiring specialist skills and expertise	R 785 000.00
Total (Excl. VAT	**R 785 000.00**
Plus 15% VAT	R 117 750.00
Total amount (Incl. VAT)	**R 902 750.00**

11.3 Estimated Monthly Recurring

Table 8: Recurring charges –SOC Security Services

Description	Monthly Total
(a) Security Incident Event Monitoring (SIEM) i) Security Event Monitoring and Threat Detection. ii) Remote Security Device Monitoring and Management (Data Collectors). iii) Security Dashboard / Portal and the portal that provide same visibility as the SOC has to the DWS security management.	R 128 697.12
i) Vulnerability / Playbook Analysis, Change - Move, Add, Change, or Delete (MACD) – Prioritisation ii) Perform Threat Hunting (manual and machine assisted methods). iii) Define together with DWS SOC Alert Triage process. iv) Define together with DWS Emergency incident response. v) Define together with DWS SOC incident response plan. vi) Research and development to implement countermeasures against cyber threats Ensure remediation of audit findings and assessments and any other findings that might be received. vii) Provide practical recommendations for remediation and prevention of threats and other related matters.	R 251 466.00

12.2 Hours of service

The service will be provided from the SITA SOC 24/7/365.

12.3 Access to Sites

It is agreed that the Department of Water and Sanitation shall arrange unhindered access to the DWS's offices for the specified SITA representatives and that SITA representatives shall be given the required access to all applicable areas / systems/ equipment in order to perform their functions and duties as covered and agreed in this proposal.

12.4 Liaison

The department shall be responsible for communication among its stakeholders and end users to ensure the successful delivery of this service, unless in cases where SITA is required to communicate directly with the end user as part of service delivery in this proposal.

12.5 Confidentiality of the proposal

This document contains confidential information regarding technical as well as pricing mechanisms, and remains the property of SITA (SOC) Ltd. This document, in either copied or any other format, shall not be made available to any other party, without the written permission of SITA (SOC) Ltd.

12.6 Proposal Validity

The information contained in this document is valid for a period of **60 days** from the day that the DWS Client Relationship Manager has provided it to the DWS. The commencement date of the service implementation is dependent on the receipt of a Government Order from the Department.

12.7 Acceptance of the proposal

Following the aforementioned, the proposal is submitted for consideration. Once this proposal is approved, the project managers shall commence with the project initiation session leading to the establishment of the project charter and plan, that shall contain the detailed plan and timelines of the deliverables agreed to with the DWS, depending on the Government Order being issued. Furthermore, this shall be fixed price project that is milestone/deliverable driven and thus invoice shall be raised on approval of deliverables agreed with the DWS during the initiation phase.

SITA will formalise the operations, maintenance and support of the service(s) with the presentation of a Service Level Agreement (SLA) Annex for this service. The SLA Annex must be signed and a Government Order must be provided to SITA, before the service shall commence. The SLA Annex will be reviewed at regular intervals to ensure that the contract remains current in terms of the service requirements as reviewed from time to time at quality of service meetings.

Annex A: Abbreviations

BA	Business Agreement
CPI	Consumer Price Index
DWS	Department of Water and Sanitation
ICT	Information Communication Technology
IR	Incident Response
IS	Information Systems
ISIR	Information Security Incident Response
IT	Information Technology
MACD	Move, Delete, Change or Delete
PAIA	Promotion of Access to Information Act
POPIA	Protection of Personal Information Act
RPO	Recovery Point Objective
TI	Threat Intelligence
RTO	Recovery Time Objective
SIEM	Security Information and Event Management
SITA (SOC) Ltd	The State Information Technology Agency, State Owned Entity, Limited
SLA	Service Level Agreement
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre
SOCP	Security Operation Centre Platform
TSD	Technical Solution Design
UBA	User Behaviour Analytics
VAT	Value-added tax, as levied in accordance with the Value Added Tax Act, 1991 (Act No. 89 of 1991)

water & sanitation
Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

D

Tracking no

ROUTE FORM

BRANCH: CORPORATE SERVICES

Reference No.:

INFORMATION AND COMMUNICATION TECHNOLOGY DEMAND PLAN FOR 2023/2024 FINANCIAL YEAR

DRAFTING OFFICIAL		SUPERVISOR	
Name: M Hlungwani Extension:7746 Office No.: 240		Name: Arthur Kekana Extension: 8701 Office No.: SED 258	
Rank: ASD ICT Financial Management	Date: 23.02.2023	Rank: CIO	Date:23.02.2023

Rank	Date	Name and Surname	Signature	Office No
D: DD		Ms. Nomusa Hlalethwa		Zwa 429
CD:		Mr. Arthur Kekana (CIO)		Sed 258
D: SS				
DDG CS 2023/02/27		ONV Fundakubi		Sed
CFO*				
CD:LS*				
CD:SS [ODG]				
COO				

* In the case of financial/legal issues

INSTRUCTIONS/REMARKS TO AUTHOR BY DIRECTOR-GENERAL

water & sanitation
Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

Annexure 4

DEMAND PLANNING TEMPLATE(SCM 4)

(DMP 1.4 SUMMARY)

Summary

PART A: (CLIENT DETAILS)

Programme/Branch:	Corporate Services	**Programme Manager:**		ONV Fundakubi	**Signature:**
Chief Directorate:	Information & Comm Technology	**Responsibility Manager:**		Mr. Arthur Kekana	**Signature:**
Programme Number:	One (1)	**Budget Controller**		Ms. Nomusa Hlalethwa	**Signature:**
Directorate:	All	**Demand Cordinator**		Mr. Morena Hlungwani	**Signature:**
Province:	HEAD OFFICE	**Office #:**	240	**Telephone:**	012-336-7746
Period:	2023/24	**Fax:**		**Email Address:**	HlungwaniM@dws.gov.za

Estimated Budget Summary:

Assets	**Total Cost(Major)**	**Total Cost(Minor)**
Computer Hardware & Systems	150 000,00	0,00
Other Machinery & Equipment	8 811 000,00	36 000,00
Furniture & Fittings	0,00	14 000,00
Transport Assets	0,00	0,00
Computer Software & Other Intangibles	57 000 000,00	0,00
Buildings and other Fixed Structures	0,00	0,00
Total Assets	***65 961 000,00***	***50 000,00***

Goods & Services	**Total Cost**
Normal Services	82 751 000,00
Projects: Business & Advisory Services	0,00
Other	0,00
Total Services	***82 751 000,00***
Estimated Total Budget	***148 762 000,00***

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

Annexure 1
DEMAND PLANNING TEMPLATE (SCM 1)

(DMP 1.1 - CAPITAL ASSETS)

PART A: (CLIENT DETAILS)

Programme/Branch:	Corporate Services	Programme Manager:		ONV Fundakubi	Signature:	
Chief Directorate:	Information & Comm Technology	Responsibility Manager:		Mr. Arthur Kekana	Signature:	
Programme Number:	One (1)	Budget Controller		Ms. Nomusa Hlalethwa	Signature:	
Directorate:	ALL	Demand Cordinator		Mr. Morena Hlungwani	Signature:	
Province:	Head Office	Office #:	240	Telephone:	012-336-7746	
Period:	2023/2024	Fax:		Email Address:	HlungwaniM@dws.gov.za	

PART B (1): (RESOURCE & COSTS DETAILS) ASSETS

Resource Required						Motivation			Cost Estimate			
Item Description	Lead Time/ Delivery Date 1st Q	2nd Q	3rd Q	4th Q		Replacement Yes/No	Barcode/ Asset Number for replacement	Reason for Acquisition/ Motivation	Quantity	Unit Cost	Total Cost	METHOD OF PROCUREMENT
	A M J	J A S	O N D	J F M								
Computer Hardware & Systems:	x											
Laptop	x					NO		Daily connectivity	2	50 000,00	100 000,00	RFQ
Monitor	x					NO		Daily connectivity	1	5 000,00	5 000,00	RFQ
Printer	x							Printing of confidential documents	3	15 000,00	45 000,00	RFQ
Total											150 000,00	
Machinery & Other Equipment:												
Lan Equimpment, Switches, Routers and Wifi			x			NO			2	4 350 000,00	8 700 000,00	Transveral Contract
Leasing of Photocopying Machine & Phones	x	x	x	x	x	NO			12	8 000,00	96 000,00	Term Contract
Projector	x					ND			1	15 000,00	15 000,00	RFQ
											0,00	
Total											8 811 000,00	
Furniture & Fittings & Office Equipment:												
Shredder											0,00	
Heater											0,00	
Fan Pedestal/Desk											0,00	
Total											0,00	
Transport Assets:												
Boat											0,00	
Total											0,00	
Computer Sofware & Other Intangibles:												

Why 12 leasing of photocopying machines required?

Resource Required																Motivation			Cost Estimate			
Item Description	Lead Time/ Delivery Date															Replace-ment Yes/No	Barcode/ Asset Number for replacement	Reason for Acquisition/ Motivation	Quantity	Unit Cost	Total Cost	METHOD OF PROCUREMENT
	1st Q			2nd Q			3rd Q			4th Q												
	A	M	J	J	A	S	O	N	D	J	F	M										
Microsoft Enterprise Agreement including True Up																			1	46 000 000,00	46 000 000,00	Term Contract
Antivirus & Encryption																			1	2 500 000,00	2 500 000,00	BID
Net-Back Licenses																			1	2 500 000,00	2 500 000,00	BID
Security Strategy Implementation																			1	6 000 000,00	6 000 000,00	Transversal Contract
Total																					57 000 000,00	
Buildings & other Fixed Structures																						
																					0,00	
																					0,00	
Total																					0,00	

Summary:

Item Description	Total Cost
Computer Hardware & Systems	150 000,00
Other Machinery & Equipment	8 811 000,00
Furniture & Fittings	0,00
Transport Assets	0,00
Computer Software and Other Intangibles	57 000 000,00
Buildings and other Fixed Structures	0,00
Total Cost	~~65 961 000,00~~ 1

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

Annexure 2

DEMAND PLANNING TEMPLATE (SCM 2)

(DMP 1.2 - MINOR ASSETS)

PART A: (CLIENT DETAILS)

Programme/Branch:	Corporate Services	**Programme Manager:**	ONV Fundakubi	**Signature:**	
Chief Directorate:	Information & Comm Technology	**Responsibility Manager:**	Mr. Arthur Kekana	**Signature:**	
Programme Number:	One (1)	**Budget Controller**	Ms. Nomusa Hlalethwa	**Signature:**	
Directorate:	All	**Demand Cordinator**	Mr. Morena Hlungwani	**Signature:**	
Province:	Head Office	**Office #:** 240	**Telephone:**	012-336-7746	
Period:	2023/24	**Fax:**	**Email Address:**	HlungwaniM@dws.gov.za	

PART B (1): (RESOURCE & COSTS DETAILS) ASSETS

Resource Required											Motivation			Cost Estimate			
Item Description	Lead Time/ Delivery Date										Replace-ment Yes/No	Barcode/ Asset Number for replacement	Reason for Acquisition/ Motivation	Quantity	Unit Cost	Total Cost	METHOD OF PROCUREMENT
	1st Q			2nd Q			3rd Q			4th Q							
	A	M	J	J	A	S	O	N	D	J	F	M									
Computer Hardware & Systems:																	
Total																	
Machinery & Other Equipment:																	
Electric Kettle		x												1	1 000,00	1 000,00	RFQ
Refridgerator		x												1	5 000,00	5 000,00	RFQ
Microwave		x												1	5 000,00	5 000,00	RFQ
LAN Tools (Toner & normal kit)														2	5 000,00	10 000,00	RFQ
Computer Peripherals														3	5 000,00	15 000,00	RFQ

Resource Required											Motivation			Cost Estimate			
Item Description	Lead Time/ Delivery Date										Replace-ment Yes/No	Barcode/ Asset Number for replacement	Reason for Acquisition/ Motivation	Quantity	Unit Cost	Total Cost	METHOD OF PROCUREMENT
	1st Q			2nd Q			3rd Q			4th Q							
	A	M	J	J	A	S	O	N	D	J	F	M						
																0,00	
Total																36 000,00	
Furniture & Fittings & Office Equipment:																	
Shredder		x												1	5 000,00	5 000,00	RFQ
Heater		x												3	3 000,00	9 000,00	RFQ
Fan Pedestal/Desk																0,00	
Total																14 000,00	
Transport Assets:																	
Boat																0,00	
Vehicle																0,00	
Trailer																0,00	
Total																0,00	
Computer Sofware & Other Intangibles:																	

water & sanitation
Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

Annexure 3

ACQUISITION MANAGEMENT DEMAND PLANNING TEMPLATE (SCM 3)

(DMP 1.3 - GOODS & SERVICES)

PART A: (CLIENT DETAILS)

Programme/Branch:	Corporate Services	**Programme Manager:**	ONV Fundakubi	**Signature:**	
Chief Directorate:	Information & Comm Technology	**Responsibility Manager:**	Mr. Arthur Kekana	**Signature:**	
Programme Number:	One (1)	**Budget Controller**	Ms. Nomusa Hlolethwa	**Signature:**	
Directorate:	All	**Demand Cordinator**	Mr. Morena Hlungwani	**Signature:**	
Province:	Head Office	**Office #:** 240	**Telephone:**	012-336-7746	
Period:	2023/24	**Fax:**	**Email Address:**	HlungwaniM@dws.gov.za	

PART B: (RESOURCE & COSTS DETAILS) Goods & Services

Resource Required		Motivation		Cost Estimate			
Item Description	Lead Time/ Delivery Date (1st Q: A M J; 2nd Q: J A S; 3rd Q: O N D; 4th Q: J F M)	Reason for Acquisition/ Motivation		Quantity	Unit Cost	Total Cost	METHOD OF PROCUREMENT
Goods & Services							
Administrative fees	x x x x x x x x x x x x	Official travelling arrangements		10	2000	20 000,00	Term Contract
Communication	x x x x x x x x x x x x	Official Cellphones and SITA Telephone		12	17000	204 000,00	Transversal Contract
Computer services (SITA & EXTERNAL) OPERATIONS		IT OPERATIONS					
SITA Datalines	x x x x x x x x x x x x	Internet and mail connectivity		12	300000	3 600 000,00	Term Contract
SITA Helpdesk	x x x x x x x x x x x x	SITA IT Help Desk call centre		12	745000	8 940 000,00	Term Contract
SITA Internet Charges	x x x x x x x x x x x x	Access to the Internet Facility		12	341000	4 092 000,00	Term Contract
SITA Persal Mainframe	x x x x x x x x x x x x	Acess to payroll and HR system		12	108000	1 346 000,00	Term Contract
SITA BAS Mainframe	x x x x x x x x x x x x	Acess to the financial system		12	208000	2 570 000,00	Term Contract
SITA LOGIS Mainframe	x x x x x x x x x x x x	Acess to the financial system		12	12000	144 000,00	Term Contract
Cloud Migration (DM02) Azure Consumption	x x x x x x x x x x x x	Infrastructure as a service		12	400000	4 800 000,00	Term Contract
IT End-User Computing Services	x x x x x x x x x x x x	Infrastructure as a service		12	2040000	24 480 000,00	Term Contract
IT Server Support Services	x x x x x x x x x x x x	Infrastructure as a service		12	660000	7 920 000,00	Term Contract
Solar-Winds Maintenance and Sytem		Infrastructure as a service		1	966000	966 000,00	Term Contract
Computer services (GOVERNANCE, RISK AND SECURITY)		IT SERVICES for Governance					
Security Operation Centre							
Back-up Solution				1	1500000	1 500 000,00	SITA Procurement
Disaster recovery as a service				1	1500000	1 500 000,00	SITA Procurement
Vulnerability Management Solution				1	1500000	1 500 000,00	SITA Procurement
SSL Certificate				1	30000	30 000,00	SITA Procurement
Transition Services	x			1	1300000	1 300 000,00	Term Contract

Item Description	Lead Time/ Delivery Date												Reason for Acquisition/ Motivation	Quantity	Unit Cost	Total Cost	METHOD OF PROCUREMENT
	1st Q			2nd Q			3rd Q			4th Q							
	A	M	J	J	A	S	O	N	D	J	F	M					
Computer services (APPLICATIONS AND BUSINESS SOLUTIONS)													IT SERVICES for Applications				
E Submission (IAE01)														1	1000000	1 000 000,00	BID/RFQ
Modern Workplace Modernisation – Paperless & ECM (IAE02)														1	2000000	2 000 000,00	Term Contract/ BID
Water Use licencing (EC02) (WARMS & WMS Assessment & technical design and implamentation)														1	2000000	2 000 000,00	Term Contract/ BID
Computer services (ENTERPRISE ARCHITECTURE)													IT SERVICES for Enterprise Architecture				
Enterprise Architecture	X	X	X	X	X	X	X	X	X	X	X	X		12	465000	5 580 000,00	Term Contract
Contractors	X	X	X	X	X	X	X	X	X	X	X	X					
LAN Cabling Maintenance and Support													Maintenance and Support	1	1000000	1 000 000,00	Term Contact
ITP WAN LAN & Desktop Support	X	X	X	X	X	X	X	X	X	X	X	X	Maintenance and Support	12	45000	540 000,00	SITA Procurement
Emrgency Repairs														1	460000	460 000,00	RFQ
Firewall Maintenance and Suuport														1	1000000	1 000 000,00	BID /RFQ
Entertainment			X			X			X			X	Meeting Entertainment	4	2000	8 000,00	Petty Cash
Consumables(Diesel, IT Consumables and other Consumables)	X	X	X	X	X	X	X	X	X	X	X	X		4	200000	800 000,00	RFQ

Water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

NEW PROJECT LIS T 2023-2024

NO	Directorate/ Implementing Agency	Detailed description of goods, works or services	Indicate Alignment to (APP) Strategic Objective	Transformation and Empowerment targets	Responsive Target	Envisaged Advert Date	Envisaged Bid Closing Date	Envisaged Evaluation Date	Envisaged Bid Award Date	Contract Expiry Date	Estimated Value Allocated for 2023/2024 financial year (Including all	Total Bid Value (Including all applicable taxes)	Deficit (Applicable) Amount based on Bid Response	COMMENT
				QSE= 15 EME= 15 WOMEN= 40 YOUTH= 30 DISABILITY=7 N/A: REFER TO COMMENT	Advertised Target for Empowerment									
1	Infrastructure and Operations	Infrastructure & Network Modernization (DM01) (IT LAN Equipment (Phase2))	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Apr-23	30-May-23	R8 700 000,00	R8 700 000,00		
2	Infrastructure and Operations	Infrastructure & Network Modernization (DM01) LAN Cabling Main & Sapp	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Jun-23	31-Jul-23	R1 000 000,00	R1 000 000,00		
3	Governance, Risk and Security	Security Strategy Implementation (Servers Firewall Cache)	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Apr-23	30-May-23	R8 000 000,00	R8 000 000,00		
4	Governance, Risk and Security	Security Strategy Implementation (Back-Up as a service)	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Apr-23	30-May-23	R1 500 000,00	R1 500 000,00		
5	Governance, Risk and Security	Security Strategy Implementation (Disaster Recovery as a service)	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Apr-23	30-May-23	R1 500 000,00	R1 500 000,00		
6	Governance, Risk and Security	Security Strategy Implementation (Vulnerability Mnagement Solution)	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Apr-23	30-May-23	R3 500 000,00	R3 500 000,00		
7	Governance, Risk and Security	Security Strategy Implementation (Net Tech UPS)	Efficient, effective and development oriented department		QSE/EME	30-Apr-23	31-May-23	30-Jun-23	31-Jul-23	31-Aug-23	R2 500 000,00	R2 500 000,00		
8	Governance, Risk and Security	Security Strategy Implementation (Antivirus & Encryption)	Efficient, effective and development oriented department		QSE/EME	28-Feb-23	31-Mar-23	30-Apr-23	31-May-23	1-Jun-23	R2 500 000,00	R2 500 000,00		
9	Governance, Risk and Security	Firewall Maintenance & Support	Efficient, effective and development oriented department		QSE/EME	31-Aug-23	30-Sep-23	15-Oct-23	30-Nov-23	1-Feb-24	R3 000 000,00	R3 000 000,00		
10	Applications and Business Solutions	E Submission (MERI)	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Apr-23	31-May-23	R1 000 000,00	R1 000 000,00		
11	Applications and Business Solutions	Modern Workplace Modernisation – Paperless & EDM (Knowledge Management) (MERI)	Efficient, effective and development oriented department		QSE/EME	30-Jun-23	31-Jul-23	15-Aug-23	15-Sep-23	15-Oct-23	R2 000 000,00	R2 000 000,00		
12	Applications and Business Solutions	Water Use licensing [EC02] (WARMS & WMS Assessment & technical design and implementation)	Enhanced regulation of the water and sanitation sector		QSE/EME	30-Jun-23	31-Jul-23	15-Aug-23	15-Sep-23	15-Oct-23	R2 000 000,00	R2 000 000,00		
13	Infrastructure and Operations	IT Outsourced Service to SITA	Efficient, effective and development oriented department		QSE/EME	N/A	N/A	N/A	30-Jun-23	1-Sep-23	R90 343 000,00	R 439 000 000,00		
TOTAL											R 121 543 000,00	R 482 290 000,00		

Annexure D

INSTALLATION ID : NAT: WATER AND SANITATION
LOCATION ID : NAT: WATER AND SANITATION
USERID : HLUNGWANIM
REPORT REQUEST ID : 00363838
SORT CRITERIA : F O S A P R M I
SELECTION CRITERIA :

1. LAST CLOSED MONTH : 05/2023
2. ITEM : I
3. INFRASTRUCTURE : S
4. OBJECTIVE : O
5. RESPONSIBILITY : R
6. FUND : F
7. PROJECT : P
8. ASSETS : A
9. REGIONAL IDENTIFIER : M

SELECTION CRITERIA : TYPE	DETAIL
FUND	ALL
OBJECTIVE	INFORMATION & COMM TECHNOLOGY
INFRASTRUCTURE	ALL
ASSETS	ALL
PROJECT	ALL
RESPONSIBILITY	DIR:ICT GOV COMP RISK & INFO SEC
REGIONAL IDENTIFIER	ALL
ITEM	ALL

SORT CRITERIA : F O S A P R M I

TOTALS : O0006 O0007 O0008 R0005 I0004

PAGE BREAK : NONE

PROFILE : SECURITY

ECONOMIC CLASS : ALL

TOT ON ECON CLASS : NO

LAST CLOSED MONTH : 05/2023

TYPE LEVEL	DESCRIPTION	EXPENSES	COMMITMENTS	BUDGET	AVAILABLE BUDGET

	O 006	DWS:CORPORATE SERVICES				
	O 007	INFORMATION & COMM TECHNOLOGY				
	R 005	DIR:ICT GOV COMP RISK & INFO SEC				
TOTAL	I 004	SALARIES AND WAGES----------	463,053.38	0.00	3,782,000.00	3,318,946.62
TOTAL	I 004	SOCIAL CONTRIBUTIONS----------	47,799.24	0.00	575,000.00	527,200.76
TOTAL	I 004	COMPUTER SERVICES----------	774,320.19	19,197.42	9,330,000.00	8,536,482.39
TOTAL	I 004	CONTRACTORS----------	0.00	0.00	1,000,000.00	1,000,000.00
TOTAL	I 004	ENTERTAINMENT----------	0.00	0.00	2,000.00	2,000.00
TOTAL	I 004	CONS SUPPLIES----------	0.00	897,668.66	900,000.00	2,331.34
TOTAL	I 004	TRAVEL AND SUBSISTENCE----------	318.56	0.00	9,000.00	8,681.44
TOTAL	I 004	TRAINING & DEVELOPMENT----------	0.00	0.00	60,000.00	60,000.00
TOTAL	I 004	OPERATING PAYMENTS----------	0.00	0.00	5,000.00	5,000.00
TOTAL	I 004	SOFTW & OTHER INTANGIBLE ASSETS ---------	0.00	0.00	5,000,000.00	5,000,000.00
TOTAL	R 005	DIR:ICT GOV COMP RISK & INFO SEC ---------	1,285,491.37	916,866.08	20,663,000.00	18,460,642.55
TOTAL	O 007	INFORMATION & COMM TECHNOLOGY----------	1,285,491.37	916,866.08	20,663,000.00	18,460,642.55
TOTAL	O 006	DWS:CORPORATE SERVICES----------	1,285,491.37	916,866.08	20,663,000.00	18,460,642.55

**** END OF REPORT RP0203BS ****

Confidential
Memo confirming availability or non-availability of funds
Chief Directorate: Financial Management

water & sanitation
Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

Tel: 012 336 7922

INTERNAL MEMO

Date: March 28, 2023	File No:2023/24 Procurement Plan
To: Chief Financial Officer	From: Chief Director: Financial Management

CONFIRMATION OF FUND ON THE 2023/24 CONSOLIDATED PROCUREMENT PLAN OF THE DEPARTMENT OF WATER AND SANITATION

1. PURPOSE

To recommend to the Chief Financial Officer to support or/ not to support the 2023/24 Procurement Plan of the Department of Water and Sanitation.

2. MOTIVATION/ ANALYSIS

2.1. Applicable Prescripts, Regulations, Circular, Policy and/or Delegations of Authority:

Financial delegations and cost containment measures must be adhered to.

2.2. Funding Requirements

The Procurement Plan as per the table below has proposed contracts to the value of R2.422 billion.

For the 2023/24 financial year, the estimated cash flow for the department will be R671.481million to fund projects that will be implemented during the financial year.

The major procurement items in the procurement plan are Flights and Accommodation, Fleet Management, and IT Outsourced Services to SITA with expected cash flow of R100 million, R150 million and R90 million respectively in the 2023/24 financial year.

The procurement process for these projects is expected to start during the 2023/24 financial year and most of the planned procurement was included in the 2023 Estimates of National Expenditure process. Funds will also be reprioritised to funds intervention such as Transactional & Project Advisors for the new departmental building amongst others.

The table below depicts the summary of the demand plan per programme and economic classification.

Programme	2023 Estimated Cash Flow R 000	Value of Planned Procurement R 000
Administration	R 412 717	R 2 019 644 0
Water Resources Management	R 87 871	R 212 900
Water Services Management	R 170 893	R 189 903
Grand Total	**R671 481**	**R 2 422 447**

Annexure A is attached for details. An amount estimated at **R674 069** is currently loaded on BAS for the financial year 2023/24 for these interventions. Some of these interventions will be implemented through the MTEF period and funding is available.

3. **RECOMMENDATION**

- Funds are available in the 2023/24 financial year, and it is therefore recommended that the Chief Financial Officer **should** support the funding of the 2023/24 procurement plan.

TG CHAUKE
ACTING CHIEF DIRECTOR: FINANCIAL MANAGEMENT SERVICES
DATE: 28 Mar 2023

RECOMMENDATION 3: SUPPORT/ ~~NOT SUPPORTED~~

F MOATSHE
CHIEF FINANCIAL OFFICER
DATE:2023/03/28

FINAL CONSOLIDATED PROCUREMENT PLAN FOR 2023/2024 FINANCIAL YEAR						
No	Directorate	Detail description of goods, works or services	Alignment to APP/Strategic Objective	Estimated Value Allocated for 2023/24 financial year (incuding all applicable taxes)	Estimated Total Bid value (including all applicable taxes)	Available Budget on BAS
PROGRAMME 1 ADMINISTRATION						
1	D: Corporate Communication	language services	meaningful engagement with communities and communicating with the public in languages of their choice	R3 000 000,00	R9 000 000,00	R1 734 000,00
2	Media Liaison	To analyse media coverage from all over the country regarding water issues	meaningful engagement with communities and communicating with the public in languages of their choice	R1 200 000,00	R1 200 000,00	R13 159 000,00
3	Media Liaison	To train senior managers of the department on Media issues	meaningful engagement with communities and communicating with the public in languages of their choice	R2 000 000,00	R2 000 000,00	
4	D: FACILITIES MANAGEMENT	FLIGHT AND ACCOMMODATION	Sustain current operations	R100 000 000,00	R500 000 000,00	R136 586 000,00
5	D: FACILITIES MANAGEMENT	FLEET MANAGEMENT	Sustain current operations	R150 000 000,00	R980 000 000,00	R26 410 000,00
6	D: FACILITIES MANAGEMENT	PLUMBING SERVICES	Sustain current operations	R500 000,00	R1 500 000,00	R5 418 000,00
7	D: FACILITIES MANAGEMENT	ELECTRICAL SERVICES	Sustain current operations	R500 000,00	R1 500 000,00	
8	D: FACILITIES MANAGEMENT	TELEPHONE/FIXED LINE SRVICES	Sustain current operations	R500 000,00	R1 500 000,00	R11 477 000,00
9	D: FACILITIES MANAGEMENT	TRANSACTIONAL ADVISORS	Sustain current operations	R21 800 000,00	R21 800 000,00	R0,00
10	D: Roodeplaat Learning Centre	Supply and delivery of grocery and cleaning products	Sustain current operations	R3 230 000,00	R9 500 000,00	R686 000,00
11	Governance, Risk and Security	Security Strategy Implementation (Security Operation Centre)	Efficient, effective and development orientated department	R 6 000 000,00	R 6 000 000,00	R 1 500 000,00
12	Governance, Risk and Security	Security Strategy Implementation (Back-Up as a service)	Efficient, effective and development orientated department	R 1 500 000,00	R 1 500 000,00	R 1 500 000,00
13	Governance, Risk and Security	Security Strategy Implementation (Disaster Recovery as a service)	Efficient, effective and development orientated department	R 1 500 000,00	R 1 500 000,00	R 1 500 000,00
14	Governance, Risk and Security	Security Strategy Implementation (Vulnerability Mnagement Soulution)	Efficient, effective and development orientated department	R 1 500 000,00	R 1 500 000,00	R 59 556 000,00
15	Governance, Risk and Security	Security Strategy Implementation (Net Back-UP)	Efficient, effective and development orientated department	R 2 500 000,00	R 7 500 000,00	
16	Governance, Risk and Security	Security Strategy Implementation (Antivirus & Encryption)	Efficient, effective and development orientated department	R 2 500 000,00	R 7 500 000,00	
17	Eastern Cape- Water Sector Support	Project Execution Plans	yes	R10 000 000,00	R10 000 000,00	R0,00
18	Eastern Cape- Infrusctructure Development	Project Execution Plans	yes	R5 000 000,00	R5 000 000,00	R0,00
19	Free State-Water Resources Support	Conditional assessment and possible upgrade of all WWTWs and WTWs in Maluti a Phofung LM	3.9 Regional Bulk Infrastructure Projects Implemented	R0	R7 010 000	R0,00
20	Free State-Water Resources Support	Conditional assessment and possible upgrade of all WWTWs in Matjhabeng LM	3.9 Regional Bulk Infrastructure Projects Implemented	R0	R7 500 000	R0,00
21	Free State-Compliance	Procurement of lab chemicals	N/A	R1 200 000	R1 200 000	R0,00
22	Kwazulu Natal: Water Sector Support	Five year Plan Ilembe District Municipality	4.1.1: Number of DMs with completed 5 Year Water & Sanitation Reliability Implementation Plans	R800 000,00	R1 400 000	R800 000,00
23	Kwazulu Natal: Water Sector Support	Five year Plan Zululand District Municipality	4.1.1: Number of DMs with completed 5 Year Water & Sanitation Reliability Implementation Plans	R800 000,00	R1 400 000	R800 000,00
24	Kwazulu Natal: Water Sector Support	Five year Plan King Cetshwayo District Municipality	4.1.1: Number of DMs with completed 5 Year Water & Sanitation Reliability Implementation Plans	R800 000,00	R1 400 000	R800 000,00
25	Kwazulu Natal: Water Sector Support	Five year Plan Uthukela District Municipality	4.1.1: Number of DMs with completed 5 Year Water & Sanitation Reliability Implementation Plans	R800 000,00	R1 400 000	R800 000,00
26	Kwazulu Natal: Water Sector Support	Project Dashboard RBIG/WSIG	4.1.1: Number of DMs with completed 5 Year Water & Sanitation Reliability Implementation Plans	R400 000,00	R1 500 000	R400 000,00
27	Kwazulu Natal: Water Sector Support	Five Year Plan for City of Ethekwini	4.1.1: Number of DMs with completed 5 Year Water & Sanitation Reliability Implementation Plans	R400 000,00	R1 400 000	R400 000,00
28	HR Performance and Development	Skill Audit for SMS and MMS employees	4.1.1: Number of DMs with completed 5 Year Water & Sanitation Reliability Implementation Plans	R3 500 000	R3 500 000	R7 108 000
29	D: FACILITIES MANAGEMENT	AIRCONDITION	Sustain current operations	R500 000,00	R1 500 000,00	R28 123 000,00

No	Directorate	Detail description of goods, works or services	Alignment to APP/Strategic Objective	Estimated Value Allocated for 2023/24 financial year (incuding all applicable taxes)	Estimated Total Bid value (including all applicable taxes)	Available Budget on BAS
30	D: SECURITY MANAGEMENT	INSTALLATIONS OF ACCESS CONTROL SYSTEMS	Sustain current operations	R8 000 000,00	R10 000 000,00	R11 288 000,00
31	Infrastructure and Operations	Infrastructure & Network Modernization (DM01) (IT LAN Equipment (Phase2))	Efficient, effective and development orientated department	R 6 144 000,00	R 6 144 000,00	R 6 495 000,00
32	Infrastructure and Operations	Infrastructure & Network Modernization (DM01) LAN Cabling Main & Supp	Efficient, effective and development orientated department	R 1 000 000,00	R 1 000 000,00	R 1 000 000,00
33	Applications and Business Solutions	E Submission (IAE01)	Efficient, effective and development orientated department	R 1 000 000,00	R 1 000 000,00	R 1 000 000,00
34	Applications and Business Solutions	Modern Workplace Modernisation – Paperless & ECM (Knowledge Management) (IAE02)	Efficient, effective and development orientated department	R 2 000 000,00	R 2 000 000,00	R 2 000 000,00
35	Applications and Business Solutions	Water Use licencing (EC02) (WARMS & WMS Assessment & technical design and Implementation)	Enhanced regulation of the water and sanitation sector	R 2 000 000,00	R 2 000 000,00	R 2 000 000,00
36	Infrastructure and Operations	IT Outsourced Services to SITA	Efficient, effective and development orientated department	R 90 343 000,00	R 439 000 000,00	R 85 909 000,00
TOTAL FOR PROGRAMME ONE				**R 432 917 000,00**	**R 2 058 854 000,00**	**R 408 449 000,00**
PROGRAMME 2: WATER RESOURCES MANAGEMENT						
37	Speciall Unit: Water Res Strat & Evaluation	Disaster Management Level 2 Plan	Operational Plan	R1 500 000,00	R 1 500 000	R 4 080 000,00
38	D: WRDP	Bridging Study: Lower Orange River : Vioolsdrift/Noordoewer Dam	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R1 000 000,00	R5 000 000,00	R28 163 000,00
39	D: WRDP	Clanwilliam Dam Raising: Conveyance Infrastructure: EIA	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R2 000 000,00	R8 000 000,00	
40	D: WRDP	Verbeeldingskraal Dam: Technical Feasibility Study	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R50 000,00	R30 000 000,00	
41	D: WRDP	Pre-Feasibility Study to develop water resources for Musina Pipeline, Musina Dam Off chane scheme, Mutale Dam, future transferes from Zimbabwe	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R1 500 000,00	R3 500 000,00	
42	D: WRDP	Pre-feasibility Study for Potential Options to Transfer Water from the Komati River System to Augment the Olifants River system	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R1 000 000,00	R2 000 000,00	
43	D: WRDP	Pre-feasibility Study for Mfolozi Catchment: raising of Klipfontein dam	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R2 000 000,00	R50 000 000,00	
44	D: SWRP	DWS: National Water and Sanitation Master Plan Implementation	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R300 000,00	R6 000 000,00	R11 771 000,00
45	D: SWRP	Change of assurance of supply on existing scheme	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R500 000,00	R2 000 000,00	
46	D: SWRP	Modelling of crop water requirements for existing irrigation schemes	Number of RID's and feasibility studies for bulk water supply and sanitation services infrastructure project plans completed according to APP	R400 000,00	R2 000 000,00	
47	DIR:RD	Update the PES EIS database (60 mnts)	The integrity of freshwater ecosystems protected	4 721 000	20 000 000	24 672 000
48	DIR:RD	Refinement of Strategic Groundwater Source Areas	The integrity of freshwater ecosystems protected	0	10 000 000	
49	Resource Quality Information Services (RQIS)	Development of a Database for NAEHMP	Ecological infrastructure protected and restore	R2 000 000,00	R2 000 000,00	R2 000 000,00
50	Water Resource Regulation	Towards Implementation of the Long-term Strategy for Acid Mine Drainage (AMD).	2.2.1 Implementation of the long term strategies for AMD mitigation	R4 000 000,00	R4 000 000,00	R0,00
51	Directorate: Waste Water Services Regulation	To provide Scientific and Technical Support to the Drinking Water Quality (Blue Drop) & Wastewater (Green Drop) Regultaion for Assessemnt of Water Supply and Wastewater Treatment Systems (Madi Project, Current Project WP 11351)	5.3.1 & 5.3.2 (Drinking) 5.1.8 & 5.1.9 (Waste)	R 43 000 000,00	R 43 000 000,00	R 20 050 000,00
52	Resource Quality Information Services (RQIS)	Replacement of AA500F and GBC AAS instrument with ICPOES	Ecological infrastructure protected and restore	R1 000 000,00	R1 000 000,00	R8 881 000,00
53	Resource Quality Information Services (RQIS)	Replacement of obsolete GCMS instrument in Organic laboratory	Ecological infrastructure protected and restore	R2 900 000,00	R2 900 000,00	
54	Directorate : Spatia Information	1. Fully Automatic Total Station 0.5 R1000, Monitoring Station with Service and Maintenance	1.2 Water resources monitoring programmes and information systems reviewed and maintained	R1 000 000,00	R1 000 000,00	R1 023 000,00
55	NHS	EXPANSION OF GROUND WATER MONITORING SITES IN EASTERN CAPE	UPDATING OF 3 MONITORING PROGRAMMES	2 000 000,00	2 000 000,00	23 637 000,00
56	NHS	ACID MINE DRAINAGE MONITORING IN MPUMALANGA REGION	UPDATING OF 3 MONITORING PROGRAMMES	2 000 000,00	2 000 000,00	
57	NHS	UPDATING OF THE HYDROGEOLOGICAL MAPS OF SOUTH AFRICA	UPDATING OF 3 MONITORING PROGRAMMES	3 000 000,00	3 000 000,00	
58	NHS	Developing a National Real-Time Data Management System (NRTDMS)	UPDATING OF 3 MONITORING PROGRAMMES	1 500 000,00	1 500 000,00	

No	Directorate	Detail description of goods, works or services	Alignment to APP/Strategic Objective	Estimated Value Allocated for 2023/24 financial year (incuding all applicable taxes)	Estimated Total Bid value (including all applicable taxes)	Available Budget on BAS
59	NHS	EIAs FOR GAUGING WEIRS	UPDATING OF 3 MONITORING PROGRAMMES	R 4 000 000,00	R 4 000 000,00	
60	CD: WUCME	Appointment of a service provider for development of e-learning system for the (Environmental Management Inspectorates [Blue Scorpions] and Water Use Compliance Monitoring and Enforcement officials) and maintenance thereof	Not on APP but aligned to 5.1.5 (5.1.5.3 Compliance and Enforcement Information Systems for WUCME)	R1 500 000,00	R1 500 000,00	R2 000 000,00
61	Water Resource Regulation	Waste Discharge Charge System (WDCS) implementation of the Mitigation Charge in the Vaal WMA	2.2.3 Waste Discharge system (WDCS) implementation country wide	R5 000 000,00	R5 000 000,00	R0,00
TOTAL FOR PROGRAMME TWO				**R 87 871 000,00**	**R 212 900 000,00**	**R 126 077 000,00**
PROGRAMME 3: WATER SERVICES MANAGEMENT						
62	Water Service Institution Management	Review of the Shareholders Oversight model including the Shareholders Compacts for Public Entities reporting to the Minister	Alignment of WB	R3 400 000,00	R3 400 000,00	R6 000 000,00
63	Water Service Institution Management	Annual Review of Boards and CEO Remuneration	Alignment of WB	R3 000 000,00	R3 000 000,00	
64	Water Service Institution Management	Assessing the impact of expansion of bulk infrastructure on the Capital requirements of Water Boards	Alignment of WB	R5 000 000,00	R5 000 000,00	
65	Water Service Institution Management	Due diligence study of the reconfiguration of Water Boards	Alignment of WB	R2 754 000,00	R2 754 000,00	
66	Water Service Institution Management	Regrading of the Water Boards	Alignment of WB	R3 000 000,00	R3 000 000,00	
67	WATER SERVICES PLANNING SUPPORT	Port Nolloth Bulk Water Supply	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 860 000,00	R1 860 000,00	R1 860 000,00
68	WATER SERVICES PLANNING SUPPORT	Postmasburg Bulk Water Supply	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R8 605 970,80	R8 605 970,80	R8 606 000,00
69	WATER SERVICES PLANNING SUPPORT	Kakamas WWTW	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 439 500,00	R2 439 500,00	R2 440 000,00
70	WATER SERVICES PLANNING SUPPORT	Kakamas BWS	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 455 000,00	R2 455 000,00	R2 455 000,00
71	WATER SERVICES PLANNING SUPPORT	Warrenton WWTW	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 922 365,66	R1 922 365,66	R1 923 000,00
72	WATER SERVICES PLANNING SUPPORT	De Aar WWTW	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 839 801,92	R2 839 801,92	R2 839 801,92
73	WATER SERVICES PLANNING SUPPORT	Philisptown BWS	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R3 136 072,23	R3 136 072,23	R3 136 000,00
Limpopo						
74	WATER SERVICES PLANNING SUPPORT	Provincial Bulk	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 400 000,00	R1 400 000,00	R1 400 000,00
75	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Waterberg	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 100 000,00	R1 100 000,00	R1 100 000,00
76	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Sekhukhune	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 500 000,00	R1 500 000,00	R1 500 000,00
77	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Vhembe	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 500 000,00	R1 500 000,00	R1 500 000,00
78	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Polokwane	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 000 000,00	R1 000 000,00	R1 000 000,00
79	WATER SERVICES PLANNING SUPPORT	Greater Letaba Water Augmentation Distribution: Mopani Works (Nkamabo BWS)	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 129 157,21	R2 129 157,21	R2 130 000,00
80	WATER SERVICES PLANNING SUPPORT	Nandoni Water Treatment Works Upgrade and extensions	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R9 989 857,09	R9 989 857,09	R9 990 000,00
81	WATER SERVICES PLANNING SUPPORT	Giyani Water Services	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R5 713 349,70	R5 713 349,70	R5 714 000,00
North West						
82	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Bojanala	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 188 913,60	R1 188 913,60	R1 189 000,00
83	WATER SERVICES PLANNING SUPPORT	Pilanesberg South Bulk Water Supply Phase 3	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 000 000,00	R1 000 000,00	R1 000 000,00
83	WATER SERVICES PLANNING SUPPORT	Pilanesberg South Bulk Water Supply Phase 2	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 000 000,00	R1 000 000,00	R1 000 000,00
84	WATER SERVICES PLANNING SUPPORT	Midvaal Bulk Water Supply Scheme	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R3 126 850,00	R3 126 850,00	R3 127 000,00
KwaZulu Natal						
85	WATER SERVICES PLANNING SUPPORT	Provincial Bulk	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 468 413,60	R1 468 413,60	R1 468 000,00

No	Directorate	Detail description of goods, works or services	Alignment to APP/Strategic Objective	Estimated Value Allocated for 2023/24 financial year (incuding all applicable taxes)	Estimated Total Bid value (including all applicable taxes)	Available Budget on BAS
86	WATER SERVICES PLANNING SUPPORT	Five Yr Plan uMgungundlovu	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 126 012,88	R1 126 012,88	R1 126 000,00
87	WATER SERVICES PLANNING SUPPORT	Amajuba regional bulk scheme	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 171 179,50	R1 171 179,50	R1 171 000,00
Free State						
88	WATER SERVICES PLANNING SUPPORT	Provincial Bulk	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 279 804,00	R1 279 804,00	R1 280 000,00
89	WATER SERVICES PLANNING SUPPORT	Mathjabeng LM Thabong Waste Water Treatment Works	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 333 400,00	R1 333 400,00	R1 333 000,00
89	WATER SERVICES PLANNING SUPPORT	Conditional assessment and possible upgrade of all WWTWs and WTWs in Mafube LM	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 771 428,57	R1 771 428,57	R1 771 000,00
90	WATER SERVICES PLANNING SUPPORT	Conditional assessment and possible upgrade of all WWTWs and WTWs in Moqhaka LM	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 842 857,14	R1 842 857,14	R1 843 000,00
Mpumalanga						
91	WATER SERVICES PLANNING SUPPORT	Provincial Bulk	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 446 872,00	R1 446 872,00	R1 447 000,00
92	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Ehlanzeni, Gert Sibande and Nkalanga	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 604 779,60	R2 604 779,60	R2 605 000,00
92	WATER SERVICES PLANNING SUPPORT	Northern Nsikazi Bulk Water Supply Phase 2	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 836 179,50	R2 836 179,50	R2 836 000,00
93	WATER SERVICES PLANNING SUPPORT	Emalahleni Bulk Water Supply Phase 3	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 116 937,50	R1 116 937,50	R1 117 000,00
Eastern Cape						
94	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Alfred Nzo	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 500 000,00	R1 500 000,00	R1 500 000,00
95	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Joe Gqabi	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 500 000,00	R1 500 000,00	R1 500 000,00
95	WATER SERVICES PLANNING SUPPORT	Provincial Bulk	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 151 701,61	R1 151 701,61	R1 152 000,00
96	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Buffalo City	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 500 000,00	R1 500 000,00	R1 500 000,00
96	WATER SERVICES PLANNING SUPPORT	Kinira Regional BWSS	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R3 532 532,50	R3 532 532,50	R3 533 000,00
97	WATER SERVICES PLANNING SUPPORT	Mkemane Regional Bulk WSS	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 179 702,11	R1 179 702,11	R1 180 000,00
97	WATER SERVICES PLANNING SUPPORT	Coffee Bay Regional Bulk Water Supply Phase 4 and 5	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 757 010,08	R2 757 010,08	R2 757 000,00
98	WATER SERVICES PLANNING SUPPORT	Lower Telle River Bulk Water Supply Scheme	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R3 041 729,20	R3 041 729,20	R3 042 000,00
98	WATER SERVICES PLANNING SUPPORT	Belmont Valley WWTW	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R4 040 434,26	R4 040 434,26	R4 040 000,00
99	WATER SERVICES PLANNING SUPPORT	Mbizana	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 114 960,46	R2 114 960,46	R2 115 000,00
99	WATER SERVICES PLANNING SUPPORT	CHDM cluster 7	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 234 718,10	R1 234 718,10	R1 235 000,00
Western Cape						
100	WATER SERVICES PLANNING SUPPORT	Provincial Bulk	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 300 000,00	R1 300 000,00	R1 300 000,00
101	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Cape Winelands	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 100 000,00	R1 100 000,00	R1 100 000,00
101	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Central Karoo	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 100 000,00	R1 100 000,00	R1 100 000,00
102	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Eden	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 100 000,00	R1 100 000,00	R1 100 000,00
102	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Overberg	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 100 000,00	R1 100 000,00	R1 100 000,00
103	WATER SERVICES PLANNING SUPPORT	Five Yr Plan West Coast	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 100 000,00	R1 100 000,00	R1 100 000,00
Gauteng						
104	WATER SERVICES PLANNING SUPPORT	Provincial Bulk	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 400 000,00	R1 400 000,00	R1 400 000,00

No	Directorate	Detail description of goods, works or services	Alignment to APP/Strategic Objective	Estimated Value Allocated for 2023/24 financial year (incuding all applicable taxes)	Estimated Total Bid value (including all applicable taxes)	Available Budget on BAS
105	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Ekhurhuleni	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 300 000,00	R1 300 000,00	R1 300 000,00
105	WATER SERVICES PLANNING SUPPORT	Five Yr Plan Sedibeng	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 300 000,00	R1 300 000,00	R1 300 000,00
106	WATER SERVICES PLANNING SUPPORT	Five Yr Plan West Rand	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 300 000,00	R1 300 000,00	R1 300 000,00
106	WATER SERVICES PLANNING SUPPORT	Sedibeng Regional Waste Water Treatment Works	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R3 077 900,68	R3 077 900,68	R3 078 000,00
107	WATER SERVICES PLANNING SUPPORT	Sebokeng Waste Water Treatment Works	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 393 088,54	R2 393 088,54	R2 393 000,00
107	WATER SERVICES PLANNING SUPPORT	Vaal River System Intervention	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 777 674,60	R1 777 674,60	R1 778 000,00
108	WATER SERVICES PLANNING SUPPORT	Westonaria Regional Bulk Sanitation (Zuurbekom)	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R2 702 846,06	R2 702 846,06	R2 703 000,00
108	WATER SERVICES PLANNING SUPPORT	WSDP PROJECTS	3.9.1 & 3.9.2: Completed Feasibility and Implementation Readiness Studies for water and wastewater services projects (RBIG)	R1 000 000,00	R1 000 000,00	R1 000 000,00
109	Water Use Efficiency	Procurement of a Professional Service Provider	Number of large water supply systems assessed for water losses	R1 000 000,00	R1 000 000,00	R1 000 000,00
109	Spec Unit: WSSE	Review of the Strategic Framework for Water Services.	YES	R1 500 000,00	R1 500 000,00	R1 500 000,00
110	Water Services Information Management	External IT Support services	yes	R12 530 000,00	R12 530 000,00	R12 530 000,00
TOTAL FOR PROGRAMME THREE				**R 150 693 000,69**	**R 150 693 000,69**	**R 139 542 801,92**
TOTAL FOR ALL PROGRAMMES				**R671 451 000,69**	**R 2 422 447 000,69**	**R 674 088 801,92**

TG CHAUKE
ACTING CHIEF DIRECTOR: FINANCIAL MANAGEMENT SERVICES
DATE: 27 Mar 2023

F MOATSHE
CHIEF FINANCIAL OFFICER
DATE: 2023/03/28

CENTRAL SUPPLIER DATABASE
FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.106 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

SUPPLIER IDENTIFICATION

Supplier number	MAAA0146218	South African company/CC registration number	1999/001899/30
Is supplier active?	Yes	Have Bank Account	Yes
Supplier type	CIPC Company	Registration date	29 Jan 1999 00:00:00:000
Supplier sub-type	State Owned Company	Created by	bavika.munien@sita.co.za
Legal name	STATE INFORMATION TECHNOLOGY AGENCY	Created date	23 May 2016 11:41:35:000
Trading name	State Information Technology Agency SOC Ltd.	Edit by	bavika.munien@sita.co.za
Identification type	South African Company/Close Corporation Registration Number	Edit date	27 Jun 2023 13:51:56:300
Government breakdown	State Owned Company (SOC Ltd)	Restricted Supplier	No
Business status	In Business	Restricted Director	No
Country of origin	South Africa	Government Employee	Yes

SUPPLIER CONTACT INFORMATION

CONTACT 1

Contact type	Administration	Do you want this contact to also be a CSD user ?	Yes
Is this your preferred Contact?	Yes	Created by	bavika.munien@sita.co.za
Name(s)	Bavika	Created date	23 May 2016 11:41:35:567
Surname	Munien	Edit by	bavika.munien@sita.co.za
Identification type	South African Identification Number	Edit date	23 May 2016 11:41:35:567
Prefer communication via email	Yes		
Email address	bavika.munien@sita.co.za		
Cellphone number	0833762156		

CONTACT 2

Contact type	Finance	Email address	tasnim.vorajee@sita.co.za
Is this your preferred Contact?	No	Telephone number	0124822122
Name(s)	Tasnim	Cellphone number	0826745050
Surname	Vorajee	Fax number	0866321133

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.126 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Identification type	South African Identification Number	Website address	www.sita.co.za
Prefer communication via cellphone	Yes	Do you want this contact to also be a CSD user ?	Yes
Prefer communication via email	Yes	Created by	bavika.munien@sita.co.za
		Created date	23 May 2016 11:41:35:630
		Edit by	bavika.munien@sita.co.za
		Edit date	26 May 2016 09:58:00:000

SUPPLIER ADDRESS INFORMATION

ADDRESS 1

Is this a preferred address?	Yes	Postal code	0001
Address line 1	459 Tsitsa Street	Ward Number	42
Address line 2	Erasmuskloof	Country	South Africa
Suburb	Erasmuskloof	This address S/A delivery	Yes
Province	Gauteng	Created by	bavika.munien@sita.co za
Municipality	City of Tshwane	Created date	23 May 2016 09:49:51:000
City	Pretoria	Edit by	bavika.munien@sita.co.za
		Edit date	23 May 2016 11:41:35:537

ADDRESS 2

Is this a preferred address?	No	Ward Number	42
Address line 1	P. O. Box 26100	Country	South Africa
Address line 2	Monument Park	Created by	bavika munien@sita.co.za
Suburb	Monument Park	Created date	23 May 2016 09:51:54:000
Province	Gauteng	Edit by	bavika.munien@sita.co.za
Municipality	City of Tshwane	Edit date	23 May 2016 11:41:35:553
City	Pretoria		
Postal code	0105		

SUPPLIER BANK ACCOUNT

BANK ACCOUNT 1

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.141 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Account type	Current Accounts	Created by	bavika.munien@sita.co.za
Bank	STANDARD BANK OF SOUTH AFRICA	Created date	02 Jun 2016 13:03:20:000
Branch number	051001	Edit by	csd.safetynetbatch@treasury.gov.za
Branch name	STANDARD BANK SOUTH AFRICA	Edit date	30 Jun 2016 16:13:23:363
Account number	410298158	Bank Verification Status	Verification Succeeded
Account holder	SITA SOC LTD	Foreign Bank Account	No
Is this a preferred account?	Yes	Is the identifier linked at the bank	Yes
Active start date	23 May 2016 09:52:42:000	Is this a Shared Funding Account	No

TAX INFORMATION

Income tax number	9511089642	Overall Tax Status	Tax Compliant
VAT number	4450180346	Created by	bavika.munien@sita.co.za
Is this supplier a VAT vendor?	Yes	Created date	23 May 2016 11:41:35:000
PAYE number	7940712401	Edit by	csd.reverifybatch@treasury.gov.za
Are you Registered with SARS?	Yes	Edit date	27 Jun 2023 13:51:57:000
Last validation date	20 Jul 2023 07:11:00:000		

B-BEEE INFORMATION

Certificate type	None		
Created by	bavika.munien@sita.co.za	Edit by	bavika.munien@sita.co.za
Created date	23 May 2016 11:41:41:897	Edit date	22 Jun 2016 09:57:15:000

DIRECTORS/MEMBERS/OWNERS INFORMATION

DIRECTOR/MEMBER 1

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.157 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Director type	Director	Created date	09 Feb 2021 09:39:08:000
Director status	Active	Edit by	csd.reverifybatch@treasury.gov.za
Name(s)	MOLATLHEGI KHUNOU	Edit date	18 Apr 2023 15:01:33:000
Surname	KGAUWE	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	20 Jul 2023 07:10:52:047
Identification type	South African Identification Number	Government Employee	Yes
South African identification number	8011225460087	Department	State Information Technology Agency;
Work permit	0000000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:517
Appointment date	01 Dec 2020 00:00:00:000	SA identification number Verified	Yes
Owner	No	SA identification number verification date	20 Jul 2023 07:10:51:720
Created by	csd.reverifybatch@treasury.gov.za	Companies involved in	MAAA0597042;

DIRECTOR/MEMBER 2

Director type	Director	Created date	22 Feb 2022 15:40:52:000
Director status	Active	Edit by	csd.reverifybatch@treasury.gov.za
Name(s)	MAKANO	Edit date	18 Apr 2023 15:01:34:000
Surname	MOSIDI	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	20 Jul 2023 07:10:52:047
Identification type	South African Identification Number	Government Employee	No
South African identification number	6401250295080	Government Employee Last Verification Date	20 Jul 2023 07:10:51:533
Work permit	0000000	SA identification number Verified	Yes
Appointment date	01 Feb 2022 00:00:00:000	SA identification number verification date	20 Jul 2023 07:10:51:737
Owner	No	Companies involved in	MAAA0169164; MAAA1151117;
Created by	csd.reverifybatch@treasury.gov.za		

DIRECTOR/MEMBER 3

Director type	Director	Created date	22 Feb 2022 15:40:53:000
Director status	Active	Edit by	csd.reverifybatch@treasury.gov.za
Name(s)	MOTLHAGO STELLA	Edit date	18 Apr 2023 15:01:34:000
Surname	BVUMA	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	20 Jul 2023 07:10:52:047

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

CSD REGISTRATION REPORT

Identification type	South African Identification Number	Government Employee	No
South African identification number	7709230426081	Government Employee Last Verification Date	20 Jul 2023 07:10:51:547
Work permit	0000000	SA identification number Verified	Yes
Appointment date	01 Feb 2022 00:00:00:000	SA identification number verification date	20 Jul 2023 07:10:51:767
Owner	No		
Created by	csd.reverifybatch@treasury.gov.za		

DIRECTOR/MEMBER 4

Director type	Director	Created date	22 Feb 2022 15:40:54:000
Director status	Active	Edit by	csd.reverifybatch@treasury.gov.za
Name(s)	ZIMBINI	Edit date	18 Apr 2023 15:01:34:000
Surname	HILL	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	20 Jul 2023 07:10:52:060
Identification type	South African Identification Number	Government Employee	No
South African identification number	7901090312085	Government Employee Last Verification Date	20 Jul 2023 07:10:51:547
Work permit	0000000	SA identification number Verified	Yes
Appointment date	01 Feb 2022 00:00:00:000	SA identification number verification date	20 Jul 2023 07:10:51:797
Owner	No	Companies involved in	MAAA0110380; MAAA0327764; MAAA0419719; MAAA0585272; MAAA0878781;
Created by	csd.reverifybatch@treasury.gov.za		

DIRECTOR/MEMBER 5

Director type	Director	Created date	22 Feb 2022 15:40:55:000
Director status	Active	Edit by	csd.reverifybatch@treasury.gov.za
Name(s)	TSHILIDZI	Edit date	18 Apr 2023 15:01:34:000
Surname	RATSHITANGA	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	20 Jul 2023 07:10:52:060
Identification type	South African Identification Number	Government Employee	Yes
South African identification number	7510075533084	Department	National:The Presidency; State Information Technology Agency;
Work permit	0000000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:580
Appointment date	01 Feb 2022 00:00:00:000	SA identification number Verified	Yes

CSD REGISTRATION REPORT

Owner	No	SA identification number verification date	20 Jul 2023 07:10:51:830
Created by	csd.reverifybatch@treasury.gov za	Companies involved in	MAAA0004912; MAAA0173338;

DIRECTOR/MEMBER 6

Director type	Director	Created date	22 Feb 2022 15:40:57:000
Director status	Active	Edit by	csd.reverifybatch@treasury.gov.za
Name(s)	VINCENT MATODZI	Edit date	18 Apr 2023 15:01:34:000
Surname	RATSHIMBILANI	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	20 Jul 2023 07:10:52:060
Identification type	South African Identification Number	Government Employee	No
South African identification number	7309056184086	Government Employee Last Verification Date	20 Jul 2023 07:10:51:580
Work permit	0000000	SA identification number Verified	Yes
Appointment date	01 Feb 2022 00:00:00:000	SA identification number verification date	20 Jul 2023 07:10:51:843
Owner	No	Companies involved in	MAAA0333974; MAAA0354850; MAAA0886018; MAAA0906162; MAAA1223996;
Created by	csd.reverifybatch@treasury.gov.za		

DIRECTOR/MEMBER 7

Director type	Director	Created date	22 Feb 2022 15:40:58:000
Director status	Active	Edit by	csd.reverifybatch@treasury.gov za
Name(s)	NOLITHA	Edit date	18 Apr 2023 15:01:35:000
Surname	PIETERSEN	Restricted Director	No
Country	South Africa	Restriction Last Verification Date	20 Jul 2023 07:10:52:060
Identification type	South African Identification Number	Government Employee	No
South African identification number	8209120627087	Government Employee Last Verification Date	20 Jul 2023 07:10:51.593
Work permit	0000000	SA identification number Verified	Yes
Appointment date	01 Feb 2022 00:00:00:000	SA identification number verification date	20 Jul 2023 07:10:51:877
Owner	No	Companies involved in	MAAA0750061; MAAA1304353;
Created by	csd.reverifybatch@treasury.gov.za		

DIRECTOR/MEMBER 8

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.221 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Director type	Director	Created by	csd.reverifybatch@treasury.gov.za
Director status	Active	Created date	22 Feb 2022 15:40:59:000
Name(s)	JEANNETTE MMATSIATE	Edit by	csd.reverifybatch@treasury.gov.za
Surname	MORWANE	Edit date	18 Apr 2023 15:01:35:000
Country	South Africa	Restricted Director	No
Identification type	South African Identification Number	Restriction Last Verification Date	20 Jul 2023 07:10:52:077
South African identification number	7909050372080	Government Employee	Yes
Work permit	0000000	Department	National:Communications and Digital Technologies;
Appointment date	01 Feb 2022 00:00:00:000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:593
Owner	No	SA identification number Verified	Yes
		SA identification number verification date	20 Jul 2023 07:10:51:893

DIRECTOR/MEMBER 9

Director type	Director	Created by	csd.reverifybatch@treasury.gov.za
Director status	Active	Created date	22 Feb 2022 15:41:00:000
Name(s)	OLWETHU	Edit by	csd.reverifybatch@treasury.gov.za
Surname	KETSEKILE	Edit date	18 Apr 2023 15:01:35:000
Country	South Africa	Restricted Director	No
Identification type	South African Identification Number	Restriction Last Verification Date	20 Jul 2023 07:10:52:077
South African identification number	8511150634085	Government Employee	No
Work permit	0000000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:610
Appointment date	01 Feb 2022 00:00:00:000	SA identification number Verified	Yes
Owner	No	SA identification number verification date	20 Jul 2023 07:10:51:907

DIRECTOR/MEMBER 10

Director type	Director	Created by	csd.reverifybatch@treasury.gov.za
Director status	Active	Created date	22 Feb 2022 15:41:01:000
Name(s)	WILLIAM	Edit by	csd.reverifybatch@treasury.gov.za
Surname	VUKELA	Edit date	18 Apr 2023 15:01:35:000
Country	South Africa	Restricted Director	No

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.253 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Identification type	South African Identification Number	Restriction Last Verification Date	20 Jul 2023 07:10:52:077
South African identification number	6912225471085	Government Employee	Yes
Work permit	0000000	Department	National:Public Service and Administration;
Appointment date	01 Feb 2022 00:00:00:000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:610
Owner	No	SA identification number Verified	Yes
		SA identification number verification date	20 Jul 2023 07:10:51:923

DIRECTOR/MEMBER 11

Director type	Director	Created by	csd.reverifybatch@treasury.gov.za
Director status	Active	Created date	22 Feb 2022 15:41:02:000
Name(s)	RENDANI	Edit by	csd.reverifybatch@treasury.gov.za
Surname	RAMABULANA	Edit date	18 Apr 2023 15:01:36:000
Country	South Africa	Restricted Director	No
Identification type	South African Identification Number	Restriction Last Verification Date	20 Jul 2023 07:10:52:077
South African identification number	8409245461087	Government Employee	No
Work permit	0000000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:627
Appointment date	01 Feb 2022 00:00:00:000	SA identification number Verified	Yes
Owner	No	SA identification number verification date	20 Jul 2023 07:10:51:940
		Companies involved in	MAAA0081561; MAAA0081726; MAAA0382206; MAAA1014583; MAAA1015091;

DIRECTOR/MEMBER 12

Director type	Director	Created by	csd.reverifybatch@treasury.gov.za
Director status	Active	Created date	22 Feb 2022 15:41:03:000
Name(s)	LAURA	Edit by	csd.reverifybatch@treasury.gov.za
Surname	MSEME	Edit date	18 Apr 2023 15:01:36:000
Country	South Africa	Restricted Director	No
Identification type	South African Identification Number	Restriction Last Verification Date	20 Jul 2023 07:10:52:093
South African identification number	6803100006080	Government Employee	Yes
Work permit	0000000	Department	National:National Treasury;

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.269 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Appointment date	01 Feb 2022 00:00:00:000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:627
Owner	No	SA identification number Verified	Yes
		SA identification number verification date	20 Jul 2023 07:10:52:000

DIRECTOR/MEMBER 13

Director type	Director	Created by	csd.reverifybatch@treasury.gov.za
Director status	Active	Created date	18 Apr 2023 15:01:36:000
Name(s)	BONGANI ANDY	Edit by	csd.reverifybatch@treasury.gov.za
Surname	MABASO	Edit date	18 Apr 2023 15:01:36:000
Country	South Africa	Restricted Director	No
Identification type	South African Identification Number	Restriction Last Verification Date	20 Jul 2023 07:10:52:093
South African identification number	8705065764082	Government Employee	Yes
Work permit	0000000	Department	State Information Technology Agency;
Appointment date	01 Apr 2023 00:00:00:000	Government Employee Last Verification Date	20 Jul 2023 07:10:51:643
Owner	No	SA identification number Verified	Yes
		SA identification number verification date	20 Jul 2023 07:10:52:013
		Companies involved in	MAAA1252999;

The CSD does not automatically verify foreign company registration number, international securities identification number, foreign identification numbers, foreign passport numbers, work permit numbers, foreign bank accounts, B-BBEE, demographic and accreditation information. Organs of State are required to manually verify this information with the applicable verification institutions as per their current policies and procedures.

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.269 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Tips and Frequently Asked Questions (FAQ)

Identifier

CSD cannot electronically verify the identity of a supplier other than a South African Individual / Sole Proprietor (through Home Affairs) or a company registered at the Companies and Intellectual Property Commission (CIPC). For this reason, a disclaimer is displayed for supply chain practitioners to obtain supporting documentation to verify the identity and legitimacy of a supplier in these cases.

Bank

For help on how to resolve bank failures click here: I received an email stating the bank information I captured on the CSD was sent for bank account validation and could not be validated. The response received from the bank contains an error message.
The various possible error messages received from the bank are highSemiBolded in red. Search for the applicable message and follow the detailed steps associated with that error message.

Tax

Tax Compliance Status
For help on how to deal with tax status differences between CSD and the tax clearance certificate click here: What should a supplier do if the tax status on CSD difference from the tax clearance certificate?

Tax Compliance Expiry Date
For help on how to deal with tax status differences between CSD and the tax clearance certificate click here: How does CSD determine the tax compliance expiry date?

CIPC

Should the director/member information reflected on the CIPC registration report differs to that reflected on CSD for help click here: The active Directors/Members are not being populated on the CSD Directors/Members screen as they appear at CIPC, how can I rectify this?

State Employee

For more information pertaining to government employment status click here: Will there be verification done to identify if a supplier is a government employee?

BBBEE

CSD does not automatically verify all certificate information with the various accreditation bodies. Organs of State are required, where not automatically verified by CSD, to manually verify this information with the applicable accreditation body as per current policies and procedures. Expired certificate information do not reflect on the report.

RESTRICTION

Restricted Supplier *- A supplier is restricted by using the identification number of the entity e.g. CIPC registration -, trust -, Social Development non-profit -, South African ID -, Foreign company registration number or ID number. If there is more than one CSD Supplier profile registered on CSD with the same entity identification number, all those related supplier profiles will be restricted.*

Restricted Director *– A director/owner is an individual person and is restricted by using the South African ID or Foreign ID number. If a director belongs to different companies and has been restricted, the director will reflect as restricted in all companies where identification number is detected.*

Restricted Suppliers & Directors are listed on CSD under Help – Am I restricted?

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

CENTRAL SUPPLIER DATABASE FOR GOVERNMENT

Report Date:
20 Jul 2023 07:11:05.269 AM
Report Ran By:
vandermerweh3@dws.gov.za

CSD REGISTRATION REPORT

Print Date: 7/20/2023 7:11:05 AM

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA