Request for proposals (RFP)

The provision or supply of Database and Information Security Maintenance and Support to CSIR for a three (3) year period on an "as and when basis"

RFP No. 3530/05/08/2022

Date of Issue	Thursday, 07 July 2022
Last date for submission of intent to bid form (Appendix A)	Thursday, 20 July 2022 @ 16:30
Briefing Session	Thursday, 21 July 2022 15:00-16:00 (Link to be shared 24 hours prior to the session)
Closing Date and Time	Friday, 05 August 2022 @ 16:30
Enquiries and submission of proposals	All responses must be submitted to: tender@csir.co.za Submissions cannot be submitted to any other address, as this will lead to elimination
Contact details	All enquiries must be submitted to tender@csir.co.za. This email is only for submission or enquiries. *(Please use the RFP number as the subject reference)*
CSIR business hours	08h00 – 16h30

TABLE OF CONTENTS

LIST OF TABLES

SECTION A – TECHNICAL INFORMATION

4 INTRODUCTION

The Council for Scientific and Industrial Research (CSIR) is one of the leading scientific research and technology development organisations in Africa. In partnership with national and international research and technology institutions, CSIR undertakes directed and multidisciplinary research and technology innovation that contributes to the improvement of the quality of life of South Africans. The CSIR's main site is in Pretoria while it is represented in other provinces of South Africa through regional offices.

5 BACKGROUND

The CSIR requires the technical support and system administration services on Databases, Information Security, and System Administration.

6 INVITATION FOR PROPOSAL

Proposals are hereby invited for:

6.1 System Administration

6.2 PostgreSQL database support and administration, and

6.3 Information Security Operations

7 PROPOSAL SPECIFICATION

All proposals are to be submitted in a format specified in this RFP (as applicable). However, service providers are welcome to submit additional or alternative proposals over and above the originally specified format (e.g. other capabilities that you may deem to be relevant).

Service providers are required to submit their RFP which detail the following:

7.1 System Administration

System administrators are responsible for the maintenance, configuration, and reliable operation of computer systems and servers. They install hardware and software and participate in research and development to continuously improve and meet the Business requirements of the organization. System administrators also actively resolve problems and issues with computer and server systems, minimising service disruptions within the organisation.

The system administration service includes service management activities such as change management, incident management, release management, configuration management, availability management, problem management, and knowledge management.

Operational requirements are detailed in the table below followed by a description of the technology stack that will be supported.

7.1.2 Operational requirements

Table 1: System administration operational requirements

Service Required	Experience	Training/Certification	Required service Level	Evaluation reports required
Install and configure new base operating systems	6 years of system administration experience with Microsoft and Open-Source operating environments, network troubleshooting, security principles, , DBMS experience, application and web technologies, identity management, governance, and compliance practices	Linux Administrator (LPIC or CompTIA Linux+ or similar)	Normal working hours (07:30-17:00)	Updated Configuration documentation Due by the 3rd working day of the month
Patch operating systems and software			Normal working hours (07:30-17:00)	N/A
Manage availability and performance of systems			Availability > 99% Critical service 24x7x365	Monthly availability reports Due by the 3rd working day of the month
Design and implement new solutions			Normal working hours (07:30-17:00)	Updated configuration documentation Due by the 3rd working day of the month
Monitor availability and performance			Availability > 99% Critical service 24x7x365	Monthly availability reports Due by the 3rd working day of the month

Access management: (Create, modify, and revoke user access control lists)			Normal working hours (07:30-17:00)	Access management documentation (Authorisation, Changes/Modification, Evidence of revoked access) Due by the 3rd working day of the month
Implement and maintain a set of general system controls required to provide the necessary assurance to the Governing Authority.			Normal working hours (07:30-17:00)	As needed/required Evidence to be kept updated in a dedicated data store for ad-hoc auditing
Monitor and manage backups			Normal working hours (07:30-17:00), and after-hours	Backup check sheet, Backup reports Daily, Weekly, and Monthly checks and corrective action reports being made available by the 3rd working day of the month
Performance and functionality troubleshooting			Normal working hours (07:30-17:00), and	Root cause analysis Reports to be made available by the 3rd
Service management				

Security compliance (baselines, anti-virus, anti-malware, access control, auditing)			after hours for emergencies	working day of the month
Monitor, tune, and configure VMware environment	6 Years virtualisation experience	VMware (VCTA)	Normal working hours (07:30-17:00)	Monthly availability reports Due by the 3rd working day of the month
Monitor and configure storage stack	6 Years storage/SAN/iSCSI experience	Any relevant vendor/storage certification	Normal working hours (07:30-17:00)	Monthly availability reports Due by the 3rd working day of the month
Network management (including designing, configuring, analysing & troubleshooting networks)	5 Years	Cisco CCNA (R&S) or CCNP (R&S)	Normal working hours (07:30-17:00)	Weekly Checklist Evidence to be kept updated in a dedicated data store for ad-hoc auditing
Management of Cisco ACI (Application Centric Infrastructure) is essential	2-4 Years	Cisco ACI	Normal working hours (07:30-17:00)	Weekly Checklist and Monthly *(Due by the 3rd working day of the month)* reports Evidence to be kept updated in a dedicated data store for ad-hoc auditing

Firewall management and administration (Experience with FortiGate administration is essential)	2-4 Years	FortiGate NSE4	Normal working hours (07:30-17:00), and after hours for emergencies	Weekly Checklist and Monthly *(Due by the 3rd working day of the month)* reports Evidence to be kept updated in a dedicated data store for ad-hoc auditing
Monitor and remedy Common Vulnerabilities and Exposures (CVE) reported on the vulnerabilities and patch of the system			Normal working hours (07:30-17:00), and after hours for emergencies	Vulnerability and patch summary (ad hoc)
Service continuity must be ensured at all times.			Availability > 99% Critical service 24x7x365	A monthly service continuity report *(Due by the 3rd working day of the month)*

7.1.3 Technology Stack

- Linux (Ubuntu, Centos)
- Windows (Server 2019)
- virtualisation (VMware)
- Containerisation (Docker, Minikube)
- Storage (HP Nimble, general SAN, iSCSI)
- Backup (Commvault)
- Monitoring (Zabbix, Prometheus, Elastic search, Logstash, Kibana)
- DNS (bind9)
- Identity and authentication (Dir389)
- Nginx
- SFTP
- PostgreSQL
- Cisco
- Cisco ACI
- Fortinet/FortiGate

7.1.4 Infrastructure landscape

The current environment consists of the following Infrastructure, running a combination of the technology stack, listed in section 4.1.3.

- 2 Windows Servers
- 50 Production and 25 Development and Testing Ubuntu servers
- 8 Production and 4 Development and Testing PostgreSQL Databases
- 13 VMWare ESXi hosts
- 6 Cisco Nexus Leaf switches
- 2 Cisco Nexus Spine switches
- 1 FortiGate Firewall
- 2 Imperva DAM VM appliances
- 2 Nimble storage appliances

Please note that this environment may be duplicated in the future, implying a 100% growth, over the next 1-2 years.

7.2 PostgreSQL database support and administration

The systems covered in this section are a mix between Online Transaction Processing and Data Lake functions supporting a large customer base with a national footprint. A proficient database administrator is required with the following responsibilities: software installation and maintenance, data extraction, transformation and loading, database backup and recovery, database security and auditing, access control, capacity planning, performance monitoring, database tuning, troubleshooting, documenting, and reporting.

Operational requirements are detailed in the table below followed by a description of the technology stack that will be supported.

7.2.2 Operational requirements

Table 2: Database Administrator operational requirements

Service Required	Experience	Training/Certification	Required service Level	Evaluation reports required
Install, configure, upgrade, and administer Databases (DB) with replication and failover as required per project	7 years	Certified PostgreSQL DBA(CPSDBA) PostgreSQL Associate Certification Advanced PostgreSQL OR similar	Normal working hours (07:30-17:00)	Summary of work done (ad hoc)
Manage DB uptime			Availability > 99% Critical service 24/7	Report failures (ad hoc) Monthly availability reports Due by the 3rd working day of the month
Monitor DB performance			Stable response times Critical service 24/7	Average Response times, Load average (weekly)
Improve DB performance as required tuning, indexing, table size, long queries			Normal working hours (07:30-17:00)	Summary of work done, and recommendations implemented (ad hoc), included in the monthly reports Due by the 3rd working day of the month
Monitor and remedy Common Vulnerabilities and Exposures (CVE) reported on the DB			Normal working hours (07:30-	Vulnerability and patch summary (ad hoc).

			17:00)	Monthly vulnerability reports Due by the 3rd working day of the month
Automate and monitor processes, backups, failover			Normal working hours (07:30-17:00)	Backup testing (Daily) Evidence reported in the backup weekly report Failover testing (monthly) Monthly back-up reports Due by the 3rd working day of the month
Monitoring existing DB integrations with external data sources			Normal working hours (07:30-17:00)	Availability/uptime (weekly) Monthly availability reports Due by the 3rd working day of the month
Manage Disaster Recovery			Critical Service 24/7	Disaster Recovery Plan Disaster recovery report (ad hoc)
Manage licensing requirements			Normal working hours (07:30-17:00)	License compliance and requirement, Monthly reported. Due by the 3rd working day of the month
OS (Operating System) Experience	4 years	Linux Administrator (LPIC or CompTIA	Normal working hours (07:30-	

		Linux+ or similar)	17:00)	
Implement and maintain a set of general system controls required to provide the necessary assurance to the Governing Authority.			Normal working hours (07:30-17:00)	As needed/required Evidence to be kept updated in a dedicated data store for ad-hoc auditing
Service continuity must be ensured at all times.			Availability > 99% Critical service 24x7x365	A monthly service continuity report *(Due by the 3rd working day of the month)*

7.2.3 Technology Stack

- PostgreSQL v9 and higher
- Monitoring (Nagios, Prometheus, Elastic search, Logstash, Kibana)
- Linux (Ubuntu, Centos)
- Windows (Server 2019)
- Virtualisation (VMware)
- Containerisation (Docker, Minikube)
- Storage (HP Nimble, general SAN, iSCSI)
- Backup (Commvault)
- Monitoring (Zabbix, Prometheus, Elastic search, Logstash, Kibana)
- DNS (bind9)
- Identity and authentication (Dir389)
- Nginx
- SFTP
- PostgreSQL
- Cisco
- Cisco ACI
- Fortinet/FortiGate

7.2.4 Infrastructure landscape

The current environment consists of the following Infrastructure, running a combination of the technology stack, listed in section 4.1.3.

- 2 Windows Servers
- 50 Production and 25 Development and Testing Ubuntu servers
- 8 Production and 4 Development and Testing PostgreSQL Databases
- 13 VMWare ESXi hosts
- 2 Imperva DAM VM appliances

Please note that this environment may be duplicated in the future, implying a 100% growth, over the next 1-2 years.

7.3 Information security Operations

Faced with ever-increasing cyber-security threats, organisations must maintain a vigilant approach to protect their systems and data, and Security Engineers play a key role in this process. Security Engineers can be responsible for several functions associated with IT security, from ensuring the security of software to selecting and/or constructing and deploying broader network security systems. The Security Engineer will be responsible for completing a thorough risk assessment, identifying vulnerabilities within the network, managing the remediation process, managing firewall rules, and configuring systems to enhance existing security features. Security Engineers are expected to respond to, and document, any security threats, resolve technical faults, and allocate resources to deliver real solutions cost-effectively. The Security Engineer must also be proficient in the skills and competencies listed in sections 4.3.1 and 4.3.2 below:

7.3.2 Operational requirements

Table 3: Security administration operational requirements

Service Required	Experience	Training/Certification	Required service Level	Evaluation reports required
Develop strategies to respond to and recover from a security breach	5+ years (Require 5 years' experience to earn CISSP)	An ICT related degree, or equivalent experience Certified Information Systems Security Professional (CISSP) CISA – Certified Information Systems Auditor (CISA) CEH – Certified Ethical Hacker (CEH) CISM – Certified Information Security Manager (CISM)	Normal working hours (07:30-17:00)	Summary of work done (ad hoc)
Develop or implement open-source/third-party tools to assist in detection, prevention, and analysis of security threats			Normal working hours (07:30-17:00)	Report failures (ad hoc)
Awareness training of the workforce on information security standards, policies, and best practices			Normal working hours (07:30-17:00)	Summary of work done (ad hoc)
Implement protections			Normal working hours (07:30-17:00)	Summary of work done and recommendations (ad hoc)
Installation and use of firewalls, data encryption, and other security products and procedures			Normal working hours (07:30-17:00)	Summary of work done and recommendations (ad hoc)
Conduct periodic network scans to find any vulnerability			Normal working hours (07:30-17:00)	Vulnerability and patch summary (ad hoc)
Oversee the penetration testing, simulating an attack on the system to find exploitable weaknesses			Normal working hours (07:30-17:00)	Summary of work done and recommendations (ad hoc)

Monitor networks and systems for security breaches, using software that detects intrusions and anomalous system behavior		ISSAP – Information Systems Security Architecture Professional (ISSAP) ISSEP – Information Systems Security Engineering Professional (ISSEP)	Critical service 24x7x365	Summary of work done and recommendations (ad hoc)
Investigate security breaches			Critical service 24x7x365	Summary of work done and recommendations (ad hoc)
Lead incident response, including steps to minimize the impact and then conducting a technical and forensic investigation into how the breach happened and the extent of the damage			Critical service 24x7x365	Summary of work done and recommendations (ad hoc)
Implement and maintain a set of general system controls required to provide the necessary assurance to the Governing Authority.			Normal working hours (07:30-17:00)	As needed/required
Service continuity must be ensured at all times.			Availability > 99% Critical service 24x7x365	A monthly service continuity report *(Due by the 3rd working day of the month)*

7.3.3 Skills and Competencies

- Expertise in anti-virus software, intrusion detection, firewalls, and content filtering
- Knowledge of risk assessment tools, technologies, and methods
- Expertise in designing secure networks, systems, and application architectures
- Disaster recovery, computer forensic tools, technologies, and methods
- Planning, researching, and developing security policies, standards, and procedures
- System administration, supporting multiple platforms and applications
- Expertise with mobile code, malicious code, and anti-virus software
- Endpoint security solutions, including file integrity monitoring and data loss prevention
- Experience and knowledge of AWS and cloud platform as a service (PaaS) security
- Experience in the implementation and administration of a Security Incident and event management system (SIEM)
- Experience in Automating security testing tools
- Experience and knowledge of in Chef (a configuration management tool), or equivalent
- Experience and knowledge of Git (a tool that helps track anomalous changes to files), or equivalent

General skills include:

- The ability to multi-task
- A trained eye for detail
- Strong organizational skills
- The ability to thrive in fast-paced, high-stress situations
- The ability to communicate network security issues to peers and management

7.3.4 Technology Stack

- PostgreSQL v9 and higher
- Monitoring (Nagios, Prometheus, Elastic search, Logstash, Kibana)
- Linux (Ubuntu, Centos)
- Windows (Server 2019)

- Virtualisation (VMware)
- Containerisation (Docker, Minikube)
- Storage (HP Nimble, general SAN, iSCSI)
- Backup (Commvault)
- Monitoring (Zabbix, Prometheus, Elastic search, Logstash, Kibana)
- DNS (bind9)
- Identity and authentication (Dir389)
- Nginx
- SFTP
- PostgreSQL
- Cisco
- Cisco ACI
- Fortinet/FortiGate

7.3.5 Infrastructure landscape

The current environment consists of the following Infrastructure, running a combination of the technology stack, listed in section 4.1.3.

- 2 Windows Servers
- 50 Production and 25 Development and Testing Ubuntu servers
- 8 Production and 4 Development and Testing PostgreSQL Databases
- 13 VMWare ESXi hosts
- 6 Cisco Nexus Leaf switches
- 2 Cisco Nexus Spine switches
- 1 FortiGate Firewall
- 2 Imperva DAM VM appliances
- 2 Nimble storage appliances

Please note that this environment may be duplicated in the future, implying a 100% growth, over the next 1-2 years.

8 ANNEXURE A: PRICING SCHEDULE

Table 4: Service Pricing

Item	Description	Size/UoM	Quantity	Total Price
1	System Administration	Each		
2	PostgreSQL database support and administration	Each		
3	Information security Operations	Each		
NB: Pricing must be inclusive of all costs to be incurred by the bidder in the delivery of the required services, including any disbursement.				
Sub-Total				
VAT 15%				
Total				

Notes:

- Quantities, refer to the number of months of the contract (36)
- Total price, refer to the total price for the services over the contract period per service.

9 FUNCTIONAL EVALUATION CRITERIA

The evaluation of the functional/technical detail of the proposal will be based on the following criteria:

The Bidder to indicate which of the sections they are bidding for or responding to, as each of the service responses will be evaluated separately:

Table 5: Bidder response to services

Item	**Description**	**Yes** *(Mark with X)*	**No** *(Mark with X)*
1	System Administration ***(Table 6)***		
2	PostgreSQL database support and administration ***(Table 7)***		
3	Information security Operations ***(Table 8)***		

Table 6: Evaluation criteria for System Administration

Functional Factors	**Proof Required**	**Weighting**	**0 points**	**5 points**	**10 points**
Company Experience	Company profile indicating the number of years they have been in existence in the service industry, on the scope in service 4.1, 4.2, or 4.3.	20	Less than 12 months	13 – 24 months	More than 24 months
Size of customer operations The service provider must have dealt with large organisations of at least 500 users.	At least three references (3) to be supplied. The total users of 500 will be determined across the largest 2 of the 3 references	10	Less than 250 users	250-499 users	More than 500 users

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Customer references The number of customers where the scope of services has been delivered	At least one customer where the scope of the service has been delivered.	10	None	One customer	One customer
Monthly SLA performance achievement Meeting at least 99% of the performance criteria	The service provider must demonstrate their understanding of the reporting requirements by supplying sample reports.	20	Less than 50% of reports	50%-75% of all reports	More than 75% of reports
Service Transition plan Covering the quality, practicality, and duration	A transition plan, covering timelines, responsibilities, and quality of delivery	20	No transition plan	Not all aspects covered	All aspects covered
System Administration	At least 2 CV's of staff covering the following skills, and >6 years of experience. • Linux Administrator (LPIC or CompTIA Linux+ or similar) • VMware (VCTA) • Any relevant vendor/storage certification • Cisco CCNA (R&S) or CCNP (R&S) • Cisco ACI	20	Falling short of experience and skills in more than 2 of the technologies	Falling short of experience and skills in 1-2 of the technologies	Falling short of experience and skills in none of the

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
	• FortiGate NSE4				

Table 7: Evaluation criteria for PostgreSQL database support and administration

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Company Experience	Company profile indicating the number of years they have been in existence in the service industry, on the scope in service 4.1, 4.2, or 4.3.	20	Less than 12 months	13 – 24 months	More than 24 months
Size of customer operations The service provider must have dealt with large organisations of at least 500 users.	At least three references (3) to be supplied. The total users of 500 will be determined across the largest 2 of the 3 references	10	Less than 250 users	250-499 users	More than 500 users
Customer references The number of customers where the scope of services has been delivered	At least one customer where the scope of the service has been delivered.	10	None	One customer	One customer

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Monthly SLA performance achievement Meeting at least 99% of the performance criteria	The service provider must demonstrate their understanding of the reporting requirements by supplying sample reports.	20	Less than 50% of reports	50%-75% of all reports	More than 75% of reports
Service Transition plan Covering the quality, practicality, and duration	A transition plan, covering timelines, responsibilities, and quality of delivery	20	No transition plan	Not all aspects covered	All aspects covered
PostgreSQL database support and administration	• At least 2 CV's of staff covering the following skills, and >5 years of experience • Certified PostgreSQL DBA(CPSDBA) • PostgreSQL Associate Certification • Advanced PostgreSQL • OR similar • Linux Administrator (LPIC or CompTIA Linux+ or similar)	20	Falling short of experience and skills in more than 2 of the technologies	Falling short of experience and skills in 1-2 of the technologies	Falling short of experience and skills in none of the

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Company Experience	Company profile indicating the number of years they have been in existence in the service industry, on the scope in service 4.1, 4.2, or 4.3.	20	Less than 12 months	13 – 24 months	More than 24 months
Size of customer operations The service provider must have dealt with large organisations of at least 500 users.	At least three references (3) to be supplied. The total users of 500 will be determined across the largest 2 of the 3 references	10	Less than 250 users	250-499 users	More than 500 users
Customer references The number of customers where the scope of services has been delivered	At least one customer where the scope of the service has been delivered.	10	None	One customer	One customer
Monthly SLA performance achievement Meeting at least 99% of the performance criteria	The service provider must demonstrate their understanding of the reporting requirements by supplying sample reports.	20	Less than 50% of reports	50%-75% of all reports	More than 75% of reports

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Service Transition plan Covering the quality, practicality, and duration	A transition plan, covering timelines, responsibilities, and quality of delivery	20	No transition plan	Not all aspects covered	All aspects covered
Information security Operations	At least 2 CV's of staff covering the following skills, and >6 years of experience • An ICT related degree, or equivalent experience • Certified Information Systems Security Professional (CISSP) • CISA – Certified Information Systems Auditor (CISA) • CEH – Certified Ethical Hacker (CEH) • CISM – Certified Information Security Manager (CISM) • ISSAP – Information Systems Security Architecture Professional (ISSAP) ISSEP – Information Systems Security Engineering Professional (ISSEP)	20	Falling short of experience and skills in more than 2 of the technologies	Falling short of experience and skills in 1-2 of the technologies	Falling short of experience and skills in none of the

Table 8: Evaluations criteria for Information Security Operations

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Company Experience	Company profile indicating the number of years they have been in existence in the service industry, on the scope in service 4.1, 4.2, or 4.3.	20	Less than 12 months	13 – 24 months	More than 24 months
Size of customer operations The service provider must have dealt with large organisations of at least 500 users.	At least three references (3) to be supplied. The total users of 500 will be determined across the largest 2 of the 3 references	10	Less than 250 users	250-499 users	More than 500 users
Customer references The number of customers where the scope of services has been delivered	At least one customer where the scope of the service has been delivered.	10	None	One customer	One customer
Monthly SLA performance achievement Meeting at least 99% of the performance criteria	The service provider must demonstrate their understanding of the reporting requirements by supplying sample reports.	20	Less than 50% of reports	50%-75% of all reports	More than 75% of reports

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Service Transition plan Covering the quality, practicality, and duration	A transition plan, covering timelines, responsibilities, and quality of delivery	20	No transition plan	Not all aspects covered	All aspects covered
Information security Operations	At least 2 CV's of staff covering the following skills, and >6 years of experience • An ICT related degree, or equivalent experience • Certified Information Systems Security Professional (CISSP) • CISA – Certified Information Systems Auditor (CISA) • CEH – Certified Ethical Hacker (CEH) • CISM – Certified Information Security Manager (CISM) • ISSAP – Information Systems Security Architecture Professional (ISSAP) ISSEP – Information Systems Security Engineering Professional (ISSEP)	20	Falling short of experience and skills in more than 2 of the technologies	Falling short of experience and skills in 1-2 of the technologies	Falling short of experience and skills in none of the

9.1 Proposals with functionality / technical points of less than the pre-determined minimum overall percentage of 70%. less than 50% on any of the individual criteria will be eliminated from further evaluation.

9.2 Refer to Annexure A (Page 14) for the scoring sheet that will be used to evaluate functionality.

10 ELIMINATION CRITERIA

Proposals will be eliminated under the following conditions:

- Submission after the deadline.
- Proposals submitted at the incorrect location.
- Failure to submit completed Annexure A: Pricing Schedule.
- Non-attendance of the online compulsory briefing session/site inspection.
- Cloud submissions via Dropbox, WeTransfer, Google Drive, etc will not be accepted.
- Non-submission of a signed Non-Disclosure Agreement.

11 NATIONAL TREASURY CENTRAL SUPPLIER DATABASE REGISTRATION

Before any negotiations will start with the winning bidder it will be required from the winning bidder to:

- be registered on National Treasury's Central Supplier Database (CSD). Registrations can be completed online at: www.csd.gov.za.
- provide the CSIR of their CSD registration number, and

provide the CSIR with a valid copy of their SANAS accredited B-BBEE certificate or affidavit. If no certificate/affidavit can be provided, no points will be scored during the evaluation process. (RSA suppliers only).

SECTION B – TERMS AND CONDITIONS

12 PROCEDURE FOR SUBMISSION OF PROPOSALS

12.1 All proposals must be submitted electronically to tender@csir.co.za.

12.2 Respondents must use the RFP number as the subject reference number when submitting their bids.

12.3 The e-mail and file sizes should not exceed a total of 25MB per e-mail.

12.4 The naming/labeling syntax of files or documents must be short and simple (e.g., Product Catalogues).

12.5 All documents submitted electronically via e-mail must be clear and visible.

12.6 All proposals, documents, and late submissions after the due date will not be evaluated.

NB: NO HARD COPIES OR PHYSICAL SUBMISSIONS WILL BE ACCEPTED

13 TENDER PROGRAMME

The tender programme, as currently envisaged, incorporates the following key dates:

• Issue of tender documents:	Thursday, 07 July 2022
• Briefing Session	Thursday 21 July 2022
• Closing / submission Date:	Friday, 05 Aug 2022
• Estimate appointment date of successful tenderer:	30 August 2022

14 SUBMISSION OF PROPOSALS

10.1 All proposals are to be submitted electronically to tender@csir.co.za . No late proposals will be accepted. Responses submitted by companies must be signed by a person or persons duly authorised.

14.2 All emailed proposal submissions are to be subject referenced with the RFP number.

14.3 All emailed proposal submissions are to be subject referenced with the RFP number.

14.4 Proposals must consist of two parts, each of which must be sent in two separate emails with the following subject:

PART 1: Technical Proposal: RFP No. 3530-05-08-2022

PART 2: Pricing Proposal, B-BBEE, and other Mandatory Documentation: 3530-05-08-2022

14.5 The CSIR will award the contract to qualified tenderer(s)' whose proposal is determined to be the most advantageous to the CSIR, taking into consideration the technical (functional) solution, price, and B-BBEE.

14.6 Proposals submitted must be in any of the following file formats:

- PDF

15 DEADLINE FOR SUBMISSION

Proposals shall be submitted at the **email address** mentioned above no later than the closing date of ***05 Aug 2022*** during CSIR's business hours. The CSIR business hours are between 08h00 and 16h30.

Where a proposal is not received by the CSIR by the due date and stipulated place, it will be regarded as a late tender. Late tenders will not be considered.

16 AWARDING OF TENDERS

16.1 Awarding of tenders will be published on the National Treasury e-tender portal or the CSIR's tender website. No regret letters will be sent out.

17 EVALUATION PROCESS

17.1 Evaluation of proposals

17.2 All proposals will be evaluated by an evaluation team for functionality, price, and B-BBEE. Based on the results of the evaluation process and upon successful negotiations, the CSIR will approve the awarding of the contract to successful tenderers.

A two-phase evaluation process will be followed.

- The first phase includes the evaluation of **elimination** and **functionality criteria**.
- The second phase includes the evaluation of **price** and **B-BBEE** status.

Pricing Proposals will only be considered after the functionality phase has been adjudicated and accepted. Only proposals that achieved the specified minimum qualification scores for functionality will be evaluated further using the preference points system.

17.3 **Preference points system**

The 80/20 preference point system will be used where 80 points will be dedicated to pricing and 20 points to B-BBEE status.

18 PRICING PROPOSAL

18.1 The pricing proposal must be cross-referenced to the sections in the Technical Proposal. Any options offered must be clearly labelled. Separate pricing must be provided for each option offered to ensure that pricing comparisons are unambiguous.

18.2 Price needs to be provided in South African Rand (excl. VAT), with details on price elements that are subject to escalation and exchange rate fluctuations indicated.

18.3 Price should include additional cost elements such as freight, insurance until acceptance, duty where applicable.

18.4 Only firm prices* will be accepted during the tender validity period. Non–firm prices** (including prices subject to rates of exchange variations) will not be considered.

18.5 *Firm price is the price that is only subject to adjustments in accordance with the actual increase or decrease resulting from the change, imposition, or abolition of customs or excise duty and any other duty, levy, or tax which, in terms of a law or regulation is binding on the contractor and demonstrably has an influence on the price of any supplies, or the rendering costs of any service, for the execution of the contract.

18.6 **Non-firm price is all prices other than “firm” prices.

18.7 Payment will be according to the CSIR Payment Terms and Conditions.

18.8 The pricing proposal must be cross-referenced to the sections in the Technical Proposal. Any options offered must be clearly labelled. Separate pricing must be provided for each option offered to ensure that pricing comparisons are clear and unambiguous.

19 VALIDITY PERIOD OF PROPOSAL

19.1 Each proposal shall be valid for a minimum period of three (3) months calculated from the closing date.

20 APPOINTMENT OF SERVICE PROVIDER

20.1 The contract will be awarded to the tenderer who scores the highest total number of points during the evaluation process, except where the law permits otherwise.

20.2 Appointment as a successful service provider shall be subject to the parties agreeing to mutually acceptable contractual terms and conditions. In the event of the parties failing to reach such an agreement CSIR reserves the right to appoint an alternative supplier.

20.3 Awarding of contracts will be announced on the National Treasury website and no regret letters will be sent to unsuccessful bidders.

21 ENQUIRIES AND CONTACT WITH THE CSIR

Any enquiry regarding this RFP shall be submitted in writing to CSIR at **tender@csir.co.za** with “**RFP 3530-05-08-2022** Proposals are hereby invited for the supply of seasonal casual labour/temporary staffing solutions to the CSIR International Convention Centre as the subject.

Any other contact with CSIR personnel involved in this tender is not permitted during the RFP process other than as required through existing service arrangements or as requested by the CSIR as part of the RFP process.

22 MEDIUM OF COMMUNICATION

All documentation submitted in response to this RFP must be in English.

23 COST OF PROPOSAL

Tenderers are expected to fully acquaint themselves with the conditions, requirements, and specifications of this RFP before submitting proposals. Each tenderer assumes all risks for resource commitment and expenses, direct or indirect, of proposal preparation and participation throughout the RFP process. The CSIR is not responsible directly or indirectly for any costs incurred by tenderers.

24 CORRECTNESS OF RESPONSES

24.1 The tenderer must confirm satisfaction regarding the correctness and validity of their proposal and that all prices and rates quoted cover all the work/items specified in the RFP. The prices and rates quoted must cover all obligations under any resulting contract.

24.2 The tenderer accepts that any mistakes regarding prices and calculations will be at their own risk.

25 VERIFICATION OF DOCUMENTS

25.1 Tenderers should check the numbers of the pages to satisfy themselves that none are missing or duplicated. No liability will be accepted by the CSIR in regarding to anything arising

25.2 The pricing schedule and B-BBEE credentials should be submitted with the proposal, but as a separate document and no such information should be available in the technical proposal.

25.3 If a courier service company is being used for the delivery of the proposal document, the RFP description must be endorsed on the delivery note/courier packaging to ensure that documents are delivered to the tender box, by the stipulated due date.

26 SUB-CONTRACTING

26.1 A tenderer will not be awarded points for B-BBEE status level if it is indicated in the tender documents that such a tenderer intends sub-contracting more than 25% of the value of the contract to any other enterprise that does not qualify for at least the points that such a tenderer qualifies for unless the intended sub-contractor is an exempted micro-enterprise that has the capability and ability to execute the sub-contract.

26.2 A tenderer awarded a contract may not sub-contract more than 25% of the value of the contract to any other enterprise that does not have an equal or higher B-BBEE status level than the person concerned, unless the contract is sub-contracted to an exempted micro-enterprise that has the capability and ability to execute the sub-contract.

27 ADDITIONAL TERMS AND CONDITIONS

27.1 A tenderer shall not assume that information and/or documents supplied to CSIR, at any time before this request, are still available to CSIR, and shall consequently not make any reference to such information document in its response to this request.

27.2 Copies of any affiliations, memberships, and/or accreditations that support your submission must be included in the tender.

27.3 In case of the proposal from a joint venture, the following must be submitted together with the proposal:

27.3.2 Joint venture Agreement including the split of work signed by both parties.

27.3.3 The original or certified copy of the B-BBEE certificate of the joint venture.

27.3.4 The Tax Clearance Certificate of each joint venture member.

27.3.5 Proof of ownership/shareholder certificates/copies, and

27.3.6 Company registration certificates.

27.4 An omission to disclose material information, a factual inaccuracy, and/or misrepresentation of fact may result in the disqualification of a tender, or cancellation of any subsequent contract.

27.5 Failure to comply with any of the terms and conditions as set out in this document will invalidate the Proposal.

28 CSIR RESERVES THE RIGHT TO

28.1 Extend the closing date.

28.2 Verify any information contained in a proposal.

28.3 Request documentary proof regarding any tendering issue.

28.4 Give preference to locally manufactured goods.

28.5 Appoint one or more service providers, separately or jointly (whether or not they submitted a joint proposal).

28.6 Award this RFP as a whole or in part.

28.7 Cancel or withdraw this RFP as a whole or in part.

29 DISCLAIMER

This RFP is a request for proposals only and not an offer document. Answers to this RFP must not be construed as acceptance of an offer or imply the existence of a contract between the parties. By submission of its proposal, tenderers shall be deemed to have satisfied themselves with and to have accepted all Terms & Conditions of this RFP. The CSIR makes no representation, warranty, assurance, guarantee, or endorsements to the tenderer concerning the RFP, whether about its accuracy, completeness, or otherwise and the CSIR shall have no liability towards the tenderer or any other party in connection therewith.

ANNEXURE A DECLARATION BY TENDERER

Only tenderers who completed the declaration below will be considered for evaluation.

RFP No: 3530-05-08-2022 Proposals are hereby invited for the benchmarking of the Legal Risk Register.

I hereby undertake to render services described in the attached tender documents to CSIR in accordance with the requirements and task directives/proposal specifications stipulated in **RFP 3530-05-08-202** Proposals are hereby invited for the benchmarking of the Legal Risk Register. at the price/s quoted. My offer/s remains binding upon me and open for acceptance by the CSIR during the validity period indicated and calculated from the closing date of the proposal.

I confirm that I am satisfied with regards to the correctness and validity of my proposal; that the price(s) and rate(s) quoted cover all the services specified in the proposal documents; that the price(s) and rate(s) cover all my obligations and I accept that any mistakes regarding price(s) and rate(s) and calculations will be at my own risk.

I accept full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on me under this proposal as the principal liable for the due fulfilment of this proposal.

I declare that I have no participation in any collusive practices with any tenderer or any other person regarding this or any other proposal.

I accept that the CSIR may take appropriate actions, deemed necessary, should there be a conflict of interest or if this declaration proves to be false.

I confirm that I am duly authorised to sign this proposal.

NAME (PRINT) ………………………………….

CAPACITY ……………………………………….

SIGNATURE …………………………………….

NAME OF FIRM ……………………….……..

DATE ………………………………….

30 ANNEXURE B SCORING SHEET TO EVALUATE FUNCTIONALITY

Table 9: Scoring sheet for System Administration

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Company Experience	Company profile indicating the number of years they have been in existence in the service industry, on the scope in service 4.1, 4.2, or 4.3.	20	Less than 12 months	13 – 24 months	More than 24 months
Size of customer operations The service provider must have dealt with large organisations of at least 500 users.	At least three references (3) to be supplied. The total users of 500 will be determined across the largest 2 of the 3 references	10	Less than 250 users	250-499 users	More than 500 users
Customer references The number of customers where the scope of services has been delivered	At least one customer where the scope of the service has been delivered.	10	None	One customer	One customer
Monthly SLA performance achievement Meeting at least 99% of the performance criteria	The service provider must demonstrate their understanding of the reporting requirements by supplying sample reports.	20	Less than 50% of reports	50%-75% of all reports	More than 75% of reports

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Service Transition plan Covering the quality, practicality, and duration	A transition plan, covering timelines, responsibilities, and quality of delivery	20	No transition plan	Not all aspects covered	All aspects covered
System Administration	At least 2 CV's of staff covering the following skills, and >6 years of experience. • Linux Administrator (LPIC or CompTIA Linux+ or similar) • VMware (VCTA) • Any relevant vendor/storage certification • Cisco CCNA (R&S) or CCNP (R&S) • Cisco ACI • FortiGate NSE4	20	Falling short of experience and skills in more than 2 of the technologies	Falling short of experience and skills in 1-2 of the technologies	Falling short of experience and skills in none of the

Table 10: Scoring sheet for PostgreSQL database support and administration

Functional Factors	**Proof Required**	**Weighting**	**0 points**	**5 points**	**10 points**
Company Experience	Company profile indicating the number of years they have been in existence in the service industry, on the scope in service 4.1, 4.2, or 4.3.	20	Less than 12 months	13 – 24 months	More than 24 months
Size of customer operations The service provider must have dealt with large organisations of at least 500 users.	At least three references (3) to be supplied. The total users of 500 will be determined across the largest 2 of the 3 references	10	Less than 250 users	250-499 users	More than 500 users
Customer references The number of customers where the scope of services has been delivered	At least one customer where the scope of the service has been delivered.	10	None	One customer	One customer
Monthly SLA performance achievement Meeting at least 99% of the performance criteria	The service provider must demonstrate their understanding of the reporting requirements by supplying sample reports.	20	Less than 50% of reports	50%-75% of all reports	More than 75% of reports

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Service Transition plan Covering the quality, practicality, and duration	A transition plan, covering timelines, responsibilities, and quality of delivery	20	No transition plan	Not all aspects covered	All aspects covered
PostgreSQL database support and administration	• At least 2 CV's of staff covering the following skills, and >5 years of experience • Certified PostgreSQL DBA(CPSDBA) • PostgreSQL Associate Certification • Advanced PostgreSQL • OR similar • Linux Administrator (LPIC or CompTIA Linux+ or similar)	20	Falling short of experience and skills in more than 2 of the technologies	Falling short of experience and skills in 1-2 of the technologies	Falling short of experience and skills in none of the

Table 11: Scoring sheet for Information Security Operations

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Company Experience	Company profile indicating the number of years they have been in existence in the service industry, on the scope in service 4.1, 4.2, or 4.3.	20	Less than 12 months	13 – 24 months	More than 24 months
Size of customer operations The service provider must have dealt with large organisations of at least 500 users.	At least three references (3) to be supplied. The total users of 500 will be determined across the largest 2 of the 3 references	10	Less than 250 users	250-499 users	More than 500 users
Customer references The number of customers where the scope of services has been delivered	At least one customer where the scope of the service has been delivered.	10	None	One customer	One customer
Monthly SLA performance achievement Meeting at least 99% of the performance criteria	The service provider must demonstrate their understanding of the reporting requirements by supplying sample reports.	20	Less than 50% of reports	50%-75% of all reports	More than 75% of reports

Functional Factors	Proof Required	Weighting	0 points	5 points	10 points
Service Transition plan Covering the quality, practicality, and duration	A transition plan, covering timelines, responsibilities, and quality of delivery	20	No transition plan	Not all aspects covered	All aspects covered
Information security Operations	At least 2 CV's of staff covering the following skills, and >6 years of experience • An ICT related degree, or equivalent experience • Certified Information Systems Security Professional (CISSP) • CISA – Certified Information Systems Auditor (CISA) • CEH – Certified Ethical Hacker (CEH) • CISM – Certified Information Security Manager (CISM) • ISSAP – Information Systems Security Architecture Professional (ISSAP) ISSEP – Information Systems Security Engineering Professional (ISSEP)	20	Falling short of experience and skills in more than 2 of the technologies	Falling short of experience and skills in 1-2 of the technologies	Falling short of experience and skills in none of the

31 ANNEXURE C – SBD1

(To be completed by the supplier and submitted with tender)