**SUPPLY, INSTALLATION, CONFIGURATION AND SUPPORT OF THE ICT INFRASTRUCTURE AND APPLICATION PERFORMANCE MONITORING SOLUTION**

**ICT INFRASTRACTURE MONITORING (Switches, Routers, Servers etc.)**

| ***#*** | ***FUNCTIONAL REQUIREMENTS*** | ***Substantiating evidence and evidence reference to be completed by bidder****.*  *Evaluation per requirement: Each requirement indicated in the tables below must be completed and will be scored.* | ***Evidence reference***  *(to be completed by bidder)* |
| --- | --- | --- | --- |
|  | Automatically discovers switches on the SASSA network, categorize them as switches, and keep an inventory of all the switches discovered | Bidder to provide details explaining how this requirement is met with product documentation | *provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x* |
|  | Provide visibility into the status and availability of switch ports | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Actively monitor switch ports and quickly notifies operators whenever a switch port or the switch goes down. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Show which ports are blocked and which ones are forwarding by displaying their statuses on a spanning tree. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor port utilization and traffic with threshold alerts. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Detect potential broadcast storms, and proactively prevent them from occurring in the future. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Identify over and underutilized ports | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Get alerts when ports start discarding packets | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Have switch port mapping to quickly discover the list of devices connected to switch ports to gain visibility into the IP, MAC, status, and availability of ports | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Automatically discover and classify interfaces mapped to the core switch | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Reporting function that provides a detailed availability report of switches | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Network Configuration Backup (NCM) is also be required to backup switch configuration and perform change and compliance management | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | SNMP and ICMP monitoring required for both switches and routers as the switches are linked to the routers to determine whether a switch is down, or if the site is down | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Periodically monitors servers via SNMP and WMI protocols to ensure that they are up and running at their optimum performance level, 24x7 | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | The tool should provide event monitoring as well as reporting on performance, capacity and availability. |  |  |
|  | The tool, should provide various system performance monitoring features such as CPU monitoring, memory monitoring, Disk monitoring up to a minute interval. It should provide a graphical view of these metrics to monitor and measure server performance, in real-time. It should provide the ability to drill down to a particular time interval to understand more about the issue in order to guide necessary steps for resolution | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | The tool should offer out-of-the-box features such as server availability monitoring and performance metrics such as page read/write, processor queue length, free physical memory, disk I/O, process queue length through SNMP and WMI protocols. The tool should provide a view of availability of all physical and virtual servers 24x7 | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | The tool should provide a holistic view of the status of servers instantly and allow for creation of custom server monitoring dashboard such as Windows server monitoring dashboard, Linux server monitoring dashboard, server performance monitoring dashboard | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor IOPS (I/O) utilization   * Identify disk saturation | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor Memory utilization | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor network latency   * Identify network packet drops | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |

**APPLICATION AND DATABASE PERFROMANCE MANAGEMENT AND MONITORING**

| ***#*** | ***SERVICE FUNCTIONAL REQUIREMENTS*** | ***Substantiating evidence and evidence reference to be completed by bidder****.*  *Evaluation per requirement: Each requirement indicated in the tables below must be completed and will be scored.* | ***Evidence reference***  *(to be completed by bidder)* |
| --- | --- | --- | --- |
|  | Application and database performance and availability monitoring i.e. a user can access and transact on it. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Dashboard that visually shows the application landscape and the status of the individual components. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | capability to monitor user experience | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | The tool to advise when a specific Region or office is unable to access the application – thereby alerting SASSA that there could be other challenges being experienced. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | automatically detect performance problems and contain analytics to diagnose possible challenges or issues in the application or database | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | report total downtime in a specific period | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor various programming languages and frameworks. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | determine and detect patterns to enable it to alert when something is outside the pattern | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | analyse and predict user access and volumes / when the application is most busy etc. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor slow-running queries | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor database connections (logins and disconnects) | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor database capacity   * Forecast table space usage | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Monitor database backups | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Collect database logs. i.e. Alert log, Listener log | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Present alerts on critical issues in a dashboard | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Troubleshoot performance issues down to component / configuration item | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Identify whether there is over allocation or shortage of memory structures in the database | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |

**ICT USER AND ADMINISTRATOR MONITORING**

| ***#*** | ***SERVICE FUNCTIONAL REQUIREMENTS*** | ***Substantiating evidence and evidence reference to be completed by bidder****.*  *Evaluation per requirement: Each requirement indicated in the tables below must be completed and will be scored.* | ***Evidence reference***  *(to be completed by bidder)* |
| --- | --- | --- | --- |
|  | Solution must be capable of producing reports that monitor activities of ICT users and administrators and report on their activities within servers hosting services such as Active Directory, SQL databases, Oracle databases, Windows logon events, Linux OS logon events | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | should be user aware, i.e. identify the actual user of the source or destination, preferably through user accounts, such as Active Directory (AD), database accounts, (Windows and Linux) operating systems local accounts | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Perform database activity monitoring. The solution must be able to provide monitoring of administrator’s activities within several databases (Microsoft SQL & ORACLE) and provide regular reports of all the changes or modification by the administrators on what was modified, when, and by who | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | perform real-time monitoring of events/data generated by workstations, servers, databases and applications | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Combine data events from disparate sources to assist with the identification of any suspicious activities and SASSA policy violation on any ICT systems monitored. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | contain a correlation engine to identify and detect patterns across the ICT monitored systems with basic predefined correlation rules available at set-up to start analysing and correlating activity out-of-the-box that reduces false-positives automatically, detects authentication failures and operational events in real-time without the need to specify particular device types | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Perform behaviour profiling to identify anomalies and deviations from normal behaviour. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Provide customizable and consolidated reporting capabilities, from detailed daily reports to monthly reports and be capable of exporting reports in various formats. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | guarantee delivery of events to the log management system and that no events will get lost if the log management system is unavailable, the solution must not drop in coming events | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Provide online options to reduce log events at the source by aggregating the log events. Aggregation must be flexible in which normalized fields can be aggregated and provide the ability to aggregate in batches or time windows | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Provide compliance auditing, alerting and reporting for governance requirements with ease. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Should be able to natively integrate with existing authentication directories to import context related to users and roles which will then correlate and attribute every event to an actual user, regardless of the event source and be able to alert or report on any activity for identities not automatically synchronized with authentication directories. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Should be able to define whitelist / blacklists that can be used as inclusion or exemption during the correlation process. The correlation engine should utilize dynamic lists to provide important information such as shared user monitoring, session tracking, attack history and privileged system access. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Should be able to provide the ability to import context and keep an inventory of all data as it relates to assets like hostname, IP & MAC address, business purpose, owner, and other business-related data. The asset inventory must be able to integrate with other network monitoring/management solutions to keep asset information up to date. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Capable of allowing the restoration of a year's worth of historical log files to perform complex pattern searches and reporting against big sources of data in a short period of time. The entire process from restoring the data to reporting results must take less than two days. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | ability to visually represent event data into a dynamically updated graph to assist ICT in determining the spread of attacks and pinpoint the original attacker during incident response and remediation | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | produce daily reports of all activities within the network for a 24-hour period covering aspects such as: All user/administrator security correlated events- failed logon and locked out accounts including service accounts, multiple host logging from single AD account, brute force attempts from a single or multiple source | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Produce weekly reports of all activities within core servers without service degradation due to the report generation such as: Weekly Active Directory activities report. Weekly Linux server login report. Weekly Windows server logon activities. Weekly SQL and Oracle databases activity reports | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |
|  | Produce alerts for the following incidents: Active Directory group policy changes, local administrator modifications and use (successful and failed login), Security Group membership changes and (user, administrator & services) account login events. | Bidder to provide details explaining how this requirement is met with product documentation | provide unique reference to locate substantiating evidence in the bid response e.g. see Annex x, section x page x |