KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

END TO END MONITORING SOLUTION

TECHNICAL SPECIFICATIONS

1.0 EXECUTIVE SUMMARY

1.1 Overview

The Authority delivers its mandate of tax collection & accounting, customs and border control as well as trade facilitation through a wide range of online systems and integration services. Technology Department supports Authority's online services hosted in its Data Centres and those hosted in the Internet cloud by managing Authority's network infrastructure, Data Centre facilities and IT equipment and applications. These require 24/7 monitoring and maintenance to reduce the down-time and thus increase availability.

Currently monitoring is done using a mix of proprietary and free open-source automated tools like *Nagios/NagVis, Cacti*, *Grafana*, *Zabbix*, *Elastic Stack (ELK)*, *VMware vROPs*, *ObiGuard DCIM*, or *IBM NetCool*, The above tools do not provide comprehensive observability of our services and supporting infrastructure. KRA is seeking to enhance the monitoring process to address these shortcomings.

1.2 Solution Brief

In order to meet the objectives defined above, KRA is seeking to acquire an End to End Monitoring Solution that will be used as the main platform for service monitoring and availability reporting. The full stack observability solution shall provide complete observability, visibility into all layers of our technology stack, from the user-facing front-end to the back-end infrastructure, by collecting and correlating telemetry data (**logs**, **metrics**, and **traces**) from various sources. This holistic approach shall allow the Authority to understand how different components interact, proactively identify performance issues and security threats, and resolve problems quickly, ultimately improving system resilience and the end-user experience. The solution will be required to provide the following:

a) Compute and Storage Infrastructure Monitoring

Infrastructure monitoring capabilities that will be used to monitor compute and storage infrastructure from a variety of hardware and storage vendors such as Dell, Huawei, Hitachi, HP or Pure-Storage.

b) Network Infrastructure Monitoring

Best in market network monitoring capabilities that will be used to monitor KRA network infrastructure from different network and security vendors such as Check-Point, F5, Cisco and Huawei or network technologies such as MPLS and Software-Defined DC network solutions, LAN, MAN, WAN or SAN.

c) Application Performance Management

Application Performance Management capabilities that will enable Full Stack Observability (Logging, Metrics and Tracing) for KRA applications as well as end user experience monitoring.

d) Business Metrics Monitoring

The ability to integrate with business systems reporting databases and provide management dashboards that indicate performance of business metrics, revenue statistics, trends and proactive business intelligence pointers to performance of the systems**.**

2.0 IMPLEMENTATION APPROACH

For the purpose of effective implementation, the above requirements have been regrouped into the following three (3) domain areas for the purpose of procurement;

a) Compute and Storage Infrastructure Monitoring Solution.

b) Network Infrastructure Monitoring Solution

c) Application Performance Management and Business Metrics Monitoring Solution

The effectiveness of implementation of monitoring systems requires grouping and scoping of related components as per domain area. KRA prefers that a single solution that provides end-to-end monitoring and reporting via a single management plane.

However, in case there is not a single turn-key solution, different components may be implemented independently as captured above so as to provide end-to-end service monitoring. The bidder will be required to ensure that the components are seamlessly integrated so as to provide the best user experience for the end users

3.0 <u>INSTRUCTIONS TO BIDDERS</u>

1. All clause by clause requirements provided under Table 4.1, 4.2 and 4.3 are **mandatory**.
2. Bidders should provide a substantive response to every requirement clause in Table 4.1, 4.2 and 4.3, clearly detailing how their proposed solution meets this requirement.
3. Successful bidders will be required to present a demo showcasing the features of the end to end monitoring solution as part of the evaluation process. The specific

requirements and evaluation criteria will be shared with the bidders as part of the technical evaluation process.

4. The evaluation will be scored as shown in the table below:

A. MANDATORY REQUIREMENTS

No	Evaluation Criteria	Requirement
1.	The bidder must be an authorized supplier of the OEM solution. A valid manufacturer authorization form must be provided as proof.	Mandatory

B. VENDOR EVALUATION CRITERIA

No	Requirement	Evaluation Criteria	Bidders' response	Max Score
1.	**Vendor Experience** Demonstrated experience through previous execution of Two (2) end to end monitoring Solution projects of similar magnitude within the last five (5) years.	**3 Marks for each project** Bidder MUST submit recommendation letters/certificate of completion for each project cited which should be supported by corresponding copies of signed contract(s) **or** copies of LSOs. The recommendation letters should have: i Contacts: postal address, telephone and email of the contact person. ii A brief description of the project delivered 1.5 Marks LSO contract 1.5 Marks recommendation letter		6

2.	**Technical staff Qualifications.** Three (3) Technical staff (one of them being a project manager) with the following academic and professional qualifications: 1) Academic Qualifications: A minimum of Relevant University Degree or Diploma. (Computer Science, IT, electronics or related fields) 2) Professional Qualifications: Valid end to end monitoring solution produce Certification. 3) Project Management qualification for team lead: Valid Project Management certification	**4 Marks for each Qualified Staff** Degree (2 Marks) Diploma (1 Mark) Valid end to end monitoring professional certification/Project Management Certification) (2 Marks) Bidders MUST attach the CV of each staff supported by copies of Academic and professional certificates.(		12
3.	**Staff Relevant experience** Each Qualified staff (refer to clause 2 above) should have experience in implementation, support and maintenance of end to end monitoring Software Solutions or experience in project management for the team lead/project manager	Staff Relevant experience • Over 3 years– 3 Marks for each qualified staff • 2-3 years – 2 Marks for each qualified staff • 1-2 years – 1 Mark for each qualified staff • Less than 1 Year - 0 Marks Note: Bidders MUST submit a copy of the CV for each staff clearly indicating the years of experience		9

		in implementing and supporting end to end monitoring solutions and the sites supported or the years of experience in project management for the implementation of a monitoring solutions.		
4.	**Technical Approach and Methodology** Bidder MUST demonstrate a good and clear understanding of KRA's Requirements. They MUST propose an approach/methodology and a work plan to capture the requirements and ensure they are comprehensively addressed in the proposed solution	Bidders to demonstrate/provide evidence of a clear and detailed understanding of the solution, including: a) Project delivery Approach/Methodology for implementation and support of the solution – 1.5 Marks b) Work plan (Bidder MUST provide a three (3) year work plan for implementation and support for the solution - 1.5 Marks		3
	Total Score			**30**
	Cut-off score is 22.5 marks			

TECHNICAL SPECIFICATIONS

Instructions to Bidders:

1. Bidders MUST complete the Table below in the format provided.
2. Bids MUST meet all mandatory (MUST) requirements in the Tables below in order to be considered for further evaluation.
3. Bidders MUST provide a substantial response or clear commitment to meeting the requirements for all features irrespective of any attached technical documents in the table format (bidders Response) below. Use of Yes, No, tick, compliant, blank spaces etc. will be considered non-responsive.
4. Bidders who do not comply with any of the below requirements will NOT be considered for further evaluation

NB: Bidders who shall meet the cut-off score for the technical and demonstration requirements shall be evaluated at the financial evaluation stage.

4.1 Compute and Storage Infrastructure Monitoring Solution

The table below specifies the requirements that shall guide in procuring monitoring solution in the area of **Compute** (processing and memory) and **Storage** (local or attached SAN, NAS and block disk storage) resources.

Table 1: *Compute and Storage Infrastructure Monitoring Solution*

SN	Feature	Minimum Requirements	Bidder Response
1.	International recognition.	Mature internationally recognized brand, in existence for at least 5 years (bidder must specify brand, model and series). The solution components MUST NOT be a product that is reaching end of life in 5 years' time. The monitoring solution should be a leader in the Gartner Magic Quadrant (or its equivalent) for Infrastructure Observability	
2.	Deployment	The solution should be able to be deployed both on-premise and in cloud. This shall offer flexibility to the customer to deploy in preferred environment.	
3.	Host Monitoring	The solution should be able to monitor, identify and remediate issues in enterprise infrastructure such as on-premise hosts, containers, and virtual machines and cloud services.	
4.	Monitored Items	The solution shall monitor the following components; - Hardware components - Operating System	
5.	Container and Kubernetes Monitoring	The solutions must support deployment and monitoring of containerised cloud native workloads. The solutions must be able to be installed in Kubernetes.	
6.	Identity and access management	The solution must support configuration of identity and access management via LDAP and SAML for SSO. The solutions	

		must support 2 factor authentication	
7.	Machine Learning and AI Support	The solution must provide out of the box support for use of machine learning and artificial intelligence models. The solution must provide anomaly detection, predictive analytics, pattern recognition, automated remediation among others.	
8.	eBPF Support	The solution must support eBPF technology to enable data collection and observability from kernel space.	
9.	Open Telemetry Support	The end to end solution must be compatible with the Open Telemetry standard and integrate seamlessly with other solutions and products that use the Open Telemetry standard/ specification.	
10.	Incident Management	The solution should be able to measure service performance by configuring Service Level Objectives and Service Level Indicators	
11.	Monitored metrics	The solution shall support monitoring of the following compute metrics: a) CPU Usage is a strong indicator of the health of both the server and the network. b) Memory - the solution should track used and available memory, cached memory and alert on thresholds c) Disk usage and IO - the solutions shall monitor disk volume usage and report per threshold set as well as input/output operation rates and latency to predicatively point out bottlenecks / error-rates. d) Network traffic (load) – solution shall monitor bandwidth both inbound (received -Rx) and outbound (transmitted -Tx) data transfers volumes in bits per second. It should also monitor latency, up-time and down-times. This shall apply to all interfaces of the servers or SAN Storage Controllers or Disk Array components – Ethernet, Fibre-Channel,	

		iSCSI or Infiniband interfaces. e) Infrastructure health – the solution should be able to provide overall operation health status of the entire data center infrastructure. The following metrics should be provided: - Uptime/Downtime - General systems availability. f) Other Custom metrics for example device metadata and inventory information to track obsolescence, maintainability etc.	
12. `	Configuration	The solution should support agent and agentless configuration which use standard network protocols – SNMP, MIBS, ICMP, PING, SSH etc. It should be deployed centrally and used to manage federated [distributed] service nodes (servers, storage controllers and other compute resources).	
13.	Deployment Mode	The solution must be deployed in high availability so as to ensure redundancy of critical components such as the data storage servers. The solution must also support horizontal scaling to allow addition of processing nodes so as to improve performance when necessary	
14.	Centralized Management	It should be deployed centrally and used to manage federated [distributed] service nodes (servers, storage controllers and other compute resources), in both physical, virtual and containerised environments.	
15.	Management Portal	The solution shall provide an interface (both web-based and console support) for configuration of monitored components and customising dashboards / thresholds. Automatic device discovery features shall be included.	
16.	Log shipping	The solution must support shipping of logs from the server or VM to the Infrastructure monitoring solution, through agents	

17.	Compatibility to existing OS or deployed platforms	The solution should be compatible to Authorities platforms; - Oracle OVM Hypervisor, VMware ESxi Hypervisor, Linux KVM Hypervisor, Dell, Oracle, IBM, HP, Cisco and Huawei Hardware Micro-code as well as Linux and Microsoft Windows Servers Operating Systems. The solution shall also be compatible to application virtualisation and containerisation.	
18.	Capacity and Scalability	The solution shall have capacity to support the following; a) At least 100 physical servers, including engineered IBM and Oracle Exa-Data machines b) At least 600 virtual machines (Servers, application containers and VDI). c) At least 5 different SAN storage systems each with over 500 TB of Data, including enterprise backup storage. The solution shall be able to scale up to double the initial capacity at implementation. *Note*: that the user base for internal servers is over 10,000 and external tax system servers exceed 5,000,000 users at peak.	
19.	Visibility Dashboards (flexible and customisable)	The solutions shall provide the following visibility / observability features; a) Online web based dash-boards – visual interactive [support drill-down] screen displays compatible with common Web browsers (Mozilla FireFox, Apple Safari, Brave, Google Chrome, Opera, Chromium and Microsoft Edge/Internet Explorer) that can be rendered over PC, Laptop, and Hand-held devices (Mobile phone & Tablets). The dashboard should support visual logical topology, graphs, table/numeric data and other visual aids for	

		performance visibility/observability. b) Historical review – the solution should support play-back of past event / graphical representation of service status at selected past time period. c) Logs View – the solution should provide real time streaming view of logs as they are ingested into the monitoring platform.	
20.	External Integration, alerting and reporting	a) E-Mail Alerting – automated mail alerting mechanism, and capable of integrating with our mail service. b) Text (SMS) alerting and integration to social media channels being added advantage. c) Logging and reporting – the solution shall support logging of performances states and support flexible generation of availability, performance reports logs analytics. d) Integration with external log / data management and analytics solution is an advantage.	
21.	Predictive failure / bottleneck detection	The solution shall support predictive failure features to provide early warning of component failures or bottlenecks.	
22.	Security and Network overheads	The solutions shall support standard network and server security features (TLS, SSL) to avoid exposing monitored server information or user data. Minimum audit logging and traffic overhead should be of added advantage.	
23.	Upgrade / scalability and security patching	The solution shall support easy upgrade and security patching /fixes to enhance stability and compatibility to future installed monitored components [fit-for-future].	
24.	User Management	The solution shall provide hierarchical usage management with user segregated roles (Administration - Read/Write, Other role users – Read/only and monitored component based user view isolations)	

25.	Training/Support and technical documentation	The solution shall come with comprehensive technical documentation for both usage (user manuals) and technical configuration (admin manuals). Training options shall be included in implementation.	
26.	Licence	The solution shall comply to standard licencing scheme based on either of the following; - Per CPU core of hosting server - Per Memory Unit on hosting service e.g. per 64GB. - Perpetual licence All software features must be licensed from day one	
27.	Support / Warranty	The solution should come with at least one (1) year post deployment warranty and three (3) year maintenance support.	
28.	Implementation services	The bidder should provide implementation services of the solution.	

4.2 Network Infrastructure Monitoring Solution

Table 2: *Network Infrastructure Monitoring Solution*

SN	Feature	Minimum Requirements	Bidder Response
1.	International recognition.	Mature internationally recognized brand, in existence for at least 5 years (bidder must specify brand, model and series). The solution components MUST NOT be a product that is reaching end of life in 5 years' time. The solution should be a leader in the Gartner Magic Quadrant (or its equivalent) for Network Infrastructure Monitoring	
2.	Deployment	The solution should be able to be deployed both on-premise and in cloud. This shall offer flexibility to the customer to deploy in preferred environment.	
3.	Monitoring Methodology	The solution must provide monitoring solutions that not only capture data but also provide detailed packet and	

		decode analysis for a wide range of industry standard protocols and applications, providing detailed decoding of well-known, complex, custom and Web-based applications protocols, and services.	
4.	Protocol Analysis	The solution must provide protocol analysis capability, single viewable page: • Summary of all packets or messages captured or traced • Detailed, full decode of a selected packet or message in plain English • Detailed, full decode of selected packet or message in Hexadecimal	
5.	Protocol Decode	The solution must provide protocol decode capabilities: • Display additional TCP-specific information such as TCP window size, info bytes, bytes in flight, etc. • Display additional RTP-specific information such as RTP time delta, packet delta, packet lengths, etc. • Display additional MDF-specific information such as latency (time delta), gap in sequence number, etc. This data should be provided in an easy to analyze graphical format along with a summary of all captured packets and Hex or plain text formats in one single display.	
6.	Container and Kubernetes Monitoring	The solutions must support deployment and monitoring of containerised cloud native workloads. The solutions must be able to be installed in Kubernetes.	
7.	Identity and access management	The solution must support configuration of identity and access management via LDAP and SAML for SSO. The solutions must support 2 factor authentication	
8.	Machine Learning and AI Support	The solution must provide out of the box support for use of machine learning and artificial intelligence	

		models. The solution must provide anomaly detection, predictive analytics, pattern recognition, automated remediation among others.	
9.	eBPF Support	The solution must support eBPF technology to enable data collection and observability from kernel space.	
10.	Open Telemetry Support	The end to end solution must be compatible with the Open Telemetry standard and integrate seamlessly with other solutions and products that use the Open Telemetry standard/ specification.	
11.	Incident Management	The solution should be able to measure service performance by configuring Service Level Objectives and Service Level Indicators	
12.	Monitored metrics	a) Device Compute metrics – CPU usage and memory usage. b) Network Ports performance – uptime/downtime of ports, network traffic received in (Rx) and transmitted out (Tx). c) Network latency – and quality of PING between data source ports and user access points or across logical partitioning of the topology; - LAN Level - WAN Level - Internet / KIXP Level. d) Transmission Error detection and performance – Quality of Service across node, per payload protocols or content compression – FTP Data, HTTPS, HTTP, PDF, PNG, FIG, HTML, XML, CSS, JSON etc. e) Traffic usage by protocol – to support monitoring of different payloads including IP-Telephony voice. f) Bandwidth monitoring – to display bandwidth utilization of the links. 8) Other Custom metrics for example	

		network device metadata and inventory information to track obsolescence, maintainability and device deployed location etc.	
13.	Configuration	The solution should support agentless configuration which use standard network protocols – SNMP, MIBS, ICMP, PING, SSH etc that do not require installation of software on the monitored device.	
14.	Source of Data	The Solution must operate at line-rate without packet loss. The solution must support the following packet data aggregation and replication profiles: One-to-One, One-to-Many, Many-to-One & Many-to-Many	
15.	Deployment Mode	The solution must be deployed in high availability so as to ensure redundancy of critical components such as the data storage servers. The solution must also support horizontal scaling to allow addition of processing nodes so as to improve performance when necessary	
16.	Deep Packet Inspection	The solution must be capable of Deep Packet Inspection (DPI) with up to Layer 7 monitoring that includes advanced application classification capabilities, allowing full visibility.	
17.	Centralized Management	It should be deployed centrally and used to manage federated [distributed] service nodes (switches, routers, access points, etc).	
18.	Management Portal	The solution shall provide an interface (both web-based and console support) for configuration of monitored components and customising dashboards / thresholds. Automatic device discovery features shall be included.	
19.	Compatibility to existing IOS or	The solution should be compatible to Authorities network landscape; -	

	deployed platforms	Current IOS of Cisco, Huawei, F5, CheckPoint, Brocade, D-Link and virtualised Software Defined Network (SDLAN, SDWAN)	
20.	Capacity and Scalability	The solution shall have capacity to support the following; a) Over 150 Wide Area Network (WAN) nodes b) Over 200 Local Area (LAN) nodes / access points per site for over 150 WAN nodes .. Wired and Wireless. c) Over 2 Internet gateways (of at least 2 Gbps) d) Over 100 Data Centre tiered nodes (Core, Distribution and Access layers) The solution shall be able to scale to up to twice the initial capacity at implementation. *Note*: that the user base for internal network is over 10,000 and external taxpayer facing network exceed 5,000,000 users at peak.	
21.	Visibility Dashboards (Flexible and customisable)	The solutions shall provide the following visibility / observability features; a) Online web based dash-boards – visual interactive [support drill-down] screen displays compatible with common Web browsers (Mozilla FireFox, Apple Safari, Brave, Google Chrome, Opera, Chromium and Microsoft Edge/Internet Explorer) that can be rendered over PC, Laptop, and Hand-held devices (Mobile phone & Tablets). The dashboard should support visual logical network topology, graphs, table/numeric data and other visual aids for performance visibility/observability. b) Historical review – the solution should support play-back of past event / graphical representation of service status at selected past time	

		period for diagnostic and root-cause analysis.	
22.	External integration, alerting and reporting	a) E-Mail Alerting – automated mail alerting mechanism, and able to integrate to our mail service. b) Text (SMS) alerting and integration to social media channels being added advantage. c) Logging and reporting – the solution shall support logging of performances states and support flexible generation of availability, performance reports logs analytics. d) Integration with external log / data management and analytics solution is an advantage.	
23.	Predictive failure / bottleneck detection	The solution shall support predictive network or device failure features to provide early warning of component failures or bottlenecks.	
24.	Security and Network overheads	a) The solutions shall support standard network and server security features (TLS, SSL) to avoid exposing monitored server information or user data. b) Minimum audit logging and traffic overhead should be of added advantage.	
25.	KPI Monitoring	The solution must combine health status KPIs, alarms and intelligent early warnings in a single, service-focused dashboard and view.	
26.	Service Dashboards	The solution must include intuitive workflows that provide business-specific and protocol-specific monitoring that allows our users to analyze relevant metrics and KPIs in order to triage application/protocol, server, and overall network performance degradation that are affecting our subscribers' experiences in the network.	
27.	Session Tracing	The solution must allow drill down from dashboards to a session tracing/analysis application, and to that sessions' related packet decode in 4	

		clicks or less, all from within one window and workflow. Please describe this workflow within your solution, detailing which applications, tools and logins are required.	
28.	Upgrade / scalability and security patching	The solution shall support easy upgrade and security patching /fixes to enhance stability and compatibility to future installed monitored components [fit-for-future].	
29.	User Management	The solution shall provide role based access management with user segregated roles (Network Administration - Read/Write, Other role users – Read/only and monitored component based user view isolations)	
30.	Reporting Services	The solution should provide network availability and capacity reports, including; *Availability*: Actual uptime vs. SLA targets, Incident logs for root-cause analysis (RCA). *Capacity*: Current capacity usage, Forecasted growth based on trends, indication for scaling, optimization, or resource planning upgrades	
31.	Training/Support and technical documentation	The solution shall come with comprehensive technical documentation for both usage (user manuals) and technical configuration (admin manuals). Training shall be included in implementation.	
32.	Licence and Support / Warranty	The solution shall comply to standard licencing scheme based on either of the following; - Per CPU core of hosting server - Per Memory Unit on hosting service e.g. per 64GB. - Perpetual licence All software features must be licensed from day one	

33.	Support / Warranty	The solution should come with at least one(1) year post deployment warranty and three (3) year maintenance support.	
34.	Implementation services	The OEM should provide implementation services of the solution.	

4.3 Application Performance Management and Business Metrics Monitoring Solution

Table 3: *Application Performance Management and Business Metrics Monitoring Solution*

SN	Feature	Minimum Requirements	Bidder Response
1.	International recognition.	Mature internationally recognized brand, in existence for at least 5 years (bidder must specify brand, model and series). The solution components MUST NOT be a product that is reaching end of life in 5 years' time. The solution should be a leader in the Gartner Magic Quadrant (or its equivalent) for Application Performance Management and Observability	
2.	Deployment	The solution should be able to be deployed both on premise and in cloud. This shall offer flexibility to the customer to deploy in preferred environment.	
3.	Container and Kubernetes Monitoring	The solutions must support deployment and monitoring of containerised cloud native workloads. The solutions must be able to be installed in Kubernetes. The solution must also be able to monitor standalone container images running via docker-compose	
4.	Identity and access management	The solution must support configuration of identity and access management via LDAP and SAML for SSO. The solutions must support 2 factor authentication	
5.	Machine Learning and AI Support	The solution must provide out of the box support for use of machine learning and artificial intelligence models. The solution must provide anomaly detection, predictive analytics, pattern recognition,	

		automated remediation through agents, among others.	
6.	eBPF Support	The solution must support eBPF technology to enable data collection and observability from kernel space.	
7.	Open Telemetry Support	The end to end solution must be compatible with the Open Telemetry standard and integrate seamlessly with other solutions and products that use the Open Telemetry standard/ specification.	
8.	Incident Management	The solution should be able to measure service performance by configuring Service Level Objectives and Service Level Indicators	
9.	Correlation	The solution must be able to correlate logs, metrics and traces so as to enable root cause analysis of incidents and problems. The solution should be able to correlate telemetry data from servers, storage, network and observability metrics in order to identify root causes of performance issues.	
10.	Logs Storage	The solution should provide a platform for storage of application logs using a scalable storage solution that provides fast searching of textual data through indexing or provides columnar based storage for quick retrieval and aggregation of log data.	
11.	Monitored metrics	The solutions should monitor; a) Memory and Processor Resources used by monitored applications. b) Number of sessions used (*Established*, *Failed* or *Waiting*) by monitored application software / service component. c) Numeric business data e.g. number of transaction per service, revenue figures or other data extracted from the logs or database. d) Uptime/downtime or state of service end-point e) Service latency / User experience simulation of user requests/responses and message queue time or error rates.	
12.	Configuration	The solution should support both Agent and Agentless configuration which use	

		standard network protocols – SNMP, MIBS, ICMP, PING, SSH etc that do not require installation of software on the monitored device.	
13.	Deployment Mode	The solution must be deployed in high availability so as to ensure redundancy of critical components such as the data storage servers. The solution must also support horizontal scaling to allow addition of processing nodes so as to improve performance when necessary	
14.	Centralized Management	It should be deployed centrally and used to manage hosted services in both physical, virtual and containerised environments.	
15.	Management Portal	The solution shall provide an interface (both web-based and console support) for configuration of monitored components and customising dashboards / thresholds. Automatic device discovery features shall be included.	
16.	End User Experience Monitoring	The solution must provide the ability to carry out end-user and mobile device monitoring of applications so as to monitor user experience.	
17.	Synthetic Monitoring	The solution must support synthetic monitoring to enable simulation of end user traffic.	
18.	End User Monitoring Metrics	The solution must monitor Core Web Vitals and provide a dashboard showing performance of the following Core Web Vitals (CWV) metrics: a. Largest Contentful Paint b. Interaction to Next Paint c. Cumulative Layout Shift	
19.	Continuous Profiling	The solution must provide capability to carry out continuous profiling of application services and operating systems (cpu, memory, disk and network) as follows: - At least Java 1.7 (SE 7) - At least Python 3 - At least Postgres 12 - At least RHEL 8 - At least Oracle 12c	

20.	Profiling Visualizations	The solution must provide a dashboard for continuous profiling that displays profiled data using a flame graph.	
21.	Application Runtime Support	The solution must support integration with following application runtimes; • At least Java 1.7 (SE 7) • At least PHP 7 • At least Python 2.7	
22.	Application Instrumentation	The solution must support instrumentation of applications through all of the following: • Manually instrumentation via agents loaded at server startup • Auto-instrumentation via agents that can be loaded after application startup • Instrumentation at code level via application libraries.	
23.	Root Cause Analysis	The solution must provide a capability to analyse thread dumps, heap dumps and garbage collection logs as part of root-cause analysis and provide dashboards and detailed results pointing to potential solutions	
24.	Webserver Support	The solution must support the following Webservers: • At least Tomcat 7 • At least Jboss AS 7/ Jboss EAP 6 • At least Weblogic 12	
25.	Compatibility to existing OS or deployed platforms	The solution should be compatible to Authorities platforms; - Oracle OVM Hypervisor, VMware ESxi Hypervisor, Linux KVM Hypervisor, Dell, Oracle, IBM, HP, Cisco and Huawei Hardware Micro-code as well as Linux and Microsoft Windows Servers Operating Systems. The solution shall also be compatible to application virtualisation and containerisation.	
26.	Capacity and Scalability	The solution shall have the capacity to support the following tiers of application / software platforms; a) Over 100 Databases (different RDBMS,	

		including NoSQL) b) Over 200 Java based containers (Web and Application servers) and other proprietary Enterprise Resource Planning (ERP) software, c) Over 10 flavours of Operating systems – Linux and Microsoft Windows. d) Over 50 critical business systems (In-house developed and off-shelf) software accessed internally (KRA Wired and VPN Network as well as over the Internet). e) Over 5 collaboration (Mail) and Work-flow software platform. *Note*: that the user base for internal software is over 10,000 and external tax system exceed 5,000,000 users at peak.	
27.	Visibility Dashboards (Flexible and customisable)	The solutions shall provide the following visibility / observability features; a) Online web based dash-boards – visual interactive [support drill-down] screen displays compatible with common Web browsers (Mozilla FireFox, Apple Safari, Brave, Google Chrome, Opera, Chromium and Microsoft Edge/Internet Explorer) that can be rendered over PC, Laptop, and Hand-held devices (Mobile phone & Tablets). The dashboard should support visual logical network topology, graphs, table/numeric data and other visual aids for performance visibility/observability. b) Historical review – the solution should support play-back of past event / graphical representation of service status at selected past time period for diagnostic and root-cause analysis. c) Logs View – the solution should provide real time streaming view of logs as they are ingested into the monitoring platform.	
28.	Reporting Services	The solution should provide application platform availability and capacity reports, including; *Availability*: Actual uptime vs. SLA targets, Incident logs for root-cause analysis (RCA).	

		Capacity: Current capacity usage, Forecasted growth based on trends, indication for scaling, optimization, or resource planning upgrades	
29.	External integration, alerting and reporting	a) E-Mail Alerting – automated mail alerting mechanism and can intergrate to our mail service. b) Text (SMS) alerting and integration to social media channels being added advantage. c) Logging and reporting – the solution shall support logging of performances states and support flexible generation of availability, performance reports logs analytics. d) Integration with external log / data management and analytics solution is an advantage.	
30.	Business Analytics	The solution must provide a functionality to monitor critical business indicators and provide alerts and dashboards for the same	
31.	Predictive failure / bottleneck detection	The solution shall provide support for predictive application failure detection to provide early warning of component failures or bottlenecks.	
32.	Security and Network overheads	The solutions shall support standard network and server security features (TLS, SSL) to avoid exposing monitored server information or user data. Minimum audit logging and traffic overhead should be of added advantage.	
33.	Upgrade / scalability and security patching	The solution shall support easy upgrade and security patching /fixes to enhance stability and compatibility to future installed monitored components [fit-for-future].	
34.	User Management	The solution shall provide role based access management with user segregated roles (System Administration - Read/Write, Other role users – Read/only and monitored component based user view isolations)	
35.	Training/Support and technical	The solution shall come with comprehensive technical documentation	

	documentation	for both usage (user manuals) and technical configuration (admin manuals). Training options shall be included in implementation.	
36.	Licencing	The solution shall comply to standard licencing scheme based on either of the following; - Per CPU core of hosting server - Per Memory Unit on hosting service e.g per 64GB. - Perpetual licence All software features must be licensed from day one	
37.	Support / Warranty	The solution should come with at least one(1) year post deployment warranty and three (3) year maintenance support.	
38.	Implementation services	The OEM should provide implementation services of the solution.	

4.4 DEMONSTRATION OF SOLUTION

A. REQUEST FOR DEMONSTRATION

Bidders are required to deliver a comprehensive demonstration of their proposed End to End Monitoring Solution as part of the evaluation process. This demonstration will be critical in assessing the capabilities and effectiveness of the monitoring solution tailored to meet the Authority's requirements.

B. DEMONSTRATION SCHEDULE

1. The demonstration should be scheduled at a mutually agreed time within four weeks after the submission of the bid.
2. Bidders should allocate sufficient time to cover all aspects of the solution thoroughly, ideally from one to two hours, allowing for questions and interactive discussions.

C. KEY FOCUS AREAS FOR DEMONSTRATION

Product Capability	Description (What It Must Include)	Score
Comprehensive Integration	Show how the solution integrates with existing systems and supports a full stack observability model across compute, storage, network, and application layers.	2

Monitoring Capabilities	Demonstrate the functionalities for monitoring compute and storage infrastructure, including hardware, operating systems, and VM/container monitoring. Showcase network infrastructure monitoring features, highlighting protocol analysis and performance metrics. Present application performance management capabilities, showing how to monitor application health and user experience.	6
User Interface and Dashboards	Provide a live walkthrough of user interfaces, including customizable dashboards and reporting features. Highlight the ease of use, flexibility, and responsiveness of the interface for monitoring real-time data.	4
Event and Incident Management	Illustrate the event logging, alerting mechanisms, and incident management workflows. Show how predictive failure detection and anomaly detection features work in real-time scenarios.	4
Machine Learning and AI Capabilities	Demonstrate the solution's support for machine learning and AI, particularly in terms of predictive analytics, automated remediation, and anomaly detection.	2
Scalability and Cloud Integration	Highlight the scalability of the solution and the options for deployment in both on-premise and cloud environments. Explain how the solution can scale to accommodate future growth requirements.	2
Total Score = 20 **Cut-off Score = 16**		**20**

5.0 PRICE SCHEDULES

The price schedule should cost all items in the scope of work and the minimum contain the following:

LOT 1			
S/No	**Name of Goods or Related Service**	**Quantity**	**KES (Inclusive of Applicable Taxes)**
1	Supply, delivery and installation of end to end monitoring solution	1	(Please indicate your price here)
2	OEM instructor led training for administrators/operators, leading up to certification	20 pax	Total cost
3	OEM led professional services to facilitate the design and deployment of the solution	Lot	Total cost
4	Enterprise support with 4hr mission critical replacements of parts and disks, operating system updates, access to manufacturer's technical support team, online troubleshooting / support tools and proactive problem diagnosis services	Lot	Total cost
5	Total Cost of ownership (product associated licenses)	Lot	Total cost
6	Partner / Vendor SLA Support (3 Years)		
	Total		(Please indicate the total price here inclusive of applicable taxes)

FINANCIAL REQUIREMENT

Bidders are required to provide a breakdown of how they arrived at the cost summary.

6.0 POST-QUALIFICATION/DUE DILIGENCE

The Procuring Entity may conduct post-qualification/due diligence on the lowest evaluated bidder before the award of the contract. This process may include, but is not limited to:

1. Verification of Documentation – Confirming the authenticity of certifications, reference letters, and any other supporting documents submitted with the bid.

2. Reference Checks – Engaging with past and current clients to verify performance, service delivery, and adherence to contractual obligations.
3. Financial Capability Assessment – Evaluating the financial strength of the bidder to ensure their ability to sustain the project, including a review of audited financial statements.
4. Reference Site Validation – Reconfirming the ability of the bidder to provide the proposed product(s) and support, in accordance with the stated service levels through site visits to the reference sites by the evaluation team.

Failure to satisfactorily pass the post-qualification and due diligence process may result in the disqualification of the bidder, and the Procuring Entity reserves the right to consider the next lowest evaluated bidder or take any other appropriate action in accordance with procurement laws and regulations.