KENYA REVENUE AUTHORITY

IT INFRASTRUCTURE UPGRADE

SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, TESTING AND COMMISSIONING OF ENTERPRISE BACKUP SOLUTION

TECHNICAL SPECIFICATIONS

1. BACKGROUND

The Kenya Revenue Authority is mandated to collect, safeguard, and manage national revenue. Its operations rely heavily on mission-critical IT systems, databases, and applications. Ensuring data availability, integrity, and recoverability is essential for business continuity, compliance, and public trust.

Currently, backup processes are fragmented, with limited automation and recovery testing. To address these gaps, the Authority seeks to procure and implement a robust enterprise backup and restore solution.

2. OBJECTIVES

1. Establish a centralized, secure, and scalable backup and restore system.
2. Ensure rapid recovery of mission-critical systems in case of data loss, corruption, or disaster.
3. Comply with national ICT policies, data protection regulations, and international best practices.
4. Minimize downtime and revenue collection disruptions.
5. Provide audit trails and reporting for compliance and governance

3. SCOPE OF WORK

The solution provider shall:

1. Assess current backup infrastructure and requirements.
2. Design and implement an enterprise-grade backup and restore solution for KRA for 2 sites i.e. Primary and Secondary Sites.
3. Provide hardware, software, and licenses as required.
4. Configure automated backup schedules for databases, applications, file systems, and virtual environments.
5. Implement disaster recovery capabilities, including offsite replication. Ensure encryption of data at rest and in transit.
6. Provide role-based access control and audit logging.
7. Train ICT staff on administration, monitoring, and troubleshooting.
8. Conduct user acceptance testing (UAT) and recovery drills.
9. Provide ongoing support and maintenance.

4. TECHNICAL REQUIREMENTS

The solution must:

1. Support heterogeneous environments (Windows, Linux, UNIX, databases, virtual machines).
2. Enable incremental, differential, and full backups.
3. Provide deduplication and compression to optimize storage.
4. Integrate with cloud and on-premises storage.
5. Offer centralized management dashboard with real-time monitoring.
6. Support Recovery Point Objective (RPO) and Recovery Time Objective (RTO) targets defined by the Authority.
7. Be scalable to accommodate future growth.
8. Comply with ISO 27001 and ITIL standards.
9. Featured in Gartner Magic Quadrant 2025 in the leader's quadrant.

5. GOVERNANCE AND COMPLIANCE

1. Align with Kenya Revenue Authority ICT governance framework.
2. Ensure compliance with Data Protection Act and relevant financial regulations.
3. Provide audit logs for all backup and restore activities.
4. Facilitate periodic independent security assessments.
5. The successful bidder is required to provide a mandatory three (3) year post warranty support and maintenance of all the solution hardware and software components.

6. DELIVERABLES

1. Inception report and implementation plan.
2. Installed and configured backup and restore solution.
3. Documentation (system design, user manuals, SOPs).
4. Training sessions for ICT staff.
5. UAT and recovery drill reports.
6. Final project completion report.

7. EVALUATION CRITERIA

Proposals will be evaluated based on:

1. Mandatory Technical compliance with requirements.
2. Vendor experience in similar projects (especially government/revenue authorities).
3. Cost-effectiveness and value for money.

4. Support and maintenance plan.
5. References and client testimonials.

8. CONFIDENTIALITY

All data handled during implementation shall remain the property of Kenya Revenue Authority. The provider shall adhere to strict confidentiality and non-disclosure agreements.

A. INSTRUCTIONS TO BIDDERS

1. The bidders are encouraged to carry out a site survey to familiarize themselves with the installation sites.

2. The bidders will be required to showcase a demo on the following key focus areas:-
   a) Table-level backup and restoration capabilities for PostgreSQL databases.
   b) Demonstrate low and scalable licensing and operational cost models.
   c) Air-gapped backup capabilities to curb against ransomware and cyber threats.
   d) Faster backups and restoration performance on Windows and Linux environments.

SOLUTION OVERVIEW AND RODUCT CHARACTERISTICS

Each requirement must be concisely substantiated / explained / articulated per requirement.

No	General Requirements	Bidders Response
GR01	Product name	
GR02	Version release number and year of release	
GR03	Date when first client site went live and the name of client	
GR04	Total number of completed (live) installations	
GR05	Does your company have a local presence in Kenya or Africa?	
GR06	What is your largest customer for this product giving the name of the customer and contact details	
GR07	Explain the solution licensing model e.g. per site, per CPU, per concurrent user, per named user, per server license, on capacity etc. Licensing model for a DR Site or a Cold site.	

GR08	Is your company an acquisition target? Any other potential business disruptions?	
GR09	What is your demonstrable experience in dealing with medium to large government entities	
GR10	What are some of the highest recognitions or awards that you have received for the product, implementation or support excellence?	

C: TECHNICAL SPECIFICATIONS

Bidders are required to provide comprehensive responses, firm commitments, and all necessary supporting documentation where applicable.

Table 2: General Requirements and TECHNICAL SPECIFICATIONS

1.2 TECHNICAL REQUIREMENTS

No.	Requirement Description	Detailed Description	Complied /Not Complied
	Architecture and Supported Platforms		
TR01	Describe the architecture of the solution (modularity, communication flows between components, numbers of components, etc.), better if supported by a high-level block diagram that explains how the solution is to be implemented for both primary site and DR site.		
TR02	Provide detailed specifications inclusive of itemized list – Bill of materials of all hardware inclusive of storage, software, databases parts etc. required.		
TR03	Provide details on the hardware including storage capacity (OS, Processor, memory, Disk capacity and number of servers) required to provide/implement the proposed solution.		

No.	Requirement Description	Detailed Description	Complied /Not Complied
TR04	Provide details of the proposed hardware appliance with storage, in terms of: • Size dimensions. • Weight of the individual Backup/recovery hardware components. • Cooling requirements etc		
TR05	Describe how granularly scalable the proposed solution is without driving huge investments for the KRA's infrastructure.		
TR06	In the case where an agent must be installed on the client platforms, how does the solution roll out client software to different platforms with minimum to no downtime?		
TR07	Typically, how would one deploy the proposed solution? Provide in detail all the available options.		
TR08	Describe the solutions for different modes of backup and recovery that can improve on the backup window for the systems.		
TR09	Define how the software system is scalable and being hardware agnostic to work with existing hardware within the authority or will the authority have to procure specialized storage for the solution?		
TR10	Ability to Support: a. 25G that can auto negotiate to 10G Network Connectivity within the data centre. b. SAN switches with 32G FC.		

No.	Requirement Description	Detailed Description	Complied /Not Complied
TR11	Describe in detail the solutions' ability to integrate into the platforms below: a. VMware, Hyper V and all other Virtual Infrastructure platforms. b. Oracle databases with Exadata platforms requiring snapshots or hot backups. c. EDB Postgres Databases d. MySQL Databases e. Microsoft Windows server 2008/2012/2016 and later platforms requiring snapshots or cold backups and file system backups. f. Linux platforms running Redhat Enterprise Linux and oracle Linux that require snapshots or cold backups and file system backups. g. Lotus Domino servers including Emails. h. Microsoft SQL server 2008/2014/2016 and later Database Servers. i. SharePoint servers 2012. j. Network devices including routers, switches, firewalls and call manager. Network devices backup through SSH, SNMP, SFTP and FTP k. SAP HANA and SAP ECC Components		
TR12	Does the proposed solution support failover without manual intervention to a second site i.e. Disaster Recovery?		
TR13	Detail how high availability, load balancing and DR is achieved. **The authority has two data centers –primary site and DR site 5 km apart.**		

No.	Requirement Description	Detailed Description	Complied /Not Complied
TR14	Does the solution support a minimum of 10 TB/Hr throughput on the target backup devices in the centralized backup solution and recovery of the same within an hour or less? Describe how continuous data protection is achieved while ensuring reduction in the number of data copies for test/dev, analytics, and disaster recovery to a single copy		
TR15	Ability to back up large databases (30 tera bytes) within 2 hours. Illustrate the methodologies of how this is achieved considering that the data will be sitting on Postgres EDB and on Oracle Database with SAN Storage), better if the response to this is supported by a high-level block diagram that explains how this will be implemented.		
TR16	System ability to support the backup of the physical and virtual servers below: a. Physical servers in production and in DR. b. HYPER – V Virtualized environment physical servers. c. VMware – Virtualized Environment d. Oracle OLVM – Virtualized environment e. Expectation of a bare metal recovery support. f. Containerized workloads on Kurbenetes.		
TR17	Support for automated and orchestrated Primary and DR Recovery processes.		
TR18	Support for full Bare Metal Recovery, for dissimilar hardware restores i.e. P2V or V2P restores.		
TR19	Support for backup of 10000 mailboxes.		
	Datacenter Backup and Recovery		

No.	Requirement Description	Detailed Description	Complied /Not Complied
TR20	The solution must provide options for backup data immutability using the following methods: Hardened repositories, Deduplication Appliances, S3 Storage (on-prem & cloud), BLOB Storage, WORM Tape support		
	Backup Operations in VM Environment		
TR21	The solution should support *image-based backups from vSphere, Hyper V, Oracle Linux VM & RedHat Virtualization		
TR22	The solution must provide efficient 'incremental forever' backup. Please outline other backup methods available		
TR23	The solution should support VM backup directly from SAN, VMFS or NFS Datastore.		
TR24	The solution should automatically detect Virtual Machines with SCSI Bus sharing and exclude them from backup		
TR25	The solution should automatically detect VMware Datastore free space and prevent backup snapshot if space is below the defined threshold		
TR26	The solution should allow the exclusion of virtual machine disks and swap files from snapshot-based backup		
TR27	The solution should allow the exclusion of Guest OS files and folders from snapshot-based backup		
TR28	The solution must dynamically integrate with vSphere tags for ongoing management		
	Agentless backup of Virtual Machines		
TR29	The solution should not require deployed Agents in virtual machines to facilitate application backup and granular recovery.		

No.	Requirement Description	Detailed Description	Complied /Not Complied
TR30	The Agentless backup should truncate the Microsoft SQL, Microsoft Exchange, and Oracle Database transaction or archive logs.		
TR31	The Agentless backup should truncate the Microsoft SQL, Microsoft Exchange, and Oracle Database transaction or archive logs.		
TR32	The solution should allow the recovery of files and application items without installing Agents in Virtual Machines.		
TR33	The solution should be able to utilize storage snapshots for creating a copy of the Virtual Machine in an isolated network environment for test purposes.		
TR34	The solution should be able to restore granular database objects. E.g at table levels		
	Backup Operations, Physical Servers Environment		
TR35	The solution should facilitate image level and file level backup of physical or cloud-based servers.		
TR36	The solution should provide backup plugins for Oracle RMAN, PG_basebackup and SAP HANA applications.		
TR37	The solution must provide application-awareness when backing up MySQL and PostgreSQL running on Linux.		
	Virtual Machines and Physical Servers recovery operations		
TR38	The solution must provide complete portability in any proprietary backup archive and should not be dependent on any point-in-time backup infrastructure e.g. central catalog, for recovery.		
TR39	The solution should provide Instant Virtual Machine recovery technology, running a Virtual Machine directly from backup repository server or storage snapshot.		

No.	Requirement Description	Detailed Description	Complied /Not Complied
TR40	The solution should provide Changed Block Tracking recovery technology for VMware Virtual Machines.		
TR41	The solution should provide the ability to start the Virtual Machine in an isolated network environment during the recovery process and inject a script into the Guest OS that allows for the server to be modified for compliance purposes prior to recovery		
TR42	The solution should provide bare metal recovery from Agent-based backup with the ability to create a bootable media for the specific server.		
TR43	The solution should allow recovery of agent-based backup to VMware or Hyper-V Virtual Machine		
	File-level recovery from VM and Agent-based backups		
TR44	The solution should facilitate file level recovery operations without the need to deploy an agent in a virtual or physical server		
TR45	The solution should be able to recover files into a virtual machine guest OS even when there is no network connection between the backup server and virtual machine.		
TR46	The solution should provide a web-based self-service user interface and ability to search for a specific file across all backups, Application items recovery from VMware and Agent-based backups		
TR47	The solution should support the granular recovery of Microsoft Active Directory, Exchange, SQL and Share Point applications.		
TR48	The solution should support granular table recovery and restore from relational Databases.		
TR49	**Training** The vendor shall provide classroom training for 20 staff in 2 groups of 10 each.		

No.	Requirement Description	Detailed Description	Complied /Not Complied
TR50	Licensing Models over a **3 Year** period: a. Expected frontend capacity for licensing purposes-**900TB** (Capacity Based) b. Expected Data Base Servers to be backed up 300 **(Server Based)**.		
TR51	Expected Backend capacity-**900TB Usable**		
Bidders who do not comply with any of the above requirements will NOT be considered for further evaluation			

1.3 BUSINESS AND FUNCTIONAL REQUIREMENTS

No	Requirement Description	Pass/ Fail	Detailed Description
FR01	The solution should support the granular recovery of Oracle Databases from image-based or Oracle RMAN backups.		
FR02	The solution to be able to restore Database backups to different OS platforms e.g from Redhat Enterprise Linux to Oracle Linux etc		
FR03	The solution should provide a web-based self-service user interface and ability to browse and recover Lotus Domino items, and PostgresSQL or Oracle Databases		
FR04	The solution should not use a third-party product for granular recovery of application items		
FR05	The solution should be able to restore a single pluggable database from a container database backup		
	Backup to Disk		
FR06	The solution must be software-defined and able to run on-premises or on any cloud platform.		
FR07	The solution must be able to scale both horizontally and vertically (i.e. scale-out and scale-up).		

FR08	The solution must provide an easy mechanism for expanding or contracting target backup storage.		
	Backup to Cloud		
FR09	The solution should natively support moving backup archives to Amazon S3 and Azure Blob Cloud Storage.		
FR10	The solution must provide incremental and granular recovery from cloud-based object storage.		
FR11	The solution should provide 100 or more Cloud Provider options for Cloud Backup storage.		
FR12	The solution should offer immutability in object storage at a bucket level		
FR13	The solution should have the option to copy or move data to object storage upon backup completion		
FR14	The solution should have the option to copy or move data to object storage upon backup completion		
FR15	The solution should support backup of workloads (IaaS), databases and file data (PaaS) running in AWS, Azure & Google (Commercial & Government tenants).		
FR16	The solution should have the ability to backup Kubernetes data using CSI to different storage targets. The backup data should be encrypted and immutable.		
	Backup data security		
FR17	The solution should encrypt backup files using the AES 256bit encryption. The encryption should not depend on the backup storage platform.		
FR18	The solution should provide AES 256bit encryption with password loss protection technology, so the data can be decrypted if the operational password is lost.		

FR19	The solution should be integrated with SAML 2.0 for extended authentication.		
FR20	The solution must provide role-based access control through a web UI for most recovery and backup operations.		
	Cyber Resilience		
FR21	Ability to proactively identify cyber threats in backup infrastructure to recognize suspicious activity and mapping of data to MITRE ATT&CK framework to identify adversary tactics, techniques, and procedures (TTPs) used during a cyber-attack.		
FR22	Indicators of Compromise to detect and report the sudden appearance of utilities which are commonly utilized by cybercriminals for lateral movement, data exfiltration, command and control, stored credential access, and more.		
FR23	Advanced Anomaly Detection which detects data encryption between restore points and presence of dark web links or ransom notes.		
FR24	Should have file system activity analysis to detect known suspicious files and extensions, mass file deletion and mass file extension change.		
FR25	Should have Advanced signature-based malware detection engine with Machine Learning and heuristic analysis to identify advanced threats such as polymorphic malware.		
FR26	Should have YARA analysis engine to help pinpoint identified ransomware strains to prevent the reintroduction of malware into the environment		
FR27	Ability to automatically scan backups for ransomware before the restore process using 3rd party malware scanners or YARA rules.		

FR28	Ability to run backups in an isolated sandbox to perform more advanced ransomware investigations, root cause analysis or to investigate for indicators of compromise and to make sandboxes accessible to 3rd party tools for advanced ransomware investigations (Data Integration API for third-party integration).		
	Backup data verification		
FR29	The solution should automatically read and verify the consistency of production data in the backup file after the backup was completed. In case data corruption is detected the solution should automatically rebuild the corrupted block with data from production.		
FR30	The solution should automatically start the virtual machines from backups and verify the operating system, and application availability. This testing must have no impact on the production network. The solution should provide a recovery verification report.		
	Backup Monitoring and Reporting		
FR31	The solution must alert on failed jobs and jobs that exceed the backup window		
FR32	The solution must alert in advance if the backup target is approaching capacity.		
FR33	The solution must provide proactive alerts to eliminate issues. These issues should be automatically detected, encompass configuration and performance and detection should be dynamically updated by the vendor.		
FR34	The solution should provide a self-assessment report. The report should detect if the solution is deployed according to best practices.		
FR35	The solution should provide capacity planning and forecast backup storage space utilization.		

FR36	The solution should provide backup infrastructure and policy changes report for audit purposes.		
	Other Requirements		
FR37	Ability for backup archives be tested for recoverability with this solution.		
FR38	Ability to demonstrate how recoverability tests performed		
FR39	The solution must provide support for Microsoft Office		
FR40	The solution must provide granular (i.e. item-level) recovery options		
	Security Requirements		
	The solution should support the following security standards.		
FR41	a) AES 265 Encryption (in flight & at rest)		
FR42	b) FIPS 140-2 support		
FR43	c) MFA & Screen timeout policies		
FR44	d) TLS 2.1 encrypted connection		
FR45	e) DoDIN APL Approved & Aligned w/ NIST Cybersecurity Framework		
FR46	RBAC policies		
FR47	ISO 27001		
FR48	CMMC v2, Level 1 Malware Detection Engine – Inline scanning of backups for malware threats		
FR49	DISA JIE/JRSS – ATO		
FR50	Hardened Linux Repository: SEC 17a-4(f), FINRA 4511(c) and CFTC 1.31(c)-(d) WORM compliant		
	Minimum Backend Backup Appliance Technical Requirement		
FR51	**Design**: **Prod Environment**-Backup storage is based on NMVe SSD Disk storage of 30TB maximum per disk Configured with 400TB usable capacity for production site.		

	DR environment - Backup storage is based on NMVe SSD Disk storage of 30TB maximum per disk Configured with 400TB usable capacity for production site.		
FR52	**Bill of Materials:** Bidder MUST provide a granular and itemized Bill of Material to be used to check/verify configurations of the solution		
FR53	**Architecture**: Nodes and controllers should work in active-active mode, balancing service loads among all controllers		
FR54	**Data encryption:** Supports encryption of stored data to prevent sensitive information leakage.		
FR55	**Multi-tenancy:** The file system multi-tenant function is configured to isolate resources between vStores.		
FR56	**Controller interconnection protocol:** The high-speed multi-controller (all controllers) interconnection architecture should be used. The controller interconnection protocol must be PCI-E/IB/RDMA, not Fibre		
FR57	Channel or IP federation.		
FR58	**Zero service interruption:** If one out of two controllers on a node fails, backup services must be switched to the normal controller within seconds, ensuring zero service interruption.		
FR59	**Cache capacity:** The total cache capacity in the system to be greater than or equal to 512 GB, and the cache capacity of any controller should be greater than or equal to 256 GB		
FR60	**Supported Disk Type:** Support SAS SSDs, NVMe SSDs or NL-SAS HDDs		
FR61	**Physical bandwidth:** The minimum physical bandwidth of each node should be 10 TB/hour or higher		

FR62	**Backup software support:** The backup storage should support mainstream backup software, such as Networker, Veritas, Commvault, Veeam or equivalent.		
FR63	**Non-disruptive upgrades:** The storage should support online non-disruptive upgrade of firmware and hardware components. Future controller and disk enclosure upgrades should be done without any data migration.		
FR64	**Frontend ports:** Support 8/16/32 Gbit/s Fibre Channel, 10GE, 25GE, 40GE, 100GE ports.		
FR65	Required: - 4* 10G SFP+ ports, 4 * 25G SFP+ ports,4*32Gbps FC per controller		
FR66	**Medium Servers requirements**		
FR67	At least 3 medium servers per site (each with 2 intel CPU/16 cores, 256gb memory ddr5, SSD 600*2, SSD 1.2tb *5, Raid controller, Ethernet network card 25g-Autonegotiate to 10gb with optical transceivers and 1* dual HBA card 32gbs) • NB: In addition to the above minimum requirement, please ensure that all specific components required to achieve this configuration are clearly provided and costed in case it is separately chargeable. E.g Backup Manager, Proxy servers etc		
FR68	The vendor is expected to provide all accessories to ensure that the complete solutions work as expected including but not limited to: • SFPs • Cables etc		
Bidders who do not comply with any of the above requirements will NOT be considered for further evaluation			

B: VENDOR EVALUATION CRITERIA

The bidder is required to complete the vendor evaluation criteria below.

Table 1: ENTERPRISE BACKUP AND RESTORE SOLUTION

No	Requirement	Evaluation Criteria	Bidders' response	Max Score
1.	**Vendor Experience** Demonstrate experience through previous execution of **two (2)** projects in deployment of enterprise backup solution of similar magnitude within the last five (5) years.	Bidder MUST submit recommendation letters/certificate of completion for each project cited, supported by copies of signed Contracts **or** copies of LSOs. In addition, the recommendation letters should have: i) Contacts: postal address, telephone and email of the contact person. ii)A brief description of the project delivered **(3 Marks for each project)**		6
2.	**Technical staff Qualifications.** Three (3) Technical staff 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 Certifications from Backup solution proposed product	Bidders MUST attach the CV of each staff supported by copies of Academic and professional certificates. 4 Marks for each Qualified Staff (1 Mark for degree or Diploma and 3 Marks for valid proposed storage vendor professional certification)		12

3.	**Staff Relevant experience** Each Qualified staff (refer to clause 2 above) should have experience in implementation, support and maintenance of the proposed enterprise backup solution vendor product.	Staff Relevant experience • More than 3 years – 3 Marks • At least 2 years but less than 3 years – 2 Marks • At least 1 year but less than 2 years – 1 Mark • Less than 1 year – 0 **Marks** Note: Bidders MUST submit a copy of the CV for each staff clearly indicating the years of experience in implementing and supporting the specific vendor product and the sites supported.		9
	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			
Bidders who do not meet the cut off score under vendor evaluation will NOT be considered for further evaluation				

Table 3: BACKUP SOLUTION PRESENTATION/DEMO

Key Areas of focus to be Demonstrated		
No.	**Item**	**Scores**
1	Table-level backup and restoration capabilities for PostgreSQL databases.	**3**
2	Demonstrate on low and scalable licensing and operational cost models.	**2**

3	Air-gapped backup capabilities to curb against ransomware and cyber threats.	**3**
4	Faster backups and restoration performance on Windows and Linux environments.	**2**
	Total score	**10**
The Demo scenarios shall be sent by email to the bidders who qualify in the technical evaluation and will be set against the product deliverables as listed in this document.		

Technical Evaluation Summary: **Enterprise Backup and Restore Solution**

The technical evaluation for this Initiative shall be based on **two (2) components**, as outlined below:

a) **Vendor Technical Evaluation**

- Total Marks: **30**
- Minimum Cut-off: **22.5 Marks**

b) **Backup Solution Presentation/Demo**

- Total Marks: **10**

The **maximum technical score** for this Initiative shall be **40 marks**.

To be considered **technically responsive**, a bidder must:

- Achieve a **minimum aggregate technical score of 30 marks out of 40**, which shall be **prorated to 75%**, and
- Meet any applicable minimum requirements under each evaluation component.

Only bidders who attain **at least 30/40 marks (75%)** in the overall technical evaluation shall be considered responsive to technical requirement.

FINANCIAL REQUIREMENT

- N/B: Bidders to provide a detailed breakdown of how they have arrived at the total cost
- Grand Total Cost –To be carried Forward to the FORM FIN 2 Summary of Costs