SHELTER AFRIQUE
Financing Affordable Housing for Africa

Date: 18th February 2026

REQUEST FOR PROPOSAL

SUPPLY AND INSTALLATION OF A CHANGE TRACKER AND ACTIVITY MONITORING SYSTEM s(AUDITOR)

1.0 Background

SHELTER-AFRIQUE Development Bank is a regional Housing Finance Institution established by African Governments, dedicated to investment in housing and urban development in African Countries. Shareholders include 44 African countries, the African Development Bank, and the African Reinsurance Corporation. The organization has its headquarters in Nairobi, Kenya, and two regional offices: Abuja, Nigeria, and Abidjan, Côte d'Ivoire.

The Bank is requesting proposals for the supply, installation, and configuration of a **unified security, compliance**, and **visibility platform** with **file integrity monitoring (FIM), database activity monitoring (DAM)** and **change tracking** capabilities at the Head Office located in Upper Hill, Longonot Road.

2.0 Scope of Work

The purpose of this RFQ is to invite technical and commercial bids for the selection of a service provider for the provision of a unified security, compliance, and visibility platform with file integrity monitoring (FIM), database activity monitoring (DAM) and change tracking capabilities.

The scope includes:

- Supply and installation of a system capable of file integrity monitoring (FIM), database activity monitoring (DAM) and change tracking.
- Configuration of the platform and integration with the existing ICT infrastructure, mainly Active Directory, file storage servers, databases such as Oracle and MS SQl and servers running on Microsoft Windows Server 2016 and above, Oracle Linux version 6 and above, Oracle Cloud Infrastructure and Microsoft Azure.
- Provide training to the technical team.
- Post implementation Support of 6 months.

- Provide Hardware environment and third-party software specification.

For detailed technical specifications, see the annexure.

3.0 Evaluation process and selection criteria

Responses to this RFQ will be evaluated and scored based on the following:

- Experience of the provider of at least five years providing similar services.
- Certified products partner of the equipment listed above. Provide a recent proof, preferably less than a year.
- Similar jobs done previously. Attach proof; provide at least three reference sites.
- Technical approach and methodology proposed
- Organisation structure and staff qualification
- Compliance with regulatory authorities
- Financial proposal. Bidder whose offer represents the best value to Shelter Afrique
- Quality and clarity of the proposal presentation

Selection will be based on 70% technical and 30% financial.
Each bid will be given a technical score. A proposal shall be rejected at this stage if it does not respond to important aspects of the Terms of Reference or if it fails to achieve the minimum technical score of 50%.

The formula for determining the final scores (sf) is the following:

Sf = 100 x Fm / F, in which Sf is the financial score, Fm is the lowest price and F the price of the proposal under consideration. Final score computed as follows:

Final Score = 0.3 Sf + 0.7

St. with St being the technical score.

The bidding firm, best qualified as per the technical score, shall be invited for further discussions.

4.0 Presentation of Proposals

To facilitate the analysis of responses to this RFQ, the proposals should be clear, comprehensive, and concise in description of the firm's capabilities to meet the requirements provided in the RFQ.

Submissions to this RFQ must include the following

4.1 Technical Proposal

i) Company Background:
   a) Provide basic information to indicate expertise and experience in this area and capacity to carry out the project, if chosen,
   b) Also provide:
      - Name of company,
      - full address, telephone and fax numbers, and e-mail address.
      - Legal status.
      - Physical address.
      - Date of establishment or registration.
      - Details of the organization structure.
      - Provide a copy of the latest tax compliance certificate from the Government Tax Collection Agency.
      - Two-year financial statements.

ii) A brief description of the firm's recent experience on projects of a similar nature.
iii) A description of the execution and work plan for undertaking the project.
iv) Provide the proposed high-level architecture of the proposed solution and how it fits into the existing IP Telephony ecosystem of the institution.
v) Any other additional information.

4.2 Financial proposal format

The financial proposal should be well itemized as per the scope of work and list of services to be supplied.
The financial proposals should be expressed in KES and inclusive of taxes, where applicable.

It should be presented **separately** from the technical proposal.

5.0 Clarification of Request for Proposal

The company may seek clarification on this RFP only up to 1 day to the end of the submission date. This should be requested in writing via email given in section 7.0.

Shelter Afrique will respond by email or letter.

6.0 Final Ranking

The bidder with the highest combined technical and financial score will be ranked first and eligible for the award of the contract.

7.0 Submission of bids

Proposals should be sent by mail to: procurement@shelterafrique.org with subject as:

SUPPLY AND INSTALLATION OF A CHANGE TRACKER AND ACTIVITY MONITORING SYSTEM

The deadline for submission of bids is the close of business on 16th March 2026

ANNEXURE

Technical Specficiations Requirements:

Bidders shall use the following options to indicate the "DEGREE OF SUPPORT OF COMPLIANCE" their solution provides for each of requirement given in the table below:

a. **FS - (Fully Supported)** the application fully supports the requirement without any modifications.

b. **PS - (Partially Supported)** the application supports the requirement with use of a system or workflow workaround.

c. **NS - (Not Supported)** the system is not capable of supporting the requirement and cannot be modified to accommodate the requirement.

A. File Integrity Monitoring (FIM) and Change Tracking Technical Specifications

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
1	Supports all Windows platforms	M		
2	Supports all Linux platforms	M		
4	Supports both physical and virtual environments	M		
5	Supports databases (Oracle, MS SQL etc)	M		
6	Supports network security devices (Firewall, Proxies, SIEM…etc)	M		
8	Solution must be able to detect, report and alert on file changes, providing clear context as to whether the Change was planned or unplanned	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
9	Solution must be able to alert on who made the change	M		
10	Solution must be able to report on changes in real time	M		
11	Solution must be able to keep multiple baselines as a referenced threshold to compare against.	M		
13	Solution must have role-based access and permissions with customized views related to the unique log in I.D.	M		
14	Solution must have a centralised, web-based GUI. The GUI should be easy to use and customizable	M		
15	Solution must support SMTP relay and be capable of sending emails to many recipients at a time, notifying of specific activity	M		
16	Solution must contain compliance reports such as: PCI-DSS, ISO27k, NIST, etc	P		
17	Solution must have pre-defined file integrity monitoring polices/profiles included out of the box	M		
18	Solution allows administrators to customize and create their own file integrity monitoring policies	M		
19	Solution must be able to integrate with a change management platform to automate the creation of planned change rules	M		
20	Solution must be able to detect, report, and alert on configuration, executable, and log file changes	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
21	Solution shall be able to monitor:	M		
22	a) Registry Keys			
	b) Configuration files			
	c) File Permissions			
	d) Customize (Specific Directories, Files, or extensions)			
	e) ACLs Rules			
	f) Routing Table			
	g) Access to Auditing/logging folders (Logs)			
	h) Group Policy			
23	Solution's report shall include at least the following data:	M		
	a) Time/Date stamp			
	b) Impacted Target (Filename, Path, Computer/IP)			
	c) Action: Deleted, Created, Modified			
	d) Process used			
	e) Unique File Hash value			
	f) File size			
24	Solution must be able to scan file content and hash values	M		
27	Solution must be able to detect a new service or process being installed on servers	M		
29	The solution should be enterprise-ready, easy to deploy, and scalable to support additional devices and applications without a change in configuration. No Changes in the existing infrastructure should be required.	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
30	Solution should require no downtime of the server or database when deploying agents.	M		
31	The resource overhead (hardware, software, latency) for the agent should not exceed 10% of the normal requirement of the CPU. There should be only one agent per machine for example.	M		
32	Solution should easily and automatically differentiate between Planned vs. Unplanned changes	O		
34	The solution should provide standard sets of CIS Certified FIM monitoring templates for each operating system	M		
36	The solution should provide a single environment for file integrity monitoring and policy-based configuration assessment for a broad range of computing systems and applications, such as servers, desktops, hypervisors, network devices, etc	M		
37	Manage all distributed devices from a single management console. The management console must be able to manage all aspects of remote devices, including user management, system management, alerting, and reporting.	O		
38	The solution should be able to generate an initial baseline version of a computing system so that integrity is based on a known good state	M		
39	The proposed solution should be able to compare an asset's configuration state against	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
	a pre-defined policy to determine whether the configuration is compliant.			
40	Solution should be able to offer the same level of features/functionality on both on-premises and Cloud.	M		
41	Solution must be able to integrate with workflow / Ticketing system to help in verifying legitimate changes	M		
42	Solution must include the ability to schedule detailed reports to multiple recipients, delivered via email.			

B. Activity Monitoring requirements and Change Tracking for OS and Databases (System Auditor)

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
	DATA COLLECTION AND STORAGE			
1	Noise-free security intelligence Collects raw machine data and transforms it into clear, actionable information about every user action, without the noise associated with raw data.	M		
2	Reliable audit data Consolidates audit data from multiple sources (event logs, configuration snapshots, change history records, etc.) to get the most reliable audit trail without gaps.	M		
3	Detailed information about every change and access event Captures and delivers full details about changes and access attempts, including when and where the change or access attempt was made, who made it, and exactly what was changed or accessed.	M		
4	Before and after values Performs full side-by-side comparisons and captures the before and after values for all modified objects.	M		
5	Consolidated approach for hybrid IT infrastructures Collects audit data from both on-premises and cloud applications such as - MS Azure, OCI, AWS - and stores it in	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
	a secure central repository, enabling unified alerting, searching, reporting and security risk analysis.			
	SUPPORTED SYSTEMS AND AUDIT SCOPE			
6	Active Directory and Group Policy • Reports on Active Directory and Group Policy changes • Provides time-specific information on AD and Group • Policy configurations, including group membership across multiple domains and effective permissions • Delivers logon auditing (including ADFS logons • Supports both trusted and non-trusted domains	M		
7	Exchange • Provides information on changes to Exchange Server configuration, Exchange databases, mailboxes, mailbox delegation and permissions • Delivers non-owner mailbox access auditing for online exchange	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
8	Windows file servers, Online SharePoint etc • Reports on changes to files, folders, shares and permissions Reports on files moved, renamed or copied • Provides information on successful and failed read attempts • Delivers time-specific information on effective permissions, including excessive access rights • Includes predefined reports on data ownership, data usage and data volumes, stale files, and duplicate files • Reports on sensitive and regulated data, including its location, effective permissions and owners, as well as successful and failed attempts to access the data and changes to its permissions • Alerts on activity related to sensitive data, including information about data sensitivity type • Enables searching for activity related to sensitive data by data sensitivity type	M		
9	Supports multiple file servers and file appliances in multiple sites, domains and Ous	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
10	Windows Server • Reports on all changes made to server configuration — hardware and software, services, applications, network settings, registry settings, DNS, file shares and more • Provides information on audit log clearance, changes to local audit policy, Windows service failures, system shutdowns and time changes • Delivers time-specific information on Windows Server configurations, including OS name and version, antivirus status, file shares, local users and groups, services, and installed programs • Reports on privileged user session start and end times	M		
11	SharePoint • Reports on changes to farm configurations and user content, permissions and permissions inheritance, group membership, and security policies • Includes read access auditing • Reports on effective access permissions and whether permissions were granted directly or via group membership • Reports on sensitive and regulated data, including its location and effective permissions, as well as attempts to access it and changes to permissions • Supports SharePoint 2016 and above	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
12	Azure AD • Reports on changes to Azure AD groups, users, passwords, roles, applications, service principals, devices, contacts and more. • Reports on user accounts, account attributes and account roles. • Audits successful and failed logon attempts, and detects those coming from outside of trusted locations. • Supports MFA-only tenants.			
13	Exchange Online • Reports on Exchange Online administrative changes, as well as changes to mailboxes, mail users, groups, permissions, policies and management roles • Audits non-owner mailbox access events • Reports on permissions to delegated mailboxes, as well as whether permissions were granted directly or via group membership • Supports MFA-only tenants	M		
14	Oracle Database • Reports on changes to roles, permissions, settings, audit policy, databases, triggers, views and more • Reports on content changes	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
	• Audits successful and failed logon attempts • Reports on data access			
15	Supports Oracle Database 11g, 12c and 19c and Oracle KVM	M		
16	SQL Server • Reports on changes to SQL Server permissions, server instances, roles and databases, tables, columns, stored procedures, etc. • Reports on content changes • Reports on data access • Audits successful and failed logon attempts • Reports on effective access permissions to SQL Server objects, as well as whether permissions were granted directly or via group membership • Alerts on activity related to sensitive data, including information about data sensitivity type • Reports on the current database configuration • Supports SQL Server 2016, 2019	P		
17	VMware • Reports on vCenter, including its servers, clusters, resource pools and hardware configurations • Reports on changes to local users, creation of users and groups	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
	• Reports on virtual machine settings, permissions and power state • Audits successful and failed logon attempts • Reports on effective access permissions in the vSphere environment, including vCenter, data centers and virtual machines			
18	Network devices • Reports on changes to network devices configurations and their status • Reports on both successful and failed attempts to log in to network devices directly or over VPN connections • Reports on scanning threats, hardware malfunctions and high-data traffic events • Supports all of the following network devices: - Cisco ASA, Cisco IOS, Cisco Meraki - Fortinet FortiGate - HPE Aruba - Juniper - Palo Alto - Pulse Connect Secure - SonicWall	M		
	REPORTING AND ALERTING			
19	Predefined reports and dashboards Includes predefined audit reports and dashboards that deliver detailed information about changes, access and	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
	configurations in a human-readable format and enable users to filter, sort and export the audit data.			
20	Custom reports Enables users to easily build custom reports based on their specific requirements, including cross-system reports.	M		
21	Email report subscriptions Automatically delivers reports to specified recipients by email or saves them to a file share on a specified schedule (daily, weekly, etc.).	M		
22	Multiple report export options Supports export of reports to all of the most common formats, including PDF, XLS(X), DOC(X) and CSV.	M		
23	State-in-time reports Shows configuration settings as they currently are or as they were at a specific moment in the past, including effective permissions by user or by object, Group Policy settings, and Windows Server configuration details.	M		
24	Out-of-the-box compliance reports Includes ready-to-use reports aligned with compliance controls from CJIS, FERPA, FISMA/NISTSP 800-53, GDPR, GLBA, HIPAA, ISO/IEC 27001, NERC CIP, PCI DSS and SOX.	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
25	Alerts Notifies designated staff about suspicious behavior or events that could turn into security incidents, including activity that exceeds the normal baseline (threshold-based alerts), by email or SMS message.	M		
26	Compliance mappings Provides easy-to-follow guides that offer a plan of attack for meeting the requirements of most common regulatory standards, including CCPA, GDPR, HIPAA and PCI DSS.	O		
	SECURITY INTELLIGENCE			
27	IT risk assessment dashboards Enables users to identify and assess risks in four key areas: users and computers, permissions, data, and infrastructure.	M		
28	Behavior anomaly discovery dashboard Improves detection of malicious actors in the IT environment by delivering an aggregated trail of anomalous user activity with the associated risk scores.	P		
29	User profile Provides key details about each user account involved in an incident, including the name of the user, their department and manager's name, whether the account is enabled, and the AD groups the account is a member of.	O		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
30	User behavior and blind spot analysis reports Delivers actionable intelligence on potential security incidents, such as activity outside business hours, unusual logons, spikes in failed activity, access to archived data, actions by previously inactive users and potentially harmful files on file servers.	M		
	MISCELLANEOUS CAPABILITIES			
31	Automated incident response Enables users to automate response to common and anticipated incidents by creating scripts that run each time a particular alert is triggered.	O		
32	AD change rollback Reverts unwanted changes to a previous state without any downtime or having to restore from backup.	O		
33	Password expiration notification Automatically reminds AD users to change their passwords before they expire.	M		
34	Inactive user tracking Automatically detects and deactivates inactive user and computer accounts based on custom criteria.	M		
35	Event log management Automatically collects, consolidates and archives event log	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
	data so users can audit generic events, service events, user logons and remote desktop sessions.			
	MANAGEMENT INTERFACE AND USAGE			
36	Centralized management console instances Supports multiple servers from a single installation, each with its own configuration settings.	M		
37	Integrated platform Supports auditing of multiple systems and applications, including systems integrated in a unified way through cross-system dashboards, reports, etc.	M		
38	Role-based access control Enables granular segregation of security monitoring duties by providing each admin with exactly the right access to audit data and settings.	M		
	INTEGRATION CAPABILITIES			
39	Can be integrated with security, compliance and IT automation tools as well as business applications to centralize auditing and reporting or facilitate IT workflows like change management and service desk.	M		

	REQUIREMENTS	Mandatory (M) / Partially (P) / Optional (O)	FS/ PS/ NS	BIDDER'S TECHNICAL REASONS SUPPORTING COMPLIANCE
40	Integration with SIEMs Protects existing investments in third-party SIEM platforms by offering integration with Splunk, HP ArcSight, IBM QRadar, Intel Security, LogRhythm, AlienVault, Solarwinds and other SIEMs, bringing more context to their output data and reducing the volume of input data.	M		

C. Hardware and third-party software requirements

The vendor should provide hardware and any third-party software requirements specifications.

This should include operating system, server/hardware specifications and any third-party licences that might be required.

The hardware and any third-party software will be procured separately.