



African Reinsurance Corporation
Société africaine de réassurance

11th December, 2018.

INVITATION TO TENDER
– SELECTION OF VENDOR FOR THE IMPLEMENTATION OF NETWORK ACCESS
CONTROL (NAC) & IDENTITY MANAGEMENT SOLUTION –

1.0 BACKGROUND

Established in 1976 by 36 member States of the African Union and the African Development Bank Group (AfDB), The African Reinsurance Corporation (AFRICA-RE), the leading reinsurance company in Africa and the Middle East, is a pan-African financial institution whose shareholding is split between African (75%) and Non-African (25%) investors. African shareholding comprises 41 African states, the AfDB and more than 100 African insurance/reinsurance companies from the 41 member countries. Headquartered in Lagos (Nigeria), Casablanca (Morocco), Nairobi (Kenya), Abidjan (Cote d'Ivoire), Ebene (Mauritius), Cairo (Egypt) and Addis Ababa (Ethiopia) as well as two subsidiaries: Africa Re (South Africa) Ltd in Johannesburg and Africa Retakaful Ltd in Cairo (Egypt).

The Corporation is currently in the process of implementing a set of technical security controls that comprise of Network Access Control (NAC), Virtual Private Network (VPN), Multi-Factor Authentication (MFA/2FA) and Privileged Identity Management (PIM) solutions. All the above-mentioned security controls will be implemented in a tightly integrated fashion.

2.0 OBJECTIVES

The main objective of this project is to strengthen the Corporation's cybersecurity defense mechanisms and efficiently reduce the network attack surface on the information system assets through a robust security management of users and guests connecting to our systems as well as monitoring and management of privileged access within the Corporation.

Vendors with necessary technical skills, experience and business knowledge are invited to submit their best proposals accordingly to the tender process described below. Below is an overview of Africa Re's current network infrastructure:

- Africa Re currently has two (2) data centers: the primary datacenter and disaster recovery site.
- Africa Re's operational network includes the Lagos (HQs) and seven Production Centers (Cairo, Casablanca, Abidjan, Nairobi, Addis-Ababa, Mauritius, and Johannesburg) with active users in these sites.
- The connectivity between Africa Re HQs and branches is through IPSec VPN.
- The proposed maximum number of VPN and NAC users is 400.

A handwritten signature in blue ink, located in the bottom right corner of the page.

- Current number of unmanaged devices for Pulse Profiler such as IP-Phones, CCTV, Printers, Scanners, etc. is 200.
- Total number of switches that the proposed NAC solution will support is 30 switches (the switch manufacturer is Cisco).
- The operating systems on endpoints i.e. PCs and mobile devices in Africa Re environment is a mix of Windows, MAC OS, Linux, iOS and Android.
- Africa Re currently use Office 365 services for about 350 users.
- Africa Re currently use Microsoft Intune MDM solution, i.e. the solutions proposed must integrate with Microsoft Intune.
- Core business applications include: Oracle ERP E-Business applications and other application solutions.
- The total number of privileged accounts to be licensed for the privileged identity management solution is 25.

3.0 DELIVERABLES

The security controls solution and implementation services required from vendors must have the following capabilities:

3.1. REQUIREMENTS FOR THE NETWORK ACCESS/ADMISSION CONTROL (NAC) SOLUTION

- a) Enforce compliance to policies, to maintain a secure network and allow access only to authorized users, employees, and external partners.
- b) Protect the Corporate network from malicious attackers.
- c) Keep authorized users compliant with corporate security policy.
- d) Enable an automated remediation process that eases the process of regaining compliance for all authorized users on the corporate network.
- e) Provide partners and visitors access to the Internet but not the corporate intranet.
- f) Consolidation of real time contextual information from networks, users, and devices.
- g) Accurate identification of every user and device on the corporate network.
- h) Integrations with Mobile Device Management (MDM) vendors (at API-level).
- i) Enforcement of granular identity-based policies on Cisco LAN, WLAN and firewall products.
- j) Guest provisioning.

3.2. REQUIREMENTS FOR THE FOR VIRTUAL PRIVATE NETWORK & MULTIFACTOR AUTHENTICATION SOLUTIONS

- a) Cloud Services Flexibility: The solution must provide secure access to Office 365, Box, Salesforce and other SaaS services of Africa Re.
- b) Automatic Compliance: Only authorized users with compliant devices should have access to applications and services in the cloud or data center to prevent data leakage.
- c) No Passwords: Single sign-on (SSO) with certificate authentication means no more passwords for users to fuss with.
- d) Users Productivity Enhancement: Enable native mobile apps such as Word, PowerPoint, Excel and other apps to boost worker productivity.
- e) Easy BYOD: Provide mobile device security container to support Africa Re's BYOD policy.
- f) Easy Integration: Integrate with existing identity stores such as Active Directory.

- g) Simplified Administration: Provide centralized management for the cloud of appliances and policies.

3.3. REQUIREMENTS FOR THE PRIVILEGED IDENTITY MANAGEMENT SOLUTION

1. Discover and locate privileged accounts to help identify privileged account risks and automate the provisioning of these accounts to a centralized, secure digital vault.
2. Secure and store privileged passwords in a highly secure repository to reduce the risk of unauthorized access and support granular access controls to ensure only authorized users may access privileged accounts.
3. Automatically rotate privileged passwords at a regular cadence or after each use based on policy and automates password changes and synchronization to reduce the operational burden on Africa-Re's IT team.
4. Secure and manage privileged accounts throughout the enterprise to protect and manage privileged accounts in the most diverse and complex IT landscape and support privileged across on-premises and cloud environments.
5. Reduce security risks, meet and prove compliance, and reduce operational costs.
6. Protect and rotate privileged SSH keys.
7. Isolate privileged user session to prevent endpoints from spreading to critical systems.
8. Monitor and record privileged session to gain a full audit trail of user activity.
9. Enforce least-privileges to control and monitor the commands super-users can run.
10. Analyze and alert on anomalous privileged account access that could indicate an attack in progress.

4.0 EVALUATION PROCESSES AND SELECTION CRITERIA

The bids submitted in response to this RFP will be evaluated and scored based on the following criteria:

- Partnership level of the Reseller with the Original Equipment Manufacturer (OEM).
- Experience of the service provider in implementing Network Access/Admission Control, Virtual Private Network, Multi-factor Authentication and Privileged Identity Management solutions.
- Technical approach and methodology.
- Project management experience and organizational staffing.
- Proposed Cost.
- Financial Information based on audited financial statements.
- Success stories of the bidder on similar projects delivered previously.
- Quality, clarity and presentation of proposal.

5.0 PRESENTATION OF TENDER

In order to facilitate the analysis of responses to this RFP, the responding vendors are required to prepare their proposals in accordance with the instructions outlined in this section. The firms/vendors whose proposals deviate from these instructions would be considered non-responsive and may be disqualified at the discretion of Africa Re.

Proposals should be clear and comprehensive. It should provide a straightforward, concise description of the vendor's capabilities to meet the requirements of the RFP. Emphasis should be laid on accuracy, completeness and clarity of content. All parts, pages, figures and tables should be numbered and clearly labeled. The proposal should be organised into the following major sections:

SECTIONS TITLE

- 1.0 Executive summary
- 2.0 Company Experience / Expertise
- 3.0 Technical approach and methodology
- 4.0 Project Management plan & Organizational staffing
- 5.0 Cost quotations
- 6.0 Financial information
- 7.0 Resumes of key staff to be deployed

5.1 Executive summary

This part of the response to the RFP should be limited to a brief narrative highlighting the vendor's proposal. The summary should contain as little technical details as possible and should be oriented towards non-technical personnel. The Executive summary should not include cost quotations.

5.2 Experience of the Vendor

The vendor must provide the following information about their company so that Africa Re can evaluate their stability and ability to support the commitments set forth in response to the RFP. Africa Re may require the vendor to provide additional documentation to support and/or clarify requested information.

[Using the format below, provide information on each relevant assignment for which your organisation, and each associate for this assignment, was legally contracted either individually, as a corporate entity or, as one of the major companies within an association, for carrying out projects similar to the ones requested under the Terms of Reference included in this document. The Proposal must demonstrate that the Vendor has a proven track record of successful experience in providing services similar in substance, complexity, value, duration, and volume of services sought in this procurement.]

Maximum 20 pages

Assignment name:	Approximate value of the contract (in currency US\$):
Country: Location within country:	Duration of assignment (months):
Name of client:	Total No of staff-months of the assignment:

Address:	Approximate value of the services provided by your firm under the contract (in currency US\$):
Start date (month/year): Completion date (month/year):	No of professional staff-months provided by associated vendors:
Name of associated consultants, if any:	Name of proposed senior professional staff of your firm involved and functions performed:
Narrative description of review engagement:	
Description of actual services provided by your staff within the assignment:	
Description of challenges encountered, and the strategy used to address and successfully close the project including time and resources:	

Authorized Signatory:

Name of Vendor:

5.3 Approach and Methodology

In this chapter, you should explain your understanding of the objectives of the assignment, approach to the services, methodology for carrying out the activities and obtaining the expected output and the degree of detail of such output. You should highlight the problems being addressed and their importance and explain the technical approach you would adopt to address them. You should also explain the methodologies you propose to adopt and highlight the compatibility of those methodologies with the proposed approach.

5.4 Project Management Plan & Organizational staffing

In this chapter, you should propose the structure and composition of your team. You should list the main disciplines of the assignment, the key expert responsible, and proposed technical and functional staff.

5.5 Cost Quotations

The proposal of the bidders should include supply and installation of items listed in the following Bill of Material (BoM):

S/N	SKU	Description	Qty	Unit
A	Network Access/Admission Control (NAC)			
1	FS-HW-5140	ForeScout 5140 HW appliance	2	No

2	FS-AC-A-HW-5140-1	ActiveCare Advanced 1 year - ForeScout 5140 HW appliance	2	No
3	FS-LIC-SEECONTROL-100	ForeScout CounterACT See + Control license for 100 endpoints	30	No
4	FS-AC-A-SEECONTROL-100-1	ActiveCare Advanced 1 year - ForeScout CounterACT See + Control for 100 endpoints	30	No
5	FS-LIC-RESILIENCY-100	ForeScout CounterACT Resiliency license for 100 endpoints	30	No
6	FS-AC-A-RESILIENCY-100-1	ActiveCare Advanced 1 year - ForeScout CounterACT Resiliency for 100 endpoints	30	No
B Virtual Private Network (VPN) and Second/Multifactor Authentication (2FA/MFA)				
7	PSA5000	Pulse Secure Appliance 5000 Base System	1	No
8	SVC-WAR-PSA5000-ND	Pulse NextDay Support for PSA5000	1	No
9	STE-ENT-100CU	Pulse Secure Access Suite - Software License - Enterprise Edition - 100CU Concurrent Sessions	4	No
10	SVC-STE-ENT-GLD-100CU-1Y	Pulse Secure Access Suite - Enterprise Edition Services (Pulse One and Pulse Workspace) and Support - Direct - Gold - 100CU Concurrent Sessions - 1 Year	4	No
11	SAS Cloud - 2FA	SAS-Cloud Service - Single Unit Capacity (Plus Support 24X7) (250-499). 12 months	300	No
12	2FA Token	Token, Bundle, Safenet OTP 110, Event (6 Digit), SAS Cloud, CAPEX	300	No
13	Mobile Token	Token, MobilePASS, Software, SAS-CLOUD, CAPEX - 12 Months	300	No
C Privileged Identity/Account Management (PIM/PAM)				
14	PAS-USER-T2	Named user licenses. Including Credential Protection, Session Isolation and Recording, and Privileged Attack Detection tier 2 [25-99]. Protecting 500 Target Systems.	25	No
15	APP-ADV-PROV-T1	Advanced Application Authentication and Credential Retrieval Agents including ISV Credential Management tier 1 [1-99]	10	No
16	PAS-ADV-TARGET-UNIX-T1	Advanced Server Protection agent and Privileged Control for Linux/Unix Servers tier 1 [1-99]	10	No
17	PAS-ADV-TARGET-WIN-T1	Advanced Server Protection agent and Privileged Control for Windows Servers tier 1 [1-99]	50	No

18	WRK-ADV-T1	Advanced Endpoint Protection agent and Privileged Control for Windows and Mac endpoints tier 1 [1-999]	300	No
19	MAINT-EU24X7	EMEA 24X7 1 Year Maintenance	1	No
D	Services			
20	Professional Services	Implementation Services	1	Lots
21	Training	Training Services and Knowledge Transfer	1	Lots

5.6 Financial Information

The vendor's financial information should be included in this section. Financial information must include audited financial information for the past three years if applicable.

5.7 Resumes

The vendor must make every effort to select staff for the assignment based on Africa Re's needs. Applicable resumes should be included in this section.

6.0 COMPANY AND OTHER GENERAL REQUIREMENTS

No.	Requirement	Vendor Response
6.1	Company Information Requirements	
a)	How long has company been in business?	
b)	How long has the company been in business providing the proposed Network Security services for complex implementation projects?	
c)	State number of employees in the company.	
b)	State total number of employees dedicated to this assignment.	

7.0 CLARIFICATION AND AMENDMENT OF REQUEST FOR PROPOSAL

The vendor may request for clarification only up to 7 days before proposal submission date. Any request for clarification must be sent in writing by letter or email to the Africa Re's address indicated below. Africa Re will respond by letter or email to such requests and will send written copies of the response (including an explanation of the query but without identifying the source of the inquiry) to all firms which intend to submit proposals. Contact for clarification - Email: icttender@africa-re.com

8.0 PROPOSAL SUBMISSION

The Proposals, which must be in duplicate copies sealed in an envelope, must be delivered to the submission address indicated below and received by Africa Re not later than **December 23, 2018**. Any proposal received by Africa Re after the submission deadline shall not be considered.

Submission Address:

The Chairman of the Tenders Committee African Reinsurance Corporation

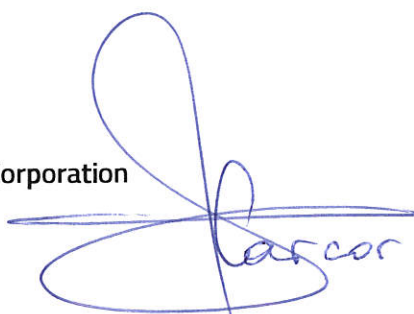
Plot 1679 Karimu Kotun Street

Victoria Island PMB 12765

Lagos, Nigeria

Email: tender@africa-re.com

For: African Reinsurance Corporation



Mr. Corneille Karekezi

Group Managing Director/Chief Executive Officer