INVITATION TO TENDER FOR THE CYBERSECURITY ASSURANCE SERVICES

This Request for Proposal invites qualified consultants or firms to provide cybersecurity assurance services to Africa Re on a renewable retainer basis following a baseline engagement. The engagement will cover technical control assurance, penetration testing, social engineering, information security governance, operational resilience, emerging technology risks, and data protection. Proposals must be received no later than **30 November 2026** and will be evaluated against the requirements and criteria set out in this document.

1. Introduction

The African Reinsurance Corporation ("Africa Re" or "the Corporation") is an international organization with a mission to foster the development of the insurance and reinsurance industry in Africa; to promote the growth of national, regional, and sub-regional underwriting and retention capacities and to support African economic development. As a supranational organisation, the Corporation was created pursuant to the Agreement establishing Africa Re which was executed in 1976 by the 42 Member-States of the African Union (AU), the African Development Bank (AfDB), 112 African insurance and reinsurance companies in Africa and 3 leading global insurance and reinsurance groups (*AXA, SanlamAllianz and Fairfax Financial Holding*). This agreement confers on the Corporation its status as a multilateral institution as well as the legal authority to operate.

With headquarters in Abuja (Nigeria), Africa Re operates through six regional offices in Abidjan (Côte d'Ivoire), Cairo (Egypt), Casablanca (Morocco), Lagos (Nigeria), Nairobi (Kenya), and Ebène (Mauritius). In addition, Africa Re has two Local Office in Addis Ababa (Ethiopia) and Khartoum (Sudan), two Underwriting Representative Offices in Kampala (Uganda) and Kinshasa (DR Congo) as well as four wholly owned subsidiaries (*Africa Re South Africa Limited in **South Africa**, African Retakaful Company in **Egypt**, Africa Re Gujarat International Finance Tec-City in **India** and Africa Re Underwriting Agency Limited in the Dubai International Financial Centre, **United Arab Emirates***).

The Corporation has the highest international financial strength and credit ratings by any indigenous reinsurer in Africa with **A (Strong / Stable Outlook)** with **Standard & Poor's** and **A (Excellent / Stable Outlook)** with **AM Best**. This is without any callable capital or preferred creditor status.

As Africa Re continues to expand its digital capabilities and strengthen technology-enabled business operations across multiple jurisdictions, cybersecurity remains a critical business priority. The Corporation recognizes that cyber threats continue to evolve in sophistication, frequency, and potential business impact. As a result, Africa Re seeks independent cybersecurity assurance to provide objective insights into the effectiveness of cybersecurity governance, risk management, operational controls, resilience capabilities, and compliance arrangements. This engagement forms part of the Corporation's broader

commitment to operational resilience, stakeholder confidence, applicable regulatory compliance, and sound risk governance.

2. Objectives

Africa Re seeks to engage a qualified and experienced consultant or firm to provide comprehensive cybersecurity assurance services for its Information and Communications Technology environment on a renewable retainer basis following the completion of the baseline engagement. The engagement shall provide independent, risk-based assurance over the design and operating effectiveness of relevant cybersecurity governance, risk management, and control processes.

The objectives of the engagement are to:

- Provide independent and objective assurance on the adequacy and effectiveness of cybersecurity governance, risk management, and internal control processes.
- Assess the effectiveness of technical, administrative, and governance controls designed to protect information assets and technology resources.
- Identify cybersecurity risks, vulnerabilities, control weaknesses, and emerging threat exposures that could impact the Corporation's strategic objectives.
- Evaluate the Corporation's preparedness, detection, response, recovery, and resilience capabilities against evolving cyber threats, including threats enabled by emerging technologies and Artificial Intelligence.
- Assess compliance with relevant cybersecurity, data protection, and industry good-practice requirements.
- Provide practical, risk-based recommendations to strengthen cybersecurity maturity, resilience, and ongoing risk management capabilities.
- Support management and governance stakeholders through periodic assurance reporting and independent cybersecurity insights.

3. Scope of Work

The cybersecurity assurance engagement shall include, at a minimum, the activities set out below. The Consultant shall apply a risk-based approach, validate findings through appropriate evidence, assess the design and operating effectiveness of relevant controls, and relate identified weaknesses to their potential business and operational impact.

For clarity and completeness, the cybersecurity assurance engagement shall be executed across the following assurance domains:

- Cybersecurity Governance and Oversight
- Cybersecurity Risk Management
- Technical Security Controls
- Security Monitoring and Incident Management
- Identity and Access Management
- Cybersecurity Awareness and Human Factors
- Third-Party and Supply Chain Security
- Operational Resilience and Business Continuity
- Emerging Technology and Artificial Intelligence Risks
- Data Protection and Regulatory Compliance.

3.1. **Cybersecurity Risk Management**: The Consultant shall assess the effectiveness of the Corporation's cybersecurity risk management processes, including:

- Identification and assessment of cybersecurity risks across critical business processes, systems, networks, and information assets.
- Evaluation of risk assessment methodologies, risk-rating frameworks, and risk appetite considerations.
- Review of cyber risk mitigation, treatment, transfer, and acceptance processes.
- Assessment of the integration of cybersecurity risks into the Enterprise Risk Management (ERM) framework.
- Review of cyber risk monitoring, reporting, escalation, and governance mechanisms.
- Evaluation of management's approach to emerging cyber threats and evolving risk exposures.

3.2. **Cybersecurity Governance and Oversight**: The Consultant shall assess the effectiveness of the Corporation's cybersecurity governance arrangements and oversight mechanisms, including:

- Review of cybersecurity governance structures, committees, and reporting lines.
- Evaluation of the roles and responsibilities of the Board, Executive Management, Audit Committee, Risk Committee, and Information Security function in overseeing cybersecurity risks.
- Assessment of cybersecurity strategies, objectives, performance measures, and reporting mechanisms.
- Assessment of management oversight over cybersecurity investments, initiatives, and resource allocation.
- Review of the integration of cybersecurity considerations into business decision-making and strategic planning.
- Evaluation of management and Board reporting related to cybersecurity risks, incidents, control weaknesses, and remediation activities.

- Assessment of the extent to which cybersecurity governance practices align with recognized standards, regulatory expectations, and industry best practices.

3.3. **Vulnerability Assessment and Technical Control Review**: The Consultant shall conduct a detailed assessment of the Corporation's internal and external ICT environment, including:

a. Internet Perimeter and External Security

- External vulnerability scanning
- Review of perimeter devices (e.g., firewalls, routers and gateways) configuration and security posture.

b. Internal Network and System Security

- Internal vulnerability scanning
- Review of access control mechanisms (logical access, privileged access);
- Assessment of email security controls;
- Wireless network security review.
- Assessment of identity and access management governance processes;
- Review of Joiner-Mover-Leaver procedures and user access lifecycle controls;
- Evaluation of privileged access management controls and monitoring activities;
- Assessment of periodic access reviews and segregation-of-duty controls;
- Evaluation of multifactor authentication implementation and effectiveness.

c. Administrative and Endpoint Controls

- Review of administrative security controls;
- Assessment of Active Directory policies and configurations;
- Mobile Device Management (MDM) controls and policies.

d. Application, Database, and Platform Security

- Database security configuration and access controls;
- Review of database security policies and procedures;
- Assessment of Microsoft Defender and Microsoft Compliance configurations.

3.4. **External Penetration Testing**: The Consultant shall perform a controlled external penetration test to simulate realistic cyberattacks against the Corporation's internet-facing systems. Testing shall be conducted only within an agreed scope, during approved testing windows, and in accordance with documented rules of engagement designed to minimise disruption to operations. The assessment shall include:

- Attempting to identify and exploit external vulnerabilities
- Testing the effectiveness of existing security controls
- Attempting to bypass perimeter defences and gain unauthorized access, where feasible
- Documenting findings, attack paths, and potential business impact.

3.5. **Social Engineering Assessment (Email Phishing)**: To evaluate employee cybersecurity awareness, the Consultant shall conduct a controlled email phishing simulation targeting a group of employees agreed with Africa Re. The simulation shall be designed and executed in accordance with approved scenarios, privacy requirements, escalation procedures, and safeguards for handling any information collected during the exercise. The assessment shall include:

- Design and execution of phishing scenarios.
- Measurement of user responses (e.g., click rates, credential submission, and reporting behaviour).
- Analysis of awareness gaps.
- Recommendations for improving employee cybersecurity awareness and training programs.

3.6. **Information Security Program Assessment**: The Consultant shall assess the organization's information security governance framework, including:

- Review of the Information Security Program structure;
- Evaluation of roles, responsibilities, and accountability;
- Review of information security policies, standards, and procedures;
- Assessment of employee cybersecurity training and awareness initiatives;
- Alignment with recognized frameworks and best practices (e.g., ISO 27001, NIST, or equivalent).

3.7. **Operational Resilience and Incident Preparedness**: The Consultant shall evaluate the organization's ability to respond to and recover from cyber incidents, including:

- Review and validation of Cyber Crisis Management Plans (CCMP);
- Assessment of incident response procedures and escalation protocols;
- Review of incident reporting, communication, and coordination mechanisms.
- Review of Business Continuity Plans (BCP) and related governance structures;
- Assessment of Disaster Recovery (DR) capabilities and recovery strategies;
- Evaluation of Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs);
- Review of business continuity and disaster recovery testing results;
- Assessment of remediation activities arising from continuity and recovery exercises;
- Evaluation of resilience against disruptive cyber incidents and operational outages.

3.8. **Artificial Intelligence (AI) Threat Assessment**: The Consultant shall assess the organization's preparedness against cybersecurity threats amplified by emerging technologies, including Artificial Intelligence. This shall include:

- Identification of AI-enabled cyber threats relevant to the organization;
- Review of controls to detect, prevent, and respond to such threats;
- Assessment of AI usage risks within the organization, where applicable;
- Recommendations to enhance resilience against AI-driven attacks.

The assessment shall also evaluate governance arrangements governing the use of Artificial Intelligence technologies within the Corporation, including:

- Acceptable-use requirements;
- Data privacy implications;
- Model governance considerations;
- Risks associated with generative AI tools;
- Third-party AI services;
- Monitoring of AI-related risks and regulatory developments

3.9. **Data Protection, Backup, and Security Policies**: The Consultant shall review data protection practices and supporting policies, including:

- Backup and disaster recovery processes;
- Incident response plans and reporting procedures;
- Employee cybersecurity awareness and training programs related to data protection;
- Alignment with applicable regulatory and data protection requirements.

3.10. **Security Monitoring and Threat Detection**: The Consultant shall assess the effectiveness of cybersecurity monitoring, detection, and response capabilities, including:

- Review of security event logging and monitoring controls.
- Assessment of threat detection mechanisms and alert management processes.
- Evaluation of security incident monitoring, escalation, and investigation procedures.
- Assessment of the adequacy of security monitoring coverage across critical systems and infrastructure.
- Review of threat intelligence utilization and integration into security operations.
- Evaluation of management reporting on cybersecurity events, incidents, and emerging threats.

3.11. **Third-Party Cybersecurity Risk Management**: The Consultant shall assess the effectiveness of controls established to manage cybersecurity risks arising from third-party relationships, including:

- Vendor and supplier cybersecurity due diligence processes.
- Review of cybersecurity requirements in contracts, service-level agreements, and outsourcing arrangements.
- Assessment of monitoring and oversight processes for outsourced and cloud-based services.
- Evaluation of third-party access controls and data protection arrangements.
- Review of critical supplier dependency risks and associated contingency measures.
- Assessment of the Corporation's ability to identify, monitor, and respond to cybersecurity incidents affecting third-party service providers.

4. Engagement Model and Delivery Cadence

Under the renewable retainer arrangement, the Consultant shall execute an Initial Baseline Assessment followed by Ongoing Targeted Assurance and Refresh Cycles scheduled bi-annually (preferably in March and October of each year). This engagement will be structured to establish a clear security baseline, track remediation progress, and provide targeted, risk-based assurance over time.

4.1. Cycle 1 - Comprehensive Baseline Assessment

The initial cycle shall serve as the baseline assessment across all specified assurance domains (Governance, Technical Controls, IAM, Operational Resilience, AI Risks, and Third-Party Risk). The objective is to evaluate the design and operating effectiveness of existing controls, establish the Corporation's baseline cybersecurity maturity level, and deliver the initial risk-rated remediation roadmap.

4.2. Cycle 2 and Subsequent Cycles - Targeted Assurance and Posture Refresh

Subsequent bi-annual cycles shall focus on maintaining continuous oversight, comprising:

- **Remediation Validation:** Testing and verifying the operational effectiveness of management actions completed since the previous assessment cycle.
- **Targeted Domain Focus:** Conducting deep-dive evaluations into specific high-risk or emerging areas as agreed upon with management prior to each cycle.
- **Postural and Maturity Refresh:** Updating the Executive Dashboard, Cyber Risk Heat Map, and Cybersecurity Maturity Assessment to reflect progress, new risk exposures, and residual risk levels.

5. Engagement Deliverables

Under the renewable retainer arrangement, **the Consultant shall conduct two cybersecurity assurance cycles annually, preferably in March and October of each year for the targeted assurance and posture refresh**. Each assurance cycle shall be performed using a risk-based methodology and shall provide independent assurance over cybersecurity governance, risk management, and control processes. At a minimum, the Consultant shall deliver the following outputs.

a. **Executive Summary**: A concise management-level report highlighting key observations, overall assurance conclusions, significant risks, management implications, and recommended actions.

b. **Cybersecurity Assurance Report**: A comprehensive report detailing:

- Scope and Methodology
- Areas Reviewed
- Findings and Observations
- Risk Ratings
- Criteria
- Root Causes

- Business Impacts
- Management Responses
- Recommendations

c. **Cybersecurity Assurance Opinion**: This is an overall professional opinion on the effectiveness of cybersecurity governance, risk management, and control processes, including an assessment of residual cyber risk exposure.

d. **Cyber Risk Heat Map**: A visual representation of identified cybersecurity risks classified according to likelihood, impact, and residual risk levels.

e. **Cybersecurity Maturity Assessment**: A maturity assessment indicating the Corporation's cybersecurity maturity level across key cybersecurity domains, benchmarked against recognized frameworks where appropriate.

f. **Management Action Tracker**: A detailed remediation register including a prioritized roadmap highlighting immediate, short-term, and medium-term remediation initiatives designed to improve cybersecurity resilience and control effectiveness. The tracker should cover:
   - Finding Reference
   - Risk Rating
   - Recommendation
   - Responsible Owner
   - Agreed Action
   - Target Completion Date
   - Implementation Status

g. **Executive Dashboard**: A summary dashboard presenting
   - Number of findings by severity
   - Risk themes and trends
   - Governance effectiveness
   - Technical control effectiveness
   - Incident readiness and resilience maturity
   - Comparative results across assurance cycles

h. **PowerPoint Presentation**: This is the presentation of key findings, assurance conclusions, risk exposures, emerging issues, and management recommendations to Executive Management and relevant governance committees.

i. **Follow-Up Assurance Activities**: The Consultant shall track the implementation status of agreed remediation actions and provide periodic updates on the effectiveness of corrective actions implemented by management.

All findings shall be assigned a risk rating based on the Corporation's risk assessment criteria and categorized as Critical, High, Moderate, or Low. Findings shall be linked to cybersecurity governance, risk

management, preventive controls, detective controls, corrective controls, and resilience capabilities where applicable.

6. Evaluation Process and Selection Criteria

Africa Re will evaluate proposals against the criteria set out below, taking into account the relevance, quality, and credibility of the evidence submitted by each Consultant. The Corporation may request clarification or supporting documentation where necessary to validate information presented in a proposal.

- In-depth knowledge of the Reinsurance/Insurance industry gained through the provision of ICT audits and relevant consulting services.
- In-depth knowledge of the International Professional Practices Framework (IPPF) of Internal Audit.
- In-depth knowledge of the control frameworks developed by ISACA in mainly Assurance, Governance, Risk and Innovation, Information and Cybersecurity.
- Demonstrated experience in conducting cybersecurity assurance engagements aligned with Internal Audit standards and professional practices.
- Ability to provide independent assurance over governance, risk management, and internal control processes.
- Experience supporting Audit Committees, Risk Committees, and Executive Management.
- Quality of proposed reporting methodology, risk-rating framework, and assurance approach.
- Experience & Expertise in ICT Audit, concerning similar projects delivered previously.
- Organization and staffing of the proposed project team.
- Proposed cost.
- Certified financial information provided.
- Quality, clarity, and presentation of the proposal.

7. Proposal Outline

To support a consistent and efficient evaluation process, responding consultants or firms shall prepare their proposals in accordance with the instructions in this section. Proposals that do not substantially follow the prescribed structure or provide the requested information may be excluded from further consideration.

Proposals shall be clear, accurate, complete, and sufficiently detailed to demonstrate the Consultant's capacity to meet the requirements of this RFP. Each proposal should present a concise description of the Consultant's relevant capabilities, proposed approach, methodology, team, deliverables, timeline, and

commercial offer. All sections, pages, figures, and tables shall be numbered and clearly labelled. Proposals shall be organised under the following major sections:

Section Titles

1. Executive Summary
2. Company Profile and Capability Statement
3. Technical Approach and Methodology
4. Organization and Staffing
5. Cost Quotations
6. Consultant's Financial Information
7. Resumes of Key Staff for the Assignment.
8. Supporting Documentation

7.1. Executive Summary

This part of the response to the RFP should be limited to a brief narrative, highlighting the Consultant'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.

7.2. Company Profile and Capability Statement

The Consultant must provide the following information about their company to enable Africa Re to comprehensively evaluate their suitability and ability to support the commitments set forth in response to the RFP. Africa Re may require the Consultant to provide additional documentation to support and/or clarify requested information.

The firm must provide the following information about their experience in ICT Audit, especially Internal Audits of ICT, following the template below:

[Using the format below, provide information on each relevant assignment for which your organization, 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 Scope included in this document. The Proposal must demonstrate that the Consultant 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.]

You are to present the information in the tabular form not exceeding 20 pages using the fields below.

- **a.** Assignment Name
- **b.** Name of Client
- **c.** Country
- **d.** Location within Country

e. Duration of Assignment (Months)
f. Approximate Value of the Services Provided by your Firm under the Contract
g. Name of Proposed Senior Professional Staff of your Firm Involved and Functions Performed
h. Start Date (Month / Year)
i. Completion Date (Month / Year)
j. Name of Associated Consultants, if any
k. Number of Professional Staff-Months provided by Associated Consultants
l. Description of Actual Services provided by your Staff within the Assignment
m. Description of Challenges Encountered, and the Strategy used to Address and Successfully close the Project including Time and Resources

7.3. Technical Approach and Methodology

In this section, you should explain your understanding of the objectives of the assignment, approach to the services, methodology to be deployed to obtain the expected output and the degree of details of such output. You should highlight the problems being addressed and their importance and explain the technical approach you would adopt to address them.

7.4. Organisation and Staffing

In this section, you should propose the structure and composition of your team to be assigned to this project. You should list the key experts and support staff that will be deployed for respective tasks. The CVs / Résumés of key staff should be added as appendices.

7.5. Cost Quotations

The proposal should include detailed cost (excluding VAT and other taxes) of services to be rendered.

7.6. Respondent's Financial Information

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

8. Clarification and Amendment

Clarifications can be requested by email only, up to five (5) business days before the date of submission of the proposal, using the Corporation's address indicated below. The subject of the email should read "**Clarification – Cybersecurity Assurance Services**".

Africa Re will respond by email to such requests. In the interest of fairness and a level playing field, all responses to such queries will be shared with all firms that have signified their intention to submit a proposal. The responses will include details of the query but without identifying the source.

Email contact for clarification: cybertender@africa-re.com

9. Proposal Submission

The following guidelines are recommended for the submission of all proposals.

9.1. General Guidelines

The proposal can be submitted by email or in hard copies or both. The proposals to be submitted as hard copies must be in a sealed envelope and marked as "**Cybersecurity Assurance Services**" while those to be submitted by email should have the subject read "**Submission - Cybersecurity Assurance Services**".

Proposals should be received by Africa Re no later than **30 November 2026**. Any proposal received by Africa Re after the submission deadline will not be considered.
Email submission address: tender@africa-re.com

9.2. Confidentiality

It is expected that the selected service provider will maintain the highest level of confidentiality regarding the information provided before, during and after the completion of the assignment. The service provider shall also maintain the highest standard of professional and ethical values and norms in providing this consultancy service and shall be required to sign a non-disclosure agreement.
The selected Consultant shall ensure that all engagement personnel maintain confidentiality over information obtained during the engagement and shall implement adequate technical and organizational measures to protect information received from Africa Re throughout the engagement lifecycle.

9.3. Intellectual Property Rights

The Corporation shall acquire the intellectual property rights on all materials, data, information and reports used, developed and produced on this engagement unless where this right is specifically excluded. All materials submitted in response to the request for proposals shall also become the property of African Reinsurance Corporation and shall not be returned to the respondent.

9.4. Other Africa Re Reserved Rights

Africa Re reserves the right, in its sole discretion, to take actions deemed in its best interest that may include any one or more of the following without incurring any liability to the affected consultant(s) or any obligation to inform the affected consultant:

- Accept or reject any, or all proposals in whole or in part at any time before engagement.
- Waive any minor irregularities or informalities in the proposal.
- Vary any timetable or schedule.
- Suspend or modify the engagement process.
- Negotiate the details of a proposal before engagement.

9.5. Ownership and Return of Proposal

All materials submitted in response to the request for proposals shall become the property of African Reinsurance Corporation and shall not be returned to the respondent.

For: African Reinsurance Corporation

Dr. Corneille Karekezi
Group Managing Director / Chief Executive Officer