Terms of Reference (TOR)

For

Information security consulting services

Background information

The African Guarantee Fund - for Small and Medium-Sized Enterprises Ltd (AGF) is a Pan-African non-bank financial institution founded by the Ministry of Foreign Affairs on behalf of the Government of Denmark through the Danish International Development Agency (DANIDA), Ministry of Foreign Affairs and Cooperation on behalf of the Government of Spain through the Spanish Agency for International Development Cooperation (AECID) and the African Development Bank (AfDB) in 2011. AGF has since been joined by the Agence Française de Développement (AFD), the Nordic Development Fund (NDF), Investment Fund for Developing Countries (IFU) and KfW.

AGF's primary mandate is to assist financial institutions (FIs) in Africa to scale up their SME financing through the provision of partial loan guarantees and capacity development assistance. It seeks to bridge the financing gap across the continent for SMEs. AGF products and services provide FIs with the means, which they can leverage in bringing their African SME financing interventions to the required scale.

AGF contributes to the promotion of economic development, vital for prosperity, stability and poverty reduction in Africa through two lines of activity:

a. Provision of a mix of financial guarantees and other products, which reduce the risks sustained by FIs when lending to SMEs that have insufficient collateral. These guarantees contribute to reduce the inability of SMEs to provide acceptable guarantees required by FIs prior to lending.

b. Support for capacity development of the partner FIs to enhance their capacity to appropriately assess loan requests from SMEs and to mitigate risks associated with the guarantee.

AGF operates according to market principles and is a commercially viable venture with operations in 40 countries in Africa and is gradually expanding to other countries to cover the whole of Africa. AGF is rated 'AA- 'by the globally renowned Fitch Ratings Agency.

Objective of the Assignment

The objective is to recruit an information security consultant in order to perform a full ICT (Information, Communication and Technology) and cybersecurity risk assessment and make appropriate recommendations to improve the current systems and policies in accordance with international recognized standards and practices.

Scope of Work

Description

The Information Security consultant is responsible for understanding and responding to threats to the security of all information, networks, and computer systems, whether on premise or cloud. The individual taking the role will monitor a variety of services and tools (including firewalls, internal account activity tools and threat information services) in order to predict, detect and diagnose threats and direct or participate in the mitigation of these threats to the business together with the ICT team and Internal Control Team.

Responsibilities

Information Security Consultant would be responsible for the following:

- Monitor information systems, computers and networks to detect cyber threats and respond to cyber threats and finally to remediate information security threats and vulnerabilities.
- Analyze, design, and facilitate capabilities, solutions, or preventative/remediation controls to protect proprietary/confidential data and systems in accordance with industry standards and governance/compliance requirements.
- Review the current procedures in information security, Technical Incident Response Planning and Business Continuity Planning and advice whether they require revision.
- Synthesize solution design, architectural patterns, policy and regulatory frameworks, privacy considerations, and risks in the creation of holistic solutions that span technologies and capabilities.
- Support the front-line defense of networks, protecting information from unauthorized access and violations. Analyze and assess potential security risks, develop plans to deal with such incidents by putting measures in place such as firewall, IPS encryption, monitoring and auditing systems for abnormal activity, and executing corrective actions. Prepare technical reports.
- Carry out tests on a system to expose weaknesses in security. Essentially, do everything a hacker would do, but do it on behalf of the organization who owns the network, for example, access information without usernames and passwords, and will try to break through whatever security applications are in place. Report findings and then suggest what upgrades/solutions to be implemented
- Analyze computer and server logs and uncover links between events, groups and individuals through pursuit of data trails
- Work across different operating system platforms and technologies to design holistic security designs that treat identified risks and enable strategic and/or tactical business or IT solutions
- Research/investigate emerging business application security topics, threats, capabilities, and solution options to create/update policy and governance, technology strategies, solution architecture and vulnerability assessments

- Applies industry standard risk management technique and knowledge across various business application security capabilities, that is , technical, application, data and mobile to determine effectiveness of controls and to create action plans that remediate identified risks
- Apply broad-based knowledge of security technologies with an in-depth/specialized knowledge of security tools like Nmap, Open VAS, Snort, Wireshark, Kali Linux etc.
- Apply systems analysis techniques, including consultations with users to determine security specifications
- Suggest and provide advice on the best solutions to backup sensitive and confidential data on the cloud for disaster recovery

Competencies

- **Analysis:** Identify and understand issues, problems and opportunities; compare data from different sources to draw conclusions.
- **Communication:** Clearly convey information and ideas through a variety of media to individuals or groups in a manner that engages the audience and helps them understand and retain the message.
- **Exercising Judgment and Decision Making:** Use effective approaches for choosing a course of action or developing appropriate solutions; recommend or take action that is consistent with available facts, constraints and probable consequences.
- **Technical and Professional Knowledge:** Demonstrate a satisfactory level of technical and professional skill or knowledge in position-related areas; remains current with developments and trends in areas of expertise.
- **Building Effective Relationships:** Develop and use collaborative relationships to facilitate the accomplishment of work goals.
- **Client Focus:** Make internal and external clients and their needs a primary focus of actions; develop and sustain productive client relationships.

- Demonstrated ability to describe non-functional requirements and translate into architecture constraints.
- Experience with banking and financial systems and business processes.

Work Experience

- Minimum ten (10) years of experience working daily with network or host-based threat detection technologies.
- Must be pro-active and a self-starter as this position requires a lot of independent work.
- Knowledge of networking technologies and protocols, including Ethernet, VLANs, TCP/IP and routing.
- Experience with security technologies including: Vulnerability Scanning, Firewalls & Log Analysis, Host-based detection tools, Security Event and Incident Management (SEIM), Antivirus, Network Packet Analyzers, malware analysis and forensics tools.
- Experience in analyzing audit logs, router logs, firewall logs, IDS logs and TCP/IP headers.

Reporting requirements/deliverables

The Information Security Consultant will need the following reporting requirements/deliverables, but not limited to:

1. Inception report. The inception report should mainly include: how the firm understands/interprets the ToRs; any additions/clarifications to the ToRs; a refined methodology to be adopted; action plan; expectations from AGF; and the preferred payment schedule.
2. Work plan of the security assessment.
3. Progress reports.
4. Vulnerability assessment technical review report.
5. Technical Incident Response review report
6. Business Continuity review report.
7. Cybersecurity policy and procedure

8. Any other report, as required.

Confidentiality

By accepting to take part in the invitation, you agree to keep in confidence all information provided to you, whether written or oral, in relation to the invitation and/or in relation to the organization's business generally which is not already in the public domain, to use it only for the purposes of this bid and for no other reason and not to disclose any of the said information to any third party.

Application

Please submit (**through the email below**) your Technical Proposals (including CVs of proposed staff), Financial Proposal (including proposed payment schedules) to the following address, on or before **June 11, 2021.** In case of any clarification, please channel them through the same email address.

Email subject: **"**IT Security consultant application**"**

Email: reception@africanguaranteefund.com