REQUEST FOR PROPOSAL FOR CYBERSECURITY SERVICES

NCBA BANK RWANDA PLC

OCTOBER 2020

Contents

1. **Invitation and Scope**

   NCBA BANK RWANDA PLC invites qualified Firms to submit proposals for the following services

   - Vulnerability assessment and penetration testing
   - Cybersecurity framework assessment
   - Cybersecurity awareness training

   The objective of this scope is to obtain an assurance from an independent third party on the control environment of NCBA Banking systems and network. And also educate the Board members and management team about the importance of information security, current cyber-security threats and trends as well as the controls that should be in place to secure the Bank's information.

2. **Contact**

   For the purposes of this procurement process, the "RFP Contact" will be:

   Email: procurementcba.rwanda@ncbagroup.com
   Tel: +250 788149500
   All inquiries shall be channeled through these contacts.

3. **Content of proposal**

   The proposal shall contain the following;

   - The profile of the bidder
   - Experience in the cybersecurity field by indicating the previous executed contracts in VAPT, Cybersecurity audit and awareness programs
   - Profile/CVs of the staff to represent the firm in each respective area of work to be done.
   - The bidder should also provide RDB certificate of registration and Tax clearance certificate.
   - Technical proposal
   - Financial and pricing element

4. **Submission of Proposals**

   The proposals shall be submitted to through email address: procurementcba.rwanda@ncbagroup.com

   The Proposal must be delivered to the address above on or before 16: 00 GMT on the 30th day of November 2020.

5. Eligibility

The invitation to bid is open to all bidders who fulfils below criteria

1) The bidder must be a Rwandan registered institution
2) The Bidder should be a regular player in cybersecurity terrain
3) The Bidder has completed at a minimum;
    a. Three commercial VAPTs in preferably in the financial sector
    b. Three commercial cybersecurity awareness campaigns preferably in financial sector
    c. Three commercial cybersecurity audits and/or IT Audits
    d. Three years of consecutive and proven expertise in the cybersecurity/IT audit area
4) The engineers representing the Firm should be Certified in the Information Security domain and Information systems Audit

6. Responsibility of the selected bidder

- *Successful bidder must ensure that during the VAPT, level of intrusiveness and boundaries of testing are not violated. The bidder should adhere to applicable laws, rules, regulation and guidelines prescribed by various regulatory, statutory and government authorities during the execution of the test.*

- *The selected bidder exercise adhere to NDA signed with the bank before commencement of the engagement*

7. Technical Requirements

7.1. Vulnerability assessment and penetration testing

a. The bidder elaborate on the following;
    1. Approach to the pentest and vulnerability assessment. The bank expects at least the following;
        i. External VAPT
        ii. Internal VAPT
    2. The methodology to be used
    3. The red team approach must be used during the VAPT
    4. Should indicate the deliverables. The Bank expects at a minimum VA and pentest Reports that contain;
        i. Management summary with overall severity
        ii. Detailed results for vulnerabilities discovered, exploited and proof of concepts

iii. Detailed explanations of the implications of the findings by indicating the business risk and impact of the identified exposure
iv. Remediation recommended to close the deficiencies identified.
v. Detailed steps (wherever/whenever applicable) to be followed while mitigating the reported deficiencies. Security issues that pose an imminent threat to the system are to be reported immediately.
vi. Reports to be delivered in a password protected Adobe(.pdf) and MS word(.doc formats

7.2. Cybersecurity framework assessment

The bidder shall provide assurance on the control environment of NCBA Bank's cybersecurity in relation to National Bank of Rwanda cybersecurity regulation.

The approach is to benchmark the NBR cybersecurity regulation and best practices under the following standards;

- National Institute of Standards and Technology (NIST)
- SysAdmin, Audit, Network and Security (SANS)
- ISO 27001

Also, the bank expects the selected firm to assess the sufficiency of the banks cyber resilience framework including:

- ***Governance****:* Review arrangements that are in place to establish, implement and review the bank's approach to managing cyber risks.
- ***Identification:*** *identify the critical business functions and supporting information assets that should be protected, in order of priority, against compromise;*
- ***Protection:*** *Assess the effectiveness of controls in line with leading-practice cyber resilience standards that protect the confidentiality, integrity and availability of its assets and services in order to prevent, limit and contain the impact of a potential cyber incident.*
- ***Detection****: Evaluate monitoring and process tools that are in place to enable the bank detect the occurrence of anomalies and events indicating a potential cyber incident;*
- ***Response and Recovery:*** *Evaluate bank's design and testing of systems and processes to enable the safe resumption of critical operations within the best practice guideline of two hours of a disruption; and*
- ***Testing:*** *Reviewing elements of the cyber resilience framework that should be rigorously tested to determine their overall* effectiveness.

7.3. Cybersecurity awareness training

a. Target groups

The Firm shall develop a cybersecurity awareness program for the following target groups

1. The NCBA Board of Directors
2. The NCBA Senior Management Team
3. The Critical third-party service providers

Below table provides a summarized information on target groups

No	Target Group	Number	Frequency
1	Board of Directors	9	Quarterly
2	Senior Management	12	Twice a year
3	Vendors & Customers	N/A	Once

b. Expectations:

The Firm is expected to design and deliver an awareness program that is in line with recognized Information security standards (ISO 27001: 2013, NIST and etc.)

Board of Directors

At a minimum, the Firm shall educate the Board members on information related to the importance of information security, current cyber-security threats and trends as well as the controls that should be in place to secure the Bank's information. The firm shall conduct quarterly awareness sessions in 2021

Senior Management

The awareness shall be scoped to cover the senior management cybersecurity responsibilities, Best practices, current global and local information security threats and trend in financial sector and evaluation of bank employees in relation to cybersecurity. The firm shall conduct quarterly sessions in 2021

Third Party service providers and customers

The firm shall provide guidance on how the bank can target the customers and third party service providers for an effective cybersecurity awareness.

c. The mode of delivery

The mode of delivery differs with Target group

No	Target Group	Channel
1	Board of Directors	Online session like MS teams, Zoom or Webex
2	Senior Management	Online session like MS teams, Zoom or Webex
4	Vendors & Customers	Documentation

----------END----------