RESERVE BANK OF MALAWI

REQUEST FOR PROPOSALS

(CONSULTING SERVICES – FIRMS SELECTION)

ASSESS AND DESIGN A CYBER SECURITY OPERATIONS CENTRE (C-SOC)

The Reserve Bank of Malawi (the Bank) was established under an Act of Parliament with the primary objective of maintaining price and financial stability. To fulfill part of this mandate, the Bank has over the years procured, developed and implemented a number of digital solutions and applications. The digitalization efforts have come along with associated cyber threats and risks that require vigilance to enhance the cyber resilience of the systems and critical infrastructure of the Bank. Therefore, as the threat landscape continues to evolve, cybersecurity efforts must follow suit.

To this end, the Bank invites reputable and experienced firms to submit their proposals for the assessment of the existing deployed cyber security solutions and design of an on-premise Cyber Security Operations Centre (C-SOC). As a crucial component of the Bank's commitment to fortifying cybersecurity resilience, the CSOC will play a vital role in safeguarding the Bank's financial infrastructure.

The key requirements include:

1. Technical Expertise:
    - Demonstrable experience in the review or assessment of the deployed cyber security solutions for financial institutions or similar critical sectors.
    - Demonstrable experience in designing CSOCs for financial institutions or similarly critical sectors.
    - Expertise in deploying advanced cybersecurity technologies, threat intelligence, Detection of Information Security Threat & Prevention of Impact/ Breach, incident response capabilities.
2. Innovation and Scalability:
    - Proven track record in delivering innovative and scalable CSOC solutions to adapt to evolving cyber threats and organizational growth.
3. Regulatory Compliance:
    - Ability to design a CSOC framework that aligns with international standards and industry best practices.
4. Collaboration and Training:
    - Experience in fostering collaboration among internal and external stakeholders.
    - Comprehensive training programs for CSOC staff to ensure proficiency in handling sophisticated cyber threats.
5. Incident Response and Recovery:
    - Demonstrated capabilities in rapid incident response and effective recovery strategies to minimize potential disruptions.

The Bank now invites interested eligible firms to provide technical and financial proposals demonstrating that they have the required qualifications and relevant

experience to perform the Services. Submissions should be technical and financial proposals. The assessment criteria are:

(i) Core business of the firm(s) and years in business. a profile of the company, its organization and staffing and at least 5 years in carrying out similar assignment of designing or implementing CSOCs or other related assignments.

(ii) Relevant experience in carrying out the assignment. Details of experience or similar assignments undertaken in the past five years, including their locations with focus on the firm's role in the assignments.

(iii) Technical and managerial capability of the firm (Provide the structure of the organization, general qualifications, and number of key staffs).

(iv) The proposed team should have at least one of the following certifications CISSP/GIAC/CISA/CISM/CCNA/GSEC and have a defined scope cybersecurity experience of at least 5 years.

(v) Curriculum vitae of all Specialists and levels of experience of the people that will work on this project. Preference is on specialists who are certified in internationally recognized cybersecurity certifications and experience in setting up Security Operations Centre in Central Banks or organizations of similar nature.

(vi) Project team leader a minimum academic qualification of a master's degree in ICT, Information Security or cybersecurity with a minimum experience of 10 years of which 5 years should be on managing projects of similar nature. Certification on ICT projects management is highly recommended.

(vii) Project member with a minimum academic qualification of a Bachelors' degree in information security or cybersecurity. In addition to academic qualifications, member should also have relevant cybersecurity certifications.

(viii) The provider must list all sites where they have undertaken work of similar nature.

(ix) Bidder must warrant that key project personnel to be deployed in this project have been sufficiently involved in the similar project in the past. Along with the proposal the bio-data of the persons doing the work be submitted indicating their qualifications, professional experience and projects handled.

(x) References from institutions where similar projects were implemented preferably at a central bank level or related sectors.

The assignment is expected to be undertaken within 40 days from contract signing date.

Bidding document can be collected from of charge through formal requesting using the following e- mail; procurement@rbm.mw .

Selection of the firm will be in accordance with the Quality and Cost based selection method as set out in the Malawi Government Public Procurement and Disposal of Public Assets Act, 2017.

Bids clearly marked; **"Tenders for assess and design a cyber security operations centre (c-soc)"** should be delivered to the address shown below on or before **08 October 2024** at **10:00 Hours.** Bids will be opened in the presence of the bidders' representatives who may choose to attend at the address shown below.

Address for inspection, clarification and collection of bidding documents:

Reserve Bank of Malawi
Business Reception
Convention Drive,
Lilongwe

Address for submission of bids:

The Chairperson,
Business Reception
RBM Internal Procurement and Disposal Committee,
P.O Box 30063,
Lilongwe,
Malawi.

Address for Bid Opening:

Reserve Bank of Malawi,
Floor 5, Auditorium,
Lilongwe,
Malawi.

Chairperson
RBM Internal Procurement and Disposal Committee