TANZANIA MORTGAGE REFINANCE COMPANY LIMITED (TMRC) TERMS OF REFERENCE FOR CYBERSECURITY CONSULTANCY.

1. INTRODUCTION.

Tanzania Mortgage Refinance Company Limited (TMRC) is a specialized financial institution established to support financial institutions in extending long-term mortgage loans to the public. TMRC operates as a private sector driven institution regulated by the Bank of Tanzania, providing liquidity to mortgage lenders through refinancing. TMRC was established in 2011 with support from the Government of Tanzania and the World Bank with the initial aim of supporting member banks to extend long-term mortgage loans to the public through the provision of long-term funds.

2. PURPOSE.

TMRC intends to engage a consultant to undertake a comprehensive cybersecurity maturity assessment and design an appropriate control framework that will allow the organization to gain a better understanding of its business processes to optimize its cyber security posture.

The range of activities to be undertaken during the assessment are enumerated in the scope of work provided in subsequent sections of this document.

2.1 Objectives of the Consultancy

- Verify whether the cyber security maturity levels are adequate in comparison to the risks, international cyber security frameworks and best practices.
- To establish the current cybersecurity state of business processes and procedures.
- Determine the overall cybersecurity maturity level of the organization and gaps thereof.
- Make recommendations on the measures to be taken to improve the Cyber Security maturity from the current level to a desired level.
- Develop a policy and process manual for cybersecurity for TMRC.

The Cybersecurity maturity assessment should cover the following key areas;

- **Leadership and governance:** to assess ownership, effective management of risk and Governance mechanisms at TMRC.
- **Information risk management:** to review the approach at TMRC for assessing, managing and monitoring risks associated to sensitive / confidential information.
- **Human factors:** review the security culture at TMRC to confirm if it empowers and helps ensure the right people, skills, culture and knowledge is conveyed to TMRC stakeholders including staff and third parties to protect the company against cyber security threats.
- **Third parties:** to review processes for identifying and managing the risk to TMRC information throughout the lifecycle of an external party in efforts to protect the company against potential cyber risks.
- **Resilience:** to assess the capabilities in place to protect TMRC against cyber risks, defend, and recover against cyber-attacks.

- **Legal and Compliance factors:** to assess TMRC's compliance against relevant regulatory and international certification standards.
- **Technical Security:** to review security solutions implemented to address identified cyber risks and protect the company against data theft.
- **Security Architecture:** to ascertain alignment of information systems with security objectives, to address potential risks to the cyber environment at TMRC.
- **Security operations:** to confirm processes for identifying and proactively preventing compromise of sensitive information and computer systems.

2.2 Scope of Work.

The Scope of work for the Consultancy shall comprise of:

i. Performing a Gap Assessment of TMRC's existing infrastructure with respect to globally accepted cybersecurity standards and best practices:
   - Review & Identify gaps with respect to Cyber Security/Resilience Framework (gaps assessment).
   - Perform a comprehensive vulnerability assessment and penetration testing as part of gap analysis using standard tools.
   - Discuss with management existing gaps in infrastructure, architecture, process and systems.
   - Review the existing processes, procedures, and systems for their adequacy and efficiency.
   - Identify gaps in TMRC's Cyber threat detection mechanisms.
   - Recommend controls required to mitigate the gaps.

ii. Creating an Assessment Report based on the gap analysis above including, but not limited to:
   - An executive summary with objectives, scope, background, summary of findings, and recommendations
   - Identification of TMRC's cybersecurity maturity gaps.
   - Recommendations for eliminating, or mitigating, security risks and increasing cybersecurity maturity levels.
   - Summary of areas reviewed/examined along with the methodologies/procedures used.
   - Recommendations on industry standards, security frameworks / best practices to mitigate and bridge the gaps.
   - Current Maturity level of the organization and desired level of maturity.
   - List of key initiatives/ Projects that must be undertaken to achieve the desired maturity level.
   - Implementation roadmap of remediations to reach the target maturity.

iii. Develop a Policy and Process for cybersecurity
   - Develop a policy and a process manual for cybersecurity for TMRC.
   - Provide training to TMRC staff on cybersecurity.

3. QUALIFICATION REQUIREMENTS FOR THE CONSULTING FIRM.

The consulting firm should meet the following requirements:

- The consulting firm should have experience of more than 5 years in conducting cybersecurity assessments of similar nature.

- The consultant must demonstrate competence in conducting comprehensive Cybersecurity Maturity Assessments and design of Cybersecurity Control Frameworks. All bidders must provide a list of at least three (3) Cybersecurity Assessments successfully conducted within the last five (5) years.
- All the Consultancy team members that are proposed to participate in the project must have bachelor's degree in ICT, Computer Science or a related field with relevant Professional Qualification i.e., CISA, CRISC, CEH or equivalents.
- The Team Leader must have more than 5 years' hands on experience in Cybersecurity and IT Assessments; and must possess a great understanding of IT risk, IT Management and Governance demonstrated through certifications such CISA, CISM, CRISC and PRINCE2/PMP.
- At least two of the proposed key personnel must have not less than 3 years' experience in undertaking comprehensive Cybersecurity Maturity Assessment and Cybersecurity Control Framework design for large and medium financial institutions.
- Consultancy team members proposed to participate in the project must be members in good standing with relevant professional bodies.

4. SUBMISSION REQUIREMENTS.

Interested firms should submit the following documents:

i. Company profile clearly stating experience in Cybersecurity Maturity Assessments and Cybersecurity Control Framework Design.
ii. Technical Proposal describing the proposed cybersecurity maturity assessment and cybersecurity control framework design methodology.
iii. Compliance certifications and regulatory adherence details.
iv. Financial proposal including service fees and implementation costs.
v. At least three (3) Cybersecurity Assessments successfully conducted within the last five (5) years.
vi. At least three references from similar engagements.

5. DEADLINE AND CONTACT INFORMATION.

All proposals must be submitted online via the TMRC Procurement Portal not later than 1600hrs on 10th July 2025 addressed to;

The Chief Executive Officer,

Tanzania Mortgage Refinance Company Limited,

P.0 BOX 7539,

Dar es Salaam.

ATTN: Chief Operations Officer

N.B:

In case of any technical challenges on the procurement portal on the URL address {https://eprocurement.tmrc.co.tz/} kindly contact the below;

Email: jmlimbilah@tmrc.co.tz / ITsupport@tmrc.co.tz; Phone : +255(0) 757 858289

6. BID OPENING

A consulting firm that wishes to participate in the bid opening should send an email to procurement@tmrc.co.tz indicating the names and email addresses of the participants.

TMRC reserves the right to accept or reject any proposal without providing reasons.