ACCOUNTANT GENERAL'S DEPARTMENT

REQUEST FOR EXPRESSION OF INTEREST
(CONSULTING SERVICES - FIRM SELECTION)

SHORTLISTING SELECTION- FIRM

Name of Country	***:***	***MALAWI***
Name of Project	***:***	***INTEGRATED FINANCIAL MANAGEMENT INFORMATION SYSTEM (IFMIS)***
Project Funding	***:***	***GOVERNMENT OF MALAWI***
Assignment Title	***:***	***ENTERPRISE CYBER SECURITY MONITORING AND THREAT DETECTION SOLUTION***
Consultancy Ref. No	***:***	***AGD/ICT-ECSMT/26-27/04***
Date of Issue	***:***	***26th November, 2026***
Date of Submission	***:***	***03rd December, 2026; 10:00 Hr Local Time***

---

1) Background

The Accountant General's Department seeks to procure and implement an Enterprise Cybersecurity Monitoring and Threat Detection Solution to strengthen the institution's cyber resilience, improve visibility across ICT infrastructure, and enhance the ability to detect, investigate, and respond to cybersecurity threats in real time.

The solution should provide comprehensive monitoring of network, user, endpoint, email, cloud, and application activities to proactively identify malicious, suspicious, or abnormal behaviour that may indicate cyber threats, data breaches, insider threats, or system compromise

2) What the solution should be able to provide

The proposed solution shall:

- Enhance visibility across the Department's ICT infrastructure.
- Detect cyber threats in real time.
- Identify previously unknown and emerging threats.
- Reduce the time required to detect and respond to security incidents.
- Strengthen protection against ransomware, phishing, malware, insider threats, and data exfiltration.
- Support compliance, audit, and governance requirements.
- Improve security operations through automation and intelligent analytics.

3) Critical features the solution must have

3.1 Intelligent Threat Detection

The solution shall:

- Utilize advanced analytics, artificial intelligence, and machine learning techniques to establish behavioural baselines for users, devices, applications, and network activities.
- Detect anomalous activities and suspicious behaviour that deviate from established baselines.
- Identify both known and previously unknown cyber threats.
- Continuously adapt to changes within the environment without extensive manual rule creation.

3.2 Continuous Security Monitoring

The solution shall provide:

- 24/7 monitoring of network traffic and ICT infrastructure.
- Real-time visibility into user activities and system interactions.
- Monitoring of internal and external communications.
- Centralized visibility through a unified management dashboard.

3.3 Automated Threat Response

The solution shall:

- Support automated or semi-automated response actions.
- Enable rapid containment of suspicious activities.

- Minimize operational disruption while responding to threats.
- Support configurable response policies and workflows.

3.4 Insider Threat Detection

The solution shall:

- Monitor user behaviour and privileged account activities.
- Detect unusual access patterns and unauthorized activities.
- Identify potential insider threats and compromised user accounts.
- Generate alerts for abnormal data access and transfer activities.

3.5 Data Protection and Exfiltration Monitoring

The solution shall:

- Detect unusual movement of sensitive information.
- Identify unauthorized transfers of data to external destinations.
- Monitor large-scale downloads, uploads, and file-sharing activities.
- Generate alerts for potential data leakage incidents.

3.6 Email Threat Protection

The solution shall:

- Detect phishing attacks, malicious attachments, and suspicious email communications.
- Identify business email compromise attempts.
- Provide visibility into email-based threats targeting staff members.
- Support proactive identification of emerging email threats.

3.7 Cloud and Hybrid Environment Monitoring

The solution shall:

- Support monitoring of cloud-based services and hybrid environments.
- Detect suspicious cloud access activities.
- Monitor user access to cloud resources and applications.
- Provide visibility into cloud security risks.

3.8 Visibility and Reporting

The solution shall provide:

- Executive dashboards for management.
- Operational dashboards for ICT and Security teams.
- Real-time alerts and notifications.

- Historical analysis and trend reporting.
- Incident investigation and forensic reporting capabilities.
- Customizable reports for audit and compliance purposes.

3.9. Integration Requirements

The solution shall integrate with:

- Active Directory and identity management systems.
- Existing firewalls and network security devices.
- Endpoint protection and endpoint detection solutions.
- Email platforms.
- Virtualization platforms.
- Security Information and Event Management (SIEM) platforms where applicable.
- Cloud platforms and services.

3.91. Scalability and Performance

The solution shall:

- Support future growth in users, systems, and network traffic.
- Operate without significant degradation in performance.
- Support distributed and multi-site environments.
- Accommodate future digital transformation initiatives.

3.92. Operational Benefits

The proposed solution is expected to deliver the following benefits:

- Improved visibility across the ICT environment.
- Faster identification of cyber threats.
- Reduced risk of ransomware and malware outbreaks.
- Early detection of insider threats.
- Improved incident response capabilities.
- Reduced operational workload through intelligent automation.
- Enhanced protection of sensitive government information.
- Improved decision-making through actionable security insights.
- Strengthened overall cybersecurity posture of the Department.

4. Deliverables

- Inception report and detailed work plan (within 2 working days of contract signing).
- Software licenses.
- Installation and configuration services.
- Integration with existing ICT infrastructure.
- Knowledge transfer and administrator training.
- Technical documentation.
- Post-implementation support and maintenance services.
- Warranty and vendor support arrangements.

5. Eligibility and Qualification Criteria

The Accountant General's Department seeks the services of firm with the following minimum qualifications;

The firm must demonstrate:

Technical Expertise

- Proven experience in implementing Enterprise Cybersecurity Monitoring and Threat Detection Solution and dSOC for financial Institutions or similar critical sectors.
- Strong expertise in deploying advanced cybersecurity technologies, threat intelligence, Detection of Information Security Threat & Prevention if Impact/Breach, incident response capabilities.

Innovation and Scalability:

- Proven track record in delivering innovative and scalable Enterprise Cybersecurity Monitoring and Threat Detection Solution and dSOC solutions to adapt to evolving cyber threats and organizational growth.

Regulatory Compliance

- Ability to design and implement Enterprise Cybersecurity Monitoring and Threat Detection Solution architecture and dSOC services that align with international standards and industry best practices.

4.Collaboration and Training

- Experience in fostering collaboration among internal and external stakeholders.

- Comprehensive training programs for Cybersecurity Staff on Enterprise Cybersecurity Monitoring and Threat Detection Solution to ensure proficiency in handling sophisticated Cyber threats using this solution.

5.Incident Response and Recovery:

- Demonstrate capabilities in rapid incident response and effective recovery strategies through Enterprise Cybersecurity Monitoring and Threat Detection Solution to minimize potential disruptions

The firm shall have staff who possess the following;

- The proposed team should have at least one of CISSP/CIAC/CISA/CISM/CCNA/CSEC certification and provide defined scope experience of at least 5 years on this solution
- Project members with a minimum academic qualification of a Bachelor's degree in information security or cybersecurity. In addition to academic qualifications, members should also have relevant cybersecurity certifications

1. Lead Engineer

Qualifications

Education

Cisco Certified Network Associate
Cisco Enterprise Core Technologies
CompTIA Security+
CompTIA Network+
Microsoft Certified Technology Specialist (MCTS)
Microsoft Certified Professional (MCP)
DSOC Certified Cyber Analyst

Experience, Technical Skills and Competencies

- managing and coordinating ICT infrastructure and cybersecurity projects.
- information security governance, risk management and security policy implementation.
- coordinating technical teams, vendors and stakeholders in ICT security initiatives.

- overseeing security monitoring, threat management and incident response activities.

2. Network Security Engineer

Qualification

CCNA, Cisco Enterprise Core Technologies,

CompTIA Network+

practical networking/firewall experience

Experience, Technical Skills and Competencies

- **Network Engineering:** Network configuration, routing, switching, connectivity and troubleshooting.
- **Cybersecurity:** Security principles, vulnerability identification, risk management and security controls.
- **Security Operations:** Cyber threat monitoring, security event analysis and incident identification.
- **Enterprise Networking:** Cisco enterprise network technologies and infrastructure management.
- **Systems Administration:** Microsoft technologies, IT systems support and troubleshooting.
- **Network Security:** Network protection, access control and secure network implementation.
- **Technical Support:** IT problem-solving, infrastructure maintenance and systems troubleshooting.

3. Cybersecurity Analyst

Qualification

CompTIA Security+

DSOC Certified Cyber Analyst

Security monitoring threat detection and incident analysis

Experience, Technical Skills and Competencies

- Security monitoring and analysis of network activities.
- Identifying suspicious network behaviour and potential cyber threats.
- Conducting vulnerability assessments and security investigations.
- Analysing security alerts and supporting incident response.

- Preparing cybersecurity incident and threat assessment report
- Security Information and Event Analysis.
- Threat detection and investigation.
- Cybersecurity incident response and handling.
- Vulnerability assessment and security analysis.
- Threat intelligence and behavioural analysis.
- Security monitoring and reporting.

For all the proposed team as highlighted above, Lead Engineer, Network Security Engineer and Cybersecurity Analyst, Curriculum Vitae with certifications and identity (Passport or National ID) must be submitted.

6. **Duration of the Assignment**

The installation and configuration of the solution is expected to be completed within **4 weeks** from the date of contract signing. The licenses should be valid for **2 years'** period.

7. **Reporting and Coordination**

The vendor will report directly to the **Accountant General's Department** through the **IFMIS Director**. All major deliverables and change requests must be formally approved by the designated IFMIS technical team.

8. **Selection of Firms**

Expression of Interest (EoI) will be evaluated or selected in accordance with the Public Procurement and Disposal of Asset Act No 7 of 2025 and Public Procurement Regulations 2025 of the Republic of Malawi under shortlisting. Participation is open to all eligible firms.

9. **Submission of Expression of Interest**

Interested eligible firms may submit expression of Interest to the Accountant General's Department (AGD), stating their interest and attaching the following documents for assessment;

Bidders must meet the following minimum requirements,

i. Official letter on letterhead expressing interest together with the financial proposal for carrying out the assignment
ii. Detailed company profile that includes number of years in providing similar services in Malawi or elsewhere, number of professional staff (permanent / temporary) qualified to perform the services as mentioned above
iii. Relevant Experience of at least **4 years** in implementing, managing and supporting **Enterprise Cybersecurity Monitoring and Threat Detection Solution**, preferably in the public sector (2021-2022 FY, 2022-2023 FY, 2023-2024 FY, 2024-2025 FY), by attaching system generated Local Purchase Orders (LPO); Copy of signed contracts by all parties; approved and accepted deliverable reports, proof of payment and payment vouchers
iv. Detailed holder signed Resumes (CVs) for key personnel; for Key personnel's who will undertake this assignment and their specific experience on projects of similar magnitude.
v. Economic capacity (turnover of the last 3 years)
vi. Copies of business registration certificates and business licenses,
vii. Copies of Tax Clearance Certificate, current and valid
viii. Audited Financial Statements for the past three (3) Years- (2022-2023 FY, 2023-2024 & 2024- 2025)
ix. Partnership or joint venture agreements where applicable

Interested firms may obtain further information from the Procurement and Disposal Unit +265 9 995 8 55 15 or email: *procurement@agd.gov.mw.* or from the address below during working hours from 08:00 am to 12.00 noon and from 13.00 hours pm to 16.30 hours on all working days

Sealed Expressions of Interest- EoI {One ORIGINAL & Four COPIES must be deposited in the tender box at the address below in person by **03rd December, 2026 before 10:00 hours local time** and the sealed envelope must be clearly **marked "**
Expression of interest for *Enterprise Cybersecurity Monitoring and Threat Detection Solution*

Address of Submission

The Chairman,

Internal Procurement and Disposal Committee,

Accountant General's Department,

Ground Floor, Tender Box placed at the entrance

Capital Hill

P.O. Box 30140,

Lilongwe 3.

Malawi

Email : *procurement@agd.gov.mw*

Phone : +265 9 998 555 15