



---

**REQUEST FOR PROPOSALS FOR PROVISION, IMPLEMENTATION AND SUPPORT OF  
A SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM  
MGL/SIEM/01/2026**

---

VENDOR'S NAME: .....

**Table of Contents**

**1 CORPORATE OVERVIEW ..... 3**

**2 INVITATION TO TENDER ..... 3**

**3 TENDERING INSTRUCTIONS..... 3**

3.1 Submission of Tender Documents .....3

3.2 Clarifications .....3

3.3 Additional Information .....4

3.4 Withdrawal of Tender .....4

3.5 Tender Currencies.....4

**4 TECHNICAL PROPOSAL & EVALUATION ..... 4**

**5 TECHNICAL PROPOSAL SUBMISSION FORM ..... 6**

**6 FINANCIAL PROPOSAL & EVALUATION ..... 7**

6.1 FINANCIAL PROPOSAL SUBMISSION FORM .....9

6.2 BUSINESS QUESTIONNAIRE.....10

6.3 SWORN STATEMENT (MANDATORY) .....12

**7 TECHNICAL REQUIREMENTS..... 13**

## **1 CORPORATE OVERVIEW**

Madison Group Limited (the company) is a locally owned financial services holding company offering Life Assurance, General Insurance, and Investment Management Services through its three main subsidiaries: Madison Life Assurance Kenya Limited, Madison General Insurance Kenya Limited, and Madison Investment Managers Limited. The company has its Head Office at Madison House, Upper Hill Close, Nairobi, with 24 branches across the country.

## **2 INVITATION TO TENDER**

Madison Group Limited invites qualified and experienced firms to submit proposals for the provision, implementation, configuration, training and support of a Security Information and Event Management System (SIEM).

The proposed solution is expected to provide centralized security monitoring, real-time visibility across Madison Group's IT environment, proactive threat detection, incident response support, regulatory compliance monitoring, risk management reporting and operational efficiency.

The need for the SIEM solution is driven by the increasing frequency and sophistication of cyber threats, regulatory obligations and the need to strengthen Madison Group's overall information security posture. The solution should enable the organization to detect, analyze, respond to and report security events from various systems, applications, network devices, endpoints and other critical IT infrastructure.

## **3 TENDERING INSTRUCTIONS**

### **3.1 Submission of Tender Documents**

Completed tender documents indicating the name of the tender and the tender reference number without identifying the bidder's name by sending an email to the Procurement Office, [procurement@madison.co.ke](mailto:procurement@madison.co.ke), not later than **Friday, 17<sup>th</sup> July 2026**.

Submission of bids shall be in two sealed envelopes clearly marked:

**MGL/SIEM/01/2026 –Technical Original**  
**MGL/ SIEM /01/2026 – Financial Original**

The bids should be addressed to:

**The Group Procurement**  
**Madison Group Limited,**  
**Madison House, Upper Hill Close**  
**P.O Box 41163-00100,**  
**NAIROBI, KENYA.**

**Tel No: +254 20 2864000, +254 70 9922000**

### **3.2 Clarifications**

Prospective bidders can request clarifications by sending an email to the Procurement Office, [procurement@madison.co.ke](mailto:procurement@madison.co.ke). The Procurement office will respond in writing to requests for clarification received not later than five (5) days before the deadline for the submission of tenders.

All correspondence related to the contract/proposal shall be made in English.

### 3.3 Additional Information

The Company reserves the right to request additional information from prospective bidders.

### 3.4 Withdrawal of Tender

The Company may at any time terminate this procurement process before the award of the contract and shall not be liable to any person for the termination.

### 3.5 Tender Currencies

Prices shall be quoted in KES / USD.

## 4 TECHNICAL PROPOSAL & EVALUATION

Bidders must provide adequate documentation to support the information required under the technical evaluation criteria. Incomplete tender submissions shall not be considered, and all documents forming part of the proposal must be completed in English.

The information submitted will be used by the Company, at its sole discretion, to assess the suitability and qualification of prospective bidders.

Bidders shall only be considered qualified where the Company is satisfied that they are duly authorized and possess the required capability, experience, qualified personnel, financial capacity and resources necessary to satisfactorily execute the project.

Points awarded for the evaluation of Full Technical Proposals are as follows:

Ref	Evaluation Criteria	Points
	<p><b>Mandatory Documents (10 Marks)</b></p> <p>Bidders are required to submit the following mandatory documents as part of their tender proposal. Failure to submit any of the required documents may render the tender application non-responsive and may lead to disqualification.</p> <ul style="list-style-type: none"><li>i. Certificate of Registration/Incorporation.</li><li>ii. Valid and certified copy of Business permit/ relevant business licences</li><li>iii. Current CR12 issued by the Registrar of Companies (Not older than 6 months)</li><li>iv. Tax compliance certificate</li><li>v. VAT &amp; PIN Certificates</li><li>vi. Filled Confidential Business Questionnaire Form</li><li>vii. Duly filled, signed &amp; stamped Sworn Statement</li><li>viii. Current Partner Certification</li><li>ix. Technical Submission Form</li><li>x. Financial Submission Form</li></ul>	<b>10</b>

	<p><b>Firm Experience</b></p> <p>i. Bidders are required to provide documentary evidence demonstrating a minimum of five (5) years’ experience in successfully undertaking similar assignments in large and complex organizations, preferably within the Banking, Financial Services and Insurance (BFSI) sector.</p> <p>The evidence may include reference letters, completion certificates, contracts, purchase orders, or any other relevant documentation confirming the bidder’s experience and capability.</p> <p>ii. Bidders must also clearly demonstrate their competence, willingness, technical capacity, resource availability and ability to deliver the required services within reasonable and agreed timelines. The Company shall assess the bidder’s experience, past performance, sector relevance and overall capacity to execute the project successfully.</p>	<p><b>5</b></p>
	<p><b>Key Personnel</b></p> <p>i. Provide current <b>CVs of 2 key staff members</b> who will be engaged in the assignment, highlighting their role in the Company, number of years of experience, and number of years with the company (4 marks)</p> <p>ii. Provide copies of relevant academic/professional certifications of the 2 key staff members above. (4 marks)</p>	<p><b>4</b></p> <p><b>4</b></p>
	<p><b>Past/present Clients</b></p> <p>Bidders shall provide documentary evidence demonstrating a minimum of five (5) years’ experience in undertaking similar assignments in large and complex organizations, preferably within the Banking, Financial Services and Insurance (BFSI) sector or other comparable corporate environments.</p> <p>Bidders shall further submit proof of successful engagement in similar projects undertaken within the last two (2) years. This should include at least four (4) client testimonials, reference letters, completion certificates, contracts, LSOs/LPOs, or other relevant documents indicating the client name, nature of assignment, project value, period of engagement and contact details for reference purposes.</p> <p>Each valid and verifiable reference shall be awarded two (2) marks.</p>	<p><b>8</b></p>
	<p><b>Financial Capability</b></p> <p>Bidders shall provide evidence of financial capacity to successfully execute the project. This shall include audited financial statements for the last two (2) completed financial years. Where the 2025 audited financial statements are not yet available, bidders may</p>	<p><b>9</b></p>

	submit the 2023 and 2024 audited financial statements together with the 2025 management accounts. The Company shall assess the bidder’s financial stability, working capital position, profitability and overall ability to meet project obligations without risk of interruption.	
	<b>Technical Requirements</b> Supply, implementation and support of SIEM solution. (Referred on Pages 13-16.)	<b>50</b>
	<b>Project Management Approach</b> (10 marks) i. Provide a detailed methodology regarding the requirements ii. Provide a detailed work plan indicating the timelines for the engagement.	<b>5</b> <b>5</b>
	<b>TOTAL TECHNICAL SCORE</b>	<b>70</b>
	<b>FINANCIAL PROPOSAL</b>	<b>30</b>

The minimum technical Score required to pass and qualify for the Financial Proposal Evaluation is **70 Points**. The financial Proposal for bidders whose technical score is less than 70 points will be rejected.

**5 TECHNICAL PROPOSAL SUBMISSION FORM**

[\_\_\_\_\_ Date \_\_\_\_\_]

To: \_\_\_\_\_ [Name and address of Client]

Ladies/Gentlemen:

We, the undersigned, offer to provide **Security Information and Event Management Solution**

\_\_\_\_\_ in accordance

with your Request for Proposal dated \_\_\_\_\_ [Date]

and our Proposal. We are hereby submitting our Proposal, which includes this Technical Proposal, [and a Financial Proposal].

We understand you are not bound to accept any Proposal that you receive.

We remain,

Yours sincerely,

\_\_\_\_\_ [Authorized Signature]:

\_\_\_\_\_ [Name and Title of Signatory]

\_\_\_\_\_ [Name of Firm]

\_\_\_\_\_ [Address]

## 6 FINANCIAL PROPOSAL & EVALUATION

**Financial Proposal Evaluation** (Weightage 30%): The Evaluation Committee will determine whether the Financial Proposals are complete, i.e., whether the tenderer has included all components as per the tender document. If not, the Committee may reject the bid as non-responsive. Financial bids shall be compared for the complete scope of work as per the Price Proposal Schedule, inclusive of all taxes and duties.

### Overall Ranking:

The combined result of the technical and financial proposals will determine the final, overall ranking. The method for obtaining the overall ranking will be as follows:

$$F = (C \text{ low} / C) \times 30$$

$$\text{Combined Final Marks (CF)} = F + T$$

Where **C low** = Lowest Price Proposal

**C** = Price of current bid in question

**F** = Financial Proposal

**T** = Technical Score of the specific Proposal in question

### Summary of Costs:

Costs	Amount
Provision of Request For Proposals For Provision, Implementation and Support of a Security Information and Event Management System for Madison Group Limited as per the terms of reference.	
Taxes	

<b>Total Cost KES</b>	
-----------------------	--

**6.1 FINANCIAL PROPOSAL SUBMISSION FORM**

\_\_\_\_\_ [Date]

To: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

[Name and address of Client]

Ladies/Gentlemen:

We, the undersigned, offer to provide a **Security Information and Event Management Solution** for ( \_\_\_\_\_ ) in accordance with your Request for Proposal dated ( \_\_\_\_\_ ) [Date] and our Proposal.

Our attached Financial Proposal is for the sum of

( \_\_\_\_\_

\_\_\_\_\_ ) [Amount in words and figures] inclusive of the taxes.

We remain,

Yours sincerely,

\_\_\_\_\_ [Authorized Signature]

\_\_\_\_\_ [Name and Title of Signatory]

\_\_\_\_\_ [Name of Firm]

\_\_\_\_\_ [Address]

## 6.2 BUSINESS QUESTIONNAIRE

### A. COMPANY INFORMATION

Company Name:

\_\_\_\_\_ *As per the certificate of incorporation*

Trading Name:

\_\_\_\_\_ *If different from the company name*

Date of incorporation:

\_\_\_\_\_

Nature of Business:

\_\_\_\_\_

Physical Location:

\_\_\_\_\_

House: \_\_\_\_\_ Street/Road:

\_\_\_\_\_

Postal Address: \_\_\_\_\_ Post Code:

\_\_\_\_\_

City/Town:

\_\_\_\_\_

KRA PIN: \_\_\_\_\_ Tax Compliance Status:

\_\_\_\_\_

No. of Staff: \_\_\_\_\_ Permanent: \_\_\_\_\_ Casual/Temporary:

\_\_\_\_\_

Key Partnerships /Certifications

(i)

\_\_\_\_\_

(ii)

\_\_\_\_\_

(iii)

---

**B. PAST/PRESENT CLIENTS**

1. Name of Client: \_\_\_\_\_

Sector: \_\_\_\_\_

Address: \_\_\_\_\_ Telephone: \_\_\_\_\_

Name of Contact: \_\_\_\_\_ Position: \_\_\_\_\_

Email address of contact: \_\_\_\_\_ Value of Contract \_\_\_\_\_

Completed/Ongoing? \_\_\_\_\_ Duration of engagement \_\_\_\_\_

Key Successes:

---

---

---

---

---

---

---

---

---

---

*(Attach proof of engagement with client testimonials/references)*

2. Name of Client: \_\_\_\_\_

Sector: \_\_\_\_\_

Address: \_\_\_\_\_ Telephone: \_\_\_\_\_

Name of Contact: \_\_\_\_\_ Position: \_\_\_\_\_

Email address of contact: \_\_\_\_\_ Value of Contract \_\_\_\_\_

Completed/Ongoing? \_\_\_\_\_ Duration of engagement \_\_\_\_\_

Key Successes:

---

---

---

---

---

*(Attach proof of engagement with a client, testimonials/references)*

3. Name of Client: \_\_\_\_\_

Sector: \_\_\_\_\_

Address: \_\_\_\_\_ Telephone: \_\_\_\_\_

Name of Contact: \_\_\_\_\_ Position: \_\_\_\_\_

Email address of contact: \_\_\_\_\_ Value of Contract \_\_\_\_\_

Completed/Ongoing? \_\_\_\_\_ Duration of engagement \_\_\_\_\_

Key Successes:

---

---

---

---

---

*(Attach proof of engagement with client testimonials/references)*

4. Name of Client: \_\_\_\_\_

Sector: \_\_\_\_\_

Address: \_\_\_\_\_ Telephone: \_\_\_\_\_

Name of Contact: \_\_\_\_\_ Position: \_\_\_\_\_

Email address of contact: \_\_\_\_\_ Value of Contract \_\_\_\_\_

Completed/Ongoing? \_\_\_\_\_ Duration of engagement \_\_\_\_\_

Key Successes:

---

---

---

---

---

---

---

*(Attach proof of engagement with a client, testimonials/references)*

### **6.3 SWORN STATEMENT (MANDATORY)**

Having studied the information in the document for the above project we/I hereby state:

- a. The information furnished in our application is accurate to the best of our knowledge.
- b. That I/We understand that I/We shall be disqualified should the information submitted here for the purpose of seeking qualification be materially inaccurate or materially incomplete.
- c. We enclose all the required documents and information required for the RFP evaluations.

**Company Name** .....

**Represented by** .....

**Date** .....

**Signature** .....

**(Full name and designation of the person signing and stamp or seal)**

**7 TECHNICAL REQUIREMENTS**

No	REQUIREMENT	VENDOR RESPONSE	
		COMPLIANCE (YES/NO)	EXPLANATION
	<b>GENERAL REQUIREMENTS</b>		
1	Must be available as Virtual Machines for on-premises and public/private cloud deployments on the following hypervisors - VMware ESX, Microsoft Hyper-V, KVM, Amazon Web Services AMI, OpenStack, Azure (only Collector)		
2	Must scale data collection by deploying multiple Collectors free of cost		
3	The SIEM MUST be able to collect logs in near real-time and start processing as soon as possible		
<b>TECHNICAL REQUIREMENTS</b>			
1	The solution MUST support integration with other security solutions. Patch & Vulnerability Management tools, IPSs, Antivirus, Database Activity Monitoring, etc.		
2	The solution MUST report on devices that are no longer actively sending logs to the SIEM solution.		

3	The system MUST give alert to administrators when vulnerabilities appear on critical systems and prioritize security alerts based upon the value of the asset being attacked and its vulnerabilities.		
4	The SIEM Cluster should not limit how much event data is stored. This limit should only be on how much storage is provided.		
5	The SIEM Cluster must be able to store both the raw event log as well as the parsed event log/normalized data.		
6	Solution should be able to perform Registry Change Monitoring for critical servers identified during the deployment and should provide a mechanism to exempt specific registry keys.		
7	The solution should allow retention of full source data at no cost on allocated SIEM storage.		
8	The solution should support searching into archived logs without having to import them.		
9	Must support an integrated enhanced data visibility with machine learning and User and Entity Behavior Analysis (UEBA). Shouldn't be provided as a separate 3rd party solution to simplify management.		
10	The solution should provide the ability to notify Security Administrators when log events have not been received from a specific system and the ability to generate such reports for a specifiable duration of time.		
11	The solution should have ability to analyze events and then send alerts to notify security staff of immediate issues. These alerts should support additional criteria such as Time of Day, Incident Severity, Affected Items and multiple actions such as email, sms, remedial action, ticket		

	creation, snmp alert, etc.		
12	The Windows and Linux Advanced Agents should support agent process and service protection. It should automatically restart if process killed.		
13	Must support at least 35 network devices and advanced monitoring for at least 70 windows/Linux servers and applications with total expected EPS.		
14	The SIEM tool should provide a graphical investigation view for investigation multiple incidents and entities that are related.		
15	The SIEM tool should have an AI advisor capability where we can integrate it with AI platforms for responses to SOC queries, analysis and recommendations for logs and incidents, and help with building reports. This does not come with the AI platform subscription.		
16	The SIEM platform should support SOAR capabilities with over 700+ connectors supported and solutions packs with out of the box scenarios for incident investigation and responses.		
17	SIEM SOC solution should be proposed with 1-year subscription for the following components only: <ul style="list-style-type: none"> <li>• SOAR Automation Playbooks</li> <li>• Threat Intelligence subscription</li> <li>• 24 x 7 Support</li> </ul>		
18	Must Actively discovering the devices within the network without an agent and using standard protocols such as:SNMP,WMI,TELNET,SSH,OPSEC		
	<b>OTHER REQUIREMENTS (MANAGED SERVICES PROVISION)</b>		
	<b>Note:</b> Managed SOC monitoring services (bidders should propose the financials in-line with managed services separately)		
1	Must deliver continuous monitoring, threat detection, incident analysis and security reporting through		

	dedicated Security Operation Center (SOC)		
2	Must offer regular health checks and performance optimization		
3	Must continuously do Incident triage, investigation and prioritization.		
4	Must deliver monthly security reports, dashboards and executive summaries.		
5	Must help in log source onboarding, integration, use case development and tuning		