MINISTRY OF FOREIGN AFFAIRS AND EXPATRIATES (MOFA)

Integrated Governance, Risk, and Compliance (GRC) Management Platform

2025

Introduction

The Ministry of Foreign Affairs (MOFA) is seeking proposals from qualified vendors for the implementation of a comprehensive, integrated Governance, Risk, and Compliance (GRC) management platform. The aim is to enhance the ministry's ability to manage cybersecurity risks, ensure compliance with national and international standards, and improve policy governance and organizational resilience.

Scope of work

Implementation of an Integrated Governance, Risk, and Compliance (GRC) Management Platform for the Ministry of Foreign Affairs (MOFA), This includes configuration, deployment, training, and ongoing advisory support.

Winning Bidder Activities

The winning bidder should perform the following besides any additional related activities needed for the successful delivering the project objectives and its cost shall be included in the fixed price submitted by the bidder:

1- The successful vendor will be expected to deliver on-premise GRC software Platform with full range of implementation Services.

2- The vendor will support the loading of the MOFA asset register and assist in enriching asset metadata within the platform.

3- Implement gap analysis based on customizable control statements and allow assignment of implementation maturity levels.

4- Provide a platform that include a comprehensive compliance tracking module, with support for mapping against major international frameworks such as ISO 27001, NIST CSF, and CMMI.

5- Implement risk identification and assessment functionality include the ability to map threats and vulnerabilities to asset groups, assign controls, and calculate risk values using dynamic formulas

6- Implement risk treatment and the risk mitigation features must support the full risk response lifecycle: Reduce, Accept, Avoid, and Transfer. The system should allow assigning risk and policy owners, managing evidence and justifications.

7- The vendor shall provide consultant-led advisory support through scheduled meetings, email communication, and real-time troubleshooting session.

8- Training and Knowledge Transfer: Training will be delivered to all relevant MOFA stakeholders, including Admins, Risk Officers, and Compliance Officers.

9- Delivery within 2 Weeks.

10-One Year Support.

11-Provide support and maintenance services on a 24X7

12-The winning bidder shall provide a Quarterly preventive maintenance

13-Provide communication channels to enable MoFA to report incidents that should be tracked and monitored till final resolution by the winning bidder, and keeping MoFA informed about the status for these incidents

14-Issue a service report after each and every site visit registering the reported incident, its root cause and the followed procedures for issue(s) successful resolution including the taken and/or suggested recommendations and measures that shall prevent such incidents / issues from reoccurring in the future.

15-The Bidder accepts to comply with all provisions, whether explicitly stated in this RFP or otherwise, stipulated in the Unified Procurement By-Law No 8 of 2022 and its Instructions, and any other provisions stated in the Standard Contracting sample Arabic Contract Agreement annexed to this RFP including general and special conditions, issued pursuant to said Unified Procurement By-Law w and Tendering Instruction.

16-The winning bidder will be expected to provide a single point of contact to which all issues can be escalated. MOFA will provide a similar point of contact

17-Bidders are responsible for the accuracy of information submitted in their proposals

18-The Winning Bidder, shall not, either during the term or after the expiration of the Contract, disclose any proprietary or confidential information relating to the Project, the Services, the Contract, or MoFA business or operations without the prior written consent of The Ministry of Foreign Affairs and Expatriates.

19-The Winning Bidder shall sign a Non-Disclosure Agreement with Ministry of Foreign Affairs and Expatriates. A confidentiality undertaking is included in Annex 2

Annex A – Compliance Matrix

Requirement Description		Compliance (FC / PC / NC)	Vendor Comments / Reference
Platform must support role-based access control for Admin, Risk Manager, Auditor, etc.			
Ability to define and customize risk scoring formulas and thresholds			
Upload assets in bulk via Excel templates with automated classification logic			
Map compliance controls to ISO 27001, NIST CSF, and CMMI frameworks			
Full mitigation workflow including Reduce, Accept, Avoid, and Transfer			
Real-time dashboards for risk, compliance, and asset reporting			
Arabic and English support across interface and reporting			
Vendor to deploy platform on-premise in a Linux-based environment			
Provide post-deployment training for Admin and Risk users			
Provide technical support via email and scheduled virtual sessions			

Bidder Qualification

1. The bidder must have minimum two engineers have :
   - ISO 27001 Implementer
   - Certified Information Security Manager
2. The bidder must have minimum 1 Active References in Jordan.

Payment Terms:

- 100 % after the delivery of the Project.

Annex1

SERVICE LEVEL REQUIREMENTS

Severity Levels

A problem is a critical or serious loss of functionality. Severity level is a mean of assessing and documenting the impact of the loss of functionality to the winning bidder and the impact to the business. The severity level gives restoration or repair priority to problems causing the greatest impact to the business. Below is a description for the various severity levels defined and used at MOFA:

Severity One (Urgent)

A severity one (1) issue is a catastrophic business impact: complete loss of a core business process which needs immediate attention

Severity Two (High)

A severity two (2) issue is critical business impact: significant loss or degradation of services

Severity Three (Medium)

A severity three (3) issue is a medium-to-low impact problem which involves partial non-critical functionality loss

Response and Resolution Matrix

Table below describes the response and resolution time required for the different problems severities at MOFA:

Severity	Response Time	Resolution Time *	Working time
1	1 Hour	4 Hours	24X 7

2	3 Hours	One working day	During the official working Hours for MoFA
3	4 Hours	Two working days	During the official working Hours for MoFA

Table 1 Response and Resolution Matrix

Where:

*Response Time: The time it takes to acknowledge MOFA 's issue in a non-automated way. It is calculated from the time of sending an email explaining the incident, opening a ticket on bidder ticketing system, or conducting a phone call with the assigned support engineer until the time that MOFA is advised their problem has been received and is being addressed

Resolution Time: Is the time taken to resolve the reported incident, Resolution Time (Restoration Time) is calculated from the end of the defined response time for each severity level as shown in the above table, it shall include the diagnostic and the fixing time for the reported incident.

ESCALATION PROCEDURES AND PENALTIES

The winning bidder is required to provide the support and maintenance services according to the Response and Resolution Matrix shown in table 1 above.
Penalty will be deducted according to table 2 below:

- If the winning bidder passed the Response Time: first level of escalation will be applied by notifying bidder's Technical Support Manager, and assigned contact person.

1.

- If the winning bidder passed the Resolution Time: MOFA is entitled to fix the problem and to apply penalty on the winning bidder in accordance with the following criteria in table 2 below and all costs incurred by MOFA for fixing the problem shall be charged to the winning bidder and deducted from his dues or the performance bond.

Severity	Definition	Support Penalty
1	Must be done, essential to business survival. Business can't continue	A penalty of 10 J.D. shall be applied for each hour pass the resolution time. This penalty shall continue for the first 24 hours (10x24). If delay continues, then a penalty of 240 J.D. per day shall be applied and for the maximum duration of 3 days; after that, 3rd party will be called to fix the problem.
2	Should be done, near essential to business survival.	A penalty of 50 J.D. shall be applied for each day pass the resolution time. This penalty will be applied for the maximum duration of 4 days; after that, 3rd party will be called to fix the problem.
3	Could be done, high benefit to business if time	A penalty of 25 J.D. shall be applied for each day pass the resolution time.

	and resources are available.	This penalty will be applied for the maximum duration of 5 days; after that, 3rd party will be called to fix the problem.

Annex 2

سرية المعلومات:

يلتزم الفريق الثاني بحفظ سرية المعلومات التي قد تعطى له من قبل الوزارة وذلك لتمكينه من القيام بواجباته في هذا المشروع، أو التي قد تصل إليه بأي طريقة كانت سواء في المراحل التحضيرية للعمل أو أثناء العمل أو بعد الانتهاء منه كما المناقص بعدم إفشاء هذه المعلومات إلى أي طرف ثالث.

ويبقى التزام المناقص بحفظ سرية المعلومات وعدم إفشاءها إلى أي طرف ثالث مستمرا حتى بعد الانتهاء من العمل على المشروع. كما يلتزم المناقص بعدم إفشاء هذه المعلومات إلى الإداريين والموظفين العاملين لديه إلا من يعمل منهم بصورة مباشرة على الأعمال الواردة في المشروع.

المعلومات ذات الطابع السري تشمل على سبيل المثال لا الحصر جميع المعلومات سواء كانت مكتوبة أو غير مكتوبة، والتي قد تصل إلى المناقص شفاها أو كتابة أو بأي طريقة أخرى، وتتعلق بوزارة الخارجية وشؤون المغتربين، كالمعلومات المتعلقة بالمواصفات والمقاييس للحواسب المستخدمة، وأماكن وجودها، والتصاميم والرسومات لشبكة الحواسب، والإحصائيات المتعلقة بالمواقع الالكترونية أو غيرها، وأي معلومات مخزنة في الحواسب، أو وسائط التخزين الالكترونية وغير الالكترونية الأخرى، والوثائق المتعلقة بالبرمجيات الحاسوبية المستخدمة أو الشبكة الحاسوبية المستخدمة، والوثائق المتعلقة بالأعمال الإدارية وشؤون الدولة، وأي وثائق أخرى، والملخصات والتقارير والدراسات والبيانات والسجلات الالكترونية وغير الالكترونية مهما كان موضوعها، وأي خطط حالية أو مستقبلية، وأي معلومة سواء تم التأشير عليها بأنها ذات طابع سري أو خاص أو لم يتم التأشير.

لا تعد المعلومات ذات طابع سري إذا أصبحت هذه المعلومات جزء من المعلومات المتاحة للعامة عن غير طريق الإخلال بالالتزام الوارد في هذا البند.