



**Extension to Request for Proposal (RFP)  
for IT Managed Service  
[www.globalrightscompliance.com](http://www.globalrightscompliance.com)**

Stichting "Global Rights Compliance Foundation", Prinses Margrietplantsoen 33, 2595 AM Gravenhage Nederland  
Kvk number 70 048436, RSIN number 85811884.

**To** : Offerors  
**From** : Global Rights Compliance Foundation ([www.globalrightscompliance.com](http://www.globalrightscompliance.com))  
**Subject** : *Request for Proposal (RFP) No: P26-015 IT Managed Service*

**RFP Issue Date** : 16.03.2026  
**RFP Closing Date** : 26.03.2026  
**RFP Extended Closing Date** : 30.03.2026  
**RFP Closing Time** : 17:00 CET Time

**The successful firm will be notified via e-mail.**

Enclosed is a Request for Proposal (RFP) for a IT Managed Service. Global Rights Compliance Foundation invites qualified firms and organisations to submit a best-price proposal for the mentioned service. The issuance of a subcontract is subject to availability of funds, successful negotiation of the subcontract budget and terms, and receiving client consent, if required. The Contract resulting from this award will be a single firm fixed price purchase order.

### **General Background**

Global Rights Compliance is an international human rights legal practice based in the UK and the Netherlands, specialising in international human rights, criminal, and humanitarian law. We have a dedicated Business and Human Rights Unit focused on providing advice to businesses, public sector institutions, civil society organisations, and investors on both the legal and practical aspects of human rights due diligence, responsible business conduct, as well as heightened human rights due diligence in conflict-affected and high-risk areas.

### **Purpose and Objective of the Service**

Global Rights Compliance currently operates a multi-project environment that relies heavily on secure and reliable IT infrastructure to support operational delivery, communication, and data protection. As the organization continues to grow in operational complexity and technology dependency, maintaining strong IT governance and security practices has become increasingly critical.

A recent internal technical review highlighted several areas where strengthening IT operational management would significantly improve the organization's security posture, operational resilience, and compliance with internationally recognized security standards, including alignment with Cyber Essentials baseline controls. The review indicated that while specialist cybersecurity tools and services are valuable, foundational IT management practices—such as consistent patch management, endpoint configuration control, access management, and asset inventory—are essential to maintaining a strong security posture and meeting compliance expectations.

Several operational risks were identified that may require structured and scalable IT management support, including:

- Inconsistent device patching and update management
- Limited centralized endpoint configuration management
- Growing vulnerability exposure as vulnerability scanning capabilities expand
- Limited internal capacity to remediate identified vulnerabilities at scale
- Lack of standardized privileged access management practices
- Potential gaps in asset inventory and device lifecycle management
- Increasing operational demand on the internal IT function

In addition, as the organization continues the rollout of vulnerability management capabilities through tools such as Qualys, it is expected that a greater number of vulnerabilities will be identified across endpoints and systems. Without a structured remediation and patch management process, there is a risk that vulnerabilities may accumulate faster than they can be addressed.

To strengthen IT operational management, enhance endpoint security controls, and support compliance with security standards, Global Rights Compliance is seeking to engage a qualified Managed Service Provider to deliver comprehensive IT managed services.

The Managed Service Provider will work alongside the internal IT function to improve operational efficiency, strengthen endpoint management practices, and support the implementation and enforcement of security baselines aligned with Cyber Essentials requirements.

## **Objectives**

The objective of this assignment is to engage a Managed Service Provider capable of delivering structured, scalable, and proactive IT management services to support the organization's operational needs and improve its security and compliance posture.

Specific objectives include:

- Strengthening endpoint configuration and device management practices
- Implementing structured and consistent patch management processes
- Supporting vulnerability remediation and risk reduction
- Enhancing asset visibility and lifecycle management
- Enforcing appropriate privileged access and account separation controls
- Improving responsiveness and efficiency of IT support services
- Supporting alignment with Cyber Essentials security requirements

## **Scope of the Service**

The selected service provider will be expected to deliver a range of IT managed services designed to support the organization's IT infrastructure, users, and security practices.

The scope of services may include, but is not limited to, the following areas:

### **a) Endpoint and Device Management**

The service provider shall provide centralized management of organizational devices to ensure consistent configuration and security baseline enforcement.

This includes:

- Endpoint configuration management
- Standard device baseline implementation
- Monitoring device health and performance
- Endpoint security policy enforcement
- Support for both office-based and remote devices

### **b) Patch and Update Management**

The service provider shall establish and maintain structured processes for operating system and application patch management.

This includes:

- Monitoring available security updates
- Deploying operating system patches in a timely manner
- Managing updates for third-party applications
- Ensuring compliance with defined patching timelines for security vulnerabilities
- Reporting patch status and compliance levels
- Vulnerability Management Support
- The service provider shall support the organization's vulnerability management processes, including integration with existing vulnerability scanning platforms such as Qualys.
- Responsibilities may include:
  - Reviewing vulnerability scan results
  - Supporting prioritization of remediation activities
  - Implementing vulnerability remediation actions
  - Monitoring vulnerability remediation progress
  - Providing reporting on vulnerability status and risk exposure

#### **c) Privileged Access and Account Management**

The service provider shall support implementation of best practices relating to user access management and administrative privilege controls.

This may include:

- Implementing separation between administrative and standard user accounts
- Supporting least-privilege access principles
- Monitoring privileged account usage
- Supporting secure credential and access management practices

#### **d) IT Asset Management**

The service provider shall support the establishment and maintenance of an accurate and comprehensive IT asset inventory.

This includes:

- Tracking organizational devices and systems
- Maintaining asset lifecycle information
- Supporting onboarding and decommissioning of devices
- Maintaining configuration records for managed endpoints
- 3.6 Helpdesk and User Support Services
- The service provider shall provide responsive IT support services to organizational staff.
- Services may include:
  - IT helpdesk support
  - Incident response and troubleshooting
  - Remote support for users
  - Issue resolution tracking and reporting

#### **e) Compliance and Security Baseline Support**

The service provider shall support the organization in maintaining security practices aligned with Cyber Essentials control requirements and other relevant organizational policies.

This may include:

- Supporting implementation of secure configuration baselines
- Assisting with compliance monitoring
- Providing recommendations for security improvements
- Supporting audit readiness where applicable

## Expected Outcomes

Through the engagement of a Managed Service Provider, the organization expects to achieve:

- Improved endpoint configuration and security management
- Reduced vulnerability exposure through structured patch management
- Improved visibility of IT assets and device lifecycle management
- Stronger enforcement of security controls and access management
- Faster resolution of IT issues impacting staff productivity
- Strengthened alignment with Cyber Essentials security requirements
- Enhanced operational resilience and IT governance

To be considered, Offerors should submit a complete proposal no later than the closing date and time indicated above. Offerors should ensure that the proposals are well written in English, easy to read, follow the instructions provided and contain only requested information.

Any questions should be submitted **in writing** and emailed to [aydineksi@globalrightscompliance.co.uk](mailto:aydineksi@globalrightscompliance.co.uk) , [procurement@grcompliance.org](mailto:procurement@grcompliance.org) no later than **8 days** from the issue date of this RFP. The solicitation number should be stated in the subject line.

Proposals must be divided into two parts: Technical Proposal and Cost/Business proposal. The email subject line should be **RFP for IT Manage Service** and sent to [aydineksi@globalrightscompliance.co.uk](mailto:aydineksi@globalrightscompliance.co.uk) , [procurement@grcompliance.org](mailto:procurement@grcompliance.org)

Please treat the information contained within this RFP with professional confidentiality. The successful company will be asked to sign a Non-Disclosure Agreement or Confidentiality Agreement prior to commencing with the work.

Sincerely,  
*GRC Procurement Department*

## Attachments:

- Attachment I :Instructions to Offerors
- Attachment II :Evaluation Criteria
- Attachment III :Cover Letter

**Attachment I**  
**INSTRUCTIONS TO OFFERORS**

**A. General Instructions**

These Instructions to Offerors will not form part of the offer or of the Contract. They are intended solely to aid Offerors in the preparation of their proposals. Please read and follow these instructions carefully.

1. The proposal and all corresponding documents related to the proposal must be written in the English language, unless otherwise explicitly allowed. Additionally, all proposals should be single-spaced with clear section headings, and be presented in the order specified in Attachment III – Evaluation Criteria.
2. Proposals must include only the Offeror's own work. No text should be copied from sources outside of your organization unless those sources are adequately cited and credited. **If GRC determines that any part of the proposal is plagiarized from outside sources, the Offeror will be automatically disqualified.**
3. Proposals and all cost and price figures must be presented in **Euros**. All prices should be gross of tax, but net of any customs duties. A firm fixed price purchase order will be issued to the successful offeror in EUR.
4. The Offeror must state in their Proposal the validity period of their offer. The minimum offer acceptance period for this RFP is **90 days** after the closing date of the RFP. If an Offeror has provided a validity period of less than 90 days, they will be asked to revise this. If the Offeror does not extend the validity period, their proposal will be rejected.
5. The Technical Proposal and Cost/Business Proposal **must** be kept separate from each other. Technical Proposals must not refer to cost or pricing information **at any point**. This will allow the technical evaluation to be made strictly based on technical merit.
6. Offerors must be licensed entities, as evidenced by submission of a copy of a valid Business License or other official registration. The copy of the license must clearly show a license number, authentication stamp and a date of issue and date of expiry.
7. No costs incurred by the Offerors in preparing and submitting the proposal are reimbursable by GRC. All such costs will be at the Offeror's expense.
8. Responsibility Determination: Award shall only be made to "responsive" companies. To enable GRC to make this decision, the Offeror must provide a cover letter, as provided in Attachment IV.
9. Late Offers: Offerors are wholly responsible for ensuring that their Offers are received in accordance with the instructions stated herein. A late Offer will be recommended for rejection, even if it was late because of circumstances beyond the Offeror's control. Late offers will only be considered at the procurement department's discretion.
10. Modification/Withdrawal of Offers: Offerors have the right to withdraw, modify or correct their offer after it has been delivered to GRC at the email address stated above, and provided that the request is made before the RFP closing date.
11. Disposition of Proposals: Proposals submitted in response to this RFP will not be returned. Reasonable effort will be made to ensure confidentiality of proposals received by all Offerors. This RFP does not seek information of a highly proprietary nature, but if such information is included in the Offeror's proposal, the Offeror must alert GRC and must annotate the material by marking it "Confidential and Proprietary" so that these sections can be treated appropriately.
12. Clarifications and Amendments to the RFP: Any questions regarding this solicitation must be **emailed** to [avdineksi@globalrightscompliance.co.uk](mailto:avdineksi@globalrightscompliance.co.uk) , [procurement@grcompliance.org](mailto:procurement@grcompliance.org) . No questions/clarifications will be entertained if they are received by another means. The solicitation number should be stated in the subject. Responses will be emailed to the requesting potential Offeror and will be sent to all organizations that are participating in this RFP.
13. GRC anticipates that discussions with Offerors will be conducted; however, GRC reserves the right to make an award without discussions. It is strongly recommended that Offerors present their best offer.

**Failure to agree and comply with any of the above specifications will result in the Offeror being considered unresponsive and the proposal may be rejected.**

**B. Submission of Proposal:**

Proposals must be submitted in **two separate sections:**

1. Technical Proposal
2. Cost/Business proposal.

Proposals must be delivered no later than the specified date/time to the email address below.

**Offerors who do not submit their technical and cost proposals separately will be automatically disqualified.**

**C. Content of Proposal:**

The proposal shall be comprised of four sections:

- i. The Cover Letter (Attachment III)
- ii. Copy of the Offeror's Valid Business license
- iii. The Technical Proposal
- iv. The Cost/Business Proposal

1) The Cover Letter: should be on the Offeror's letterhead and **MUST** contain the information requested in Attachment III.

2) Business License

3) Technical Proposal:

- a. Should **clearly & precisely** address theoretical and practical aspects that the Offeror has considered and will employ to carry out the statement of work.
- b. The Technical Proposal is the opportunity for the Offeror to demonstrate that the firm is "technically capable" of implementing the activity and should demonstrate the Offeror's understanding of and capabilities to carry out the work, and address the key issues described in the Evaluation Criteria in Attachment III.
- c. The Technical Proposal should be divided into clearly separate sections following the same order of the Evaluation Criteria in Attachment III. A mis-ordered proposal that makes information hard to find will result in lower scores.
- d. **If an Offeror submits a proposal that fails to respond to the majority of the information requested in this RFP, as outlined specifically in the statement of work and the evaluation criteria, the Offeror's proposal will be automatically disqualified.**

4) The Cost/Business Proposal: must be in a separate section from the technical proposal and will primarily indicate the cost for performing the work specified in this RFP. At a minimum, the Cost/Business proposal should include the following information:

- a. A detailed budget that provides a breakdown of costs.
- b. Detailed and comprehensive cost notes that provide information on each of the line items in the budget and explain why these items are needed for implementation of the activity.

**Failure to comply with any of the above points will result in the Offeror being considered "unresponsive" and the proposal may be rejected.**

If an Offeror provides insufficient information in their technical and/or cost proposal, GRC reserves the right to request additional information, or to request a revised proposal from the Offeror.

**Attachment II  
EVALUATION CRITERIA**

Basis of Award: The award will be made to the offeror whose offer presents the Best Value: the optimal combination of technical merits and reasonable cost. Proposals will be scored on technical factors first.

**EVALUATION CRITERIA**

**1. Technical Competence – presented in the Technical Proposal (100 points)**

**A. Technical Approach 70 points**

Provide a clear, specific, and succinct technical proposal that covers both the conceptual and practical approaches of how to achieve the objectives of this project. Specifically, please address the following, **in the order specified below**:

Item	Requirement	Points Available
1. Willingness to work	Please state that you are willing to implement the scope of work as detailed in the announcement. A positive statement is required. Offerors that do not provide a positive statement will be automatically disqualified.	Pass/Fail
2. Technical Approach & Understanding	<ul style="list-style-type: none"> <li>Understanding of the scope (multi-project environment, security needs)</li> <li>Clarity and structure of methodology</li> <li>Proactive approach (monitoring, automation, prevention)</li> </ul>	20 points
3. Endpoint & Patch Management	<ul style="list-style-type: none"> <li>Centralized endpoint management capability</li> <li>Patch management process (automation, timelines)</li> <li>Enforcement of security configurations</li> </ul>	15 points
4. Vulnerability & Security Management	<ul style="list-style-type: none"> <li>Approach to vulnerability management (e.g. Qualys or similar tools)</li> <li>Remediation capability</li> <li>Alignment with Cyber Essentials or similar standards</li> </ul>	10 points
5.IT Support & Service Delivery	<ul style="list-style-type: none"> <li>Helpdesk structure and support model</li> <li>SLA / response and resolution times</li> <li>Remote support capability</li> </ul>	10 points
6.Asset & Access Management	<ul style="list-style-type: none"> <li>IT asset tracking and inventory</li> <li>Device lifecycle management</li> <li>Privileged access / least privilege approach</li> </ul>	10 points
7.Team Experience & Capacity	<ul style="list-style-type: none"> <li>Qualifications and certifications</li> <li>Adequacy of staffing and expertise</li> </ul>	5 points
		70 points

If an Offeror submits a proposal that fails to respond to the majority of the information requested in this RFP, as outlined specifically in the statement of work and the evaluation criteria, the Offeror’s proposal will be automatically disqualified.

**B. Past Performance and Experience – Please include 3 Examples 30 points.**

1. Activity title
2. Location of work
3. Short description and why it is relevant to this RFP.
4. Performance Information (date, duration and if completed on schedule)

**C. Attachments Not Scored**

You may include recommendation/appreciation letters and certificates as attachments, or any other documentation you wish to further support your proposal, stapled/bound separately from the rest of the technical proposal. Content presented here will not be scored.

4. **Cost Reasonableness and Financial Capability** – presented in the Cost/Business Proposal.

**Not Scored**

- a) Please submit a detailed budget to carry out this work. GRC's review of the Cost Proposal shall determine if the overall costs proposed are realistic for the work to be performed, reflect a correct understanding of the project requirements, and are consistent with the Offeror's Technical Proposal. GRC will also review individual line items and determine if they are allowable, allocable, and reasonable.
- b. Submit reasonably comprehensive budget narrative/ budget notes that provide information on each of the line items in the budget and explain why these items are needed for implementation of the activity.

Offerors that do not provide the above-required items as part of their Cost/Business proposal, that provides a proposal that represents a poor understanding of the work to be performed, or that presents unrealistic, unallowable, unallowable, or unreasonable items and costs, in the reviewer's evaluation, will be considered unresponsive and may be disqualified from further consideration.

**Best value determination for award**

GRC will evaluate proposals on a best value basis. in accordance with its procurement standards. In all solicitations, GRC will consider and conduct an evaluation based on both technical capacity and cost. The relative importance of these two factors will vary depending on the nature of the activity. In rare cases, GRC may also award a firm other than the highest technically rated Offeror or the lowest price Offeror.

**GRC reserves the right to request additional supporting documentation or a revised proposal from an Offeror if insufficient information has been provided in the Offeror's technical and/or cost proposal. If the requested information is not provided, GRC has the right to disqualify the firm from further consideration.**

**ATTACHMENT III**

**FORMAT FOR PROPOSAL COVER LETTER – TO BE PRINTED ON ORGANIZATIONAL LETTERHEAD**

To: GRC Procurement Team  
City, Country  
<Date>

Dear Sir / Madam:

We, the undersigned, offer to undertake the **[Insert RFP No.]**, **[Insert project title]**, in accordance with your Request for Proposal dated **[Insert MM/DD/YYYY]** and our Technical and Cost/Business Proposal submitted herein.

Our organization's details are as follows:

- i. Company's Name
- ii. Company's Address
- iii. Name of Company's authorized representative:
- iv. Telephone #/Cellular Phone #, Email address:
- v. Validity Period of Proposal
- vi. A valid Business License

Our proposal shall be binding upon us, subject to any modifications resulting from negotiation, up to expiration of the validity period of the proposal. We understand you are not bound to accept this or any Proposal you receive.

We also certify that our organization:

- (a) has adequate financial resources including appropriate insurance coverage to perform the work stated herein, or the ability to obtain them without delay.
- (b) is able to comply with the described delivery or performance schedule, taking into consideration all existing commitments and constraints.

- (c) has a satisfactory performance record.
- (d) has a satisfactory record of integrity and business ethics.
- (e) has the necessary technical capacity, equipment and facilities, or the ability to obtain them; and
- (f) is otherwise qualified and eligible to receive an award under applicable laws and regulations.

Sincerely,

Authorized Signature:  
Name and Title of Signatory:  
Date: