ANNEX 1 SPECIFICATION OF REQUIREMENTS

1 Background

ECMWF computing resources are accessed by ECMWF staff, hundreds of third-party users, thousands of identifiable external users, and an ever-growing web user population made up of tens of thousands of members of the public.

The security review of the ECMWF IT infrastructure is a key component of the ECMWF risk management program and one of the recurrent activities performed by ECMWF's internal Information Security team which is responsible for the management of information security and assurance at ECMWF. The review will address the security risks and the impact to confidentiality, integrity and availability of services and data. This provides a good indication on how to prioritise, plan, budget and manage the risks in a structured manner.

ECMWF feels it is important to maintain an up-to-date view on the security posture of the IT infrastructure by engaging an external partner to perform vulnerability assessment, penetration testing and security architecture review activities. The deliverables of these activities will be used to evaluate the level of risk and to define the consequent remediation plan.

2 Objectives of this ITT

The purpose of this ITT is for ECMWF to enter into an agreement with a single provider for delivery of IT Security review Services and consultancy services to ECMWF. The contract term will be for a minimum period of two (2) years with an option of yearly extensions to a further two (2) years.

The objective of the subsequent contract is to assess and review the security posture of the IT infrastructures, including the creation of a remediation plan to resolve the discovered vulnerabilities, and to secure best value for money in the consultancy services to support the remediation plan, and to secure best value for money in the consultancy services for future ECMWF information security activities.

The services expected under the contract will be both in the form specific deliverables for Work Packages 1-4, and optional consultancy services for Work Package 5 that may be commissioned by ECMWF during the contract based on the resources and rates agreed.

Work Packages (WP):

- **WP1 - Vulnerability assessments**
- **WP2 - Penetration tests**
- **WP3 - Security architecture review**
- **WP4 - ISO 27001 GAP Analysis**
- **WP5 - Consultancy services**

Activities such as selection, procurement and deployment of security controls, safeguards, or services as well as configuration change, patch installation or software updates identified and suggested in the remediation plan are outside the scope of this ITT. Successful Tenderer awarded as a result of this ITT, or any entities affiliated with them, shall be ineligible to participate in future potential procurements for provision of supplies or services related to the implementation of the recommendations.

Each of the work packages is detailed in the dedicated sections below. The output of Work Package 1-4 shall be a written report that includes all summarised data, conclusions, and recommendations.

3 Envisaged Timeline for the Implementation

The timeline for executing Work Packages 1-4 activities varies according to the complexity of the target systems, the scope of the assessments, and the availability of resources.

Additional considerations:

Overlap: While these activities are outlined sequentially, there can be some overlap. For example, vulnerability assessment results might inform the penetration testing scope, and findings from both assessments can be used to validate and enhance the security architecture.

ECMWF Involvement: It is essential to regularly engage with EMCWF throughout the process to ensure alignment with business goals, address any emerging concerns, and provide updates on assessment progress.

Remediation Period: It is essential to allocate time for ECMWF to address and remediate the identified vulnerabilities and issues between each phase.

Reporting: Each phase shall conclude with a comprehensive and understandable report, including prioritized recommendations for mitigating identified risks.

4 Specification of Requirements

4.1 General requirements

The supplier shall demonstrate to be in line with the following general requirements applicable to all the work packages presented below.

- **Qualifications and Experience**

Tenderers must have a proven track record and relevant experience in providing information security services, including ISO 27001 Gap Analysis, IT Security Architecture Review, Penetration Testing, and Vulnerability Assessment.

Proof of recent industry certifications and qualifications for the tenderers' key personnel should be provided.

Tenderers must supply recent references from previous clients who have received similar services, allowing ECMWF to verify their track record and performance (in line with Annex 2 Tender submission form).

- **Compliance Requirements**

Tenderers must adhere to all applicable laws, regulations, and industry standards concerning information security services. Compliance with data protection and privacy laws, as well as adherence to ethical hacking guidelines, is mandatory.

- **Insurance**

Tenderers should have appropriate liability insurance coverage to protect against any potential incidents or errors during the engagement.

- **Confidentiality**

A commitment to maintaining the confidentiality and security of all data, information, and findings related to the engagement is required. Tenderers must ensure the protection of all data and information they will deal with during the engagement, including compliance with data protection and handling requirements.

- **Methodology and Approach**

Detailed descriptions of the proposed methodologies and approaches for each service should be provided as a part of the tender response. These should be aligned with industry best practices and follow appropriate industry wide, highly recognized methodologies and standards:

  - Support various types of assessment approach such as White Box, Black Box or Grey Box testing as well as position the tests externally, internally, or both.
  - Confirm and obtain ECMWF's approval on Scope of Services (Initial scope is provided in section 5 - Scope of Services) including a test plan in writing prior to service commencement.
  - Engage ECMWF prior to actual test to confirm logistics and time arrangement, understand goals and objective ECWMF would like to achieve during the activities.
  - Discuss and confirm with ECMWF on its risk tolerance and culture to ensure ECMWF approves the test approach.
  - Stipulate any specific limitations, constraints, liabilities, and mutual indemnification.
  - Establish a communication plan so that various stakeholders at the ECMWF's organization will know about any tests.
  - Clean up properly after services completion ensuring environments are not impacted by the activities.
- **Reporting and Documentation**

Tenderers must provide clear, comprehensive, and timely reports for each service. Reports should include findings, recommendations, and a roadmap for improvements.

- **Project Timeline**

Tenderers must commit to the agreed-upon project start and end dates for each service.

- **Escalation Procedures**

Establish an incident and escalation management process to handle issues that may happen during the test. Clear procedures for resolving disputes, issues, or unexpected incidents during the engagement should be outlined.

4.2 Work Package 1 – Vulnerability assessments

The objective of this engagement is to identify and assess potential vulnerabilities in ECMWF IT systems, applications, and networks.

The Vulnerability Assessment project will include the following activities:

- **Preparation and Scoping:**
  - Collaborate with ECMWF to refine the initial scope (see Section 5), objectives, and targets for the vulnerability assessment engagement.
- **Information Gathering:**
  - Collect information about the systems, applications, and networks to be assessed, such as IP addresses, URLs, and system architecture.
- **Vulnerability Scanning:**
  - Conduct automated vulnerability scanning to identify potential weaknesses and security flaws.
- **Manual Assessment:**
  - Perform manual assessment and validation of identified vulnerabilities to eliminate false positives.

- **Risk Analysis:**
    - Assess the severity and potential impact of vulnerabilities and prioritize them based on risk.
- **Recommendations:**
    - Provide recommendations for mitigating identified vulnerabilities and improving overall security posture.

Deliverables:

The following deliverables are expected from the selected tenderer:

- **Vulnerability Assessment Report:**
    - A comprehensive report detailing the findings, including vulnerabilities, their severity, and potential impact.
- **Recommendations Report:**
    - A document outlining recommended actions to mitigate identified vulnerabilities and enhance security.
- **Executive Summary:**
    - A high-level summary of the findings and key recommendations for management.
- **Presentation:**
    - A presentation to the ECMWF management team summarizing the findings and recommendations.

4.3 Work Package 2 – Penetration testing services

The objective of this engagement is to evaluate the security of ECMWF IT systems, applications, and networks through penetration testing. The Penetration Testing work package will include the following activities:

- **Preparation and Scoping:**
    - Collaborate with ECMWF to refine the initial scope (see Section 5), objectives, and targets for the penetration testing engagement.
- **Information Gathering:**
    - Collect information about the systems and applications to be tested, such as IP addresses, URLs, and system architecture.
- **Vulnerability Assessment:**
    - Conduct vulnerability scanning and assessment to identify potential weaknesses and security flaws.
- **Penetration Testing:**
    - Perform controlled and ethical penetration testing, simulating real-world attacks to exploit vulnerabilities.
- **Exploitation and Reporting:**
    - Document and report on successful exploits, including the potential impact of each vulnerability.
- **Recommendations:**
    - Provide recommendations for mitigating identified vulnerabilities and improving overall security posture.

Deliverables:

The following deliverables are expected from the selected tenderer:

- **Penetration Testing Report:**
    - A comprehensive report detailing the findings, including vulnerabilities, exploitation details, and the potential impact on ECMWF.
- **Recommendations Report:**
    - A document outlining recommended actions to mitigate identified vulnerabilities and improve security.
- **Executive Summary:**
    - A high-level summary of the findings and key recommendations for management.
- **Presentation:**
    - A presentation to the ECMWF management team summarizing the findings and recommendations.

4.4 Work Package 3 – Security architecture review

The purpose of this engagement is to assess and provide recommendations to enhance the security architecture of ECMWF IT systems, ensuring they align with industry best practices and meet ECMWF's security objectives.

The IT Security Architecture Review project will include the following activities:

- **Preparation and Planning:**
    - The selected tenderer will work closely with ECMWF team to understand ECMWF current IT infrastructure, security policies, and business requirements.
- **Documentation and Asset Review:**
    - Evaluate existing documentation, architecture diagrams, asset inventory, and security controls relevant to ECMWF IT systems.
- **Technical Assessment:**
    - Perform a technical assessment of the security architecture, including network infrastructure, access controls, encryption methods, and security configurations.
- **Threat and Vulnerability Analysis:**
    - Identify potential threats and vulnerabilities in the security architecture, including those related to hardware, software, and personnel.
- **Gap Analysis:**
    - Conduct a gap analysis to identify weaknesses and areas of improvement in the current security architecture.
- **Recommendations:**
    - Provide comprehensive recommendations for enhancing the IT security architecture, including suggested improvements, priorities, and implementation strategies.

Deliverables:

- **IT Security Architecture Review Report:**
    - A detailed report summarizing the findings, including identified weaknesses and potential risks in the current architecture.
- **Gap Analysis Report:**

    - A report outlining gaps in the current security architecture.
- **Recommendations Report:**
    - A document outlining recommended improvements, priorities, and strategies for enhancing the IT security architecture.
- **Presentation:**
    - A presentation to the ECMWF management team summarizing the findings and recommendations.

4.5 Work Package 4 - ISO27001 Gap Analysis

ECMWF is seeking qualified and experienced tenderers to provide a comprehensive ISO 27001 Gap Analysis. The objective of this engagement is to assess the current state of ECMWF information security management system (ISMS) and identify gaps and weaknesses against the ISO 27001 ISMS standard. The organization is not currently ISO27001 certified. The scope of the gap analysis will be the whole organization. Further information about ECMWF can be found at https://www.ecmwf.int/en/about

The ISO 27001 Gap Analysis work package will include the following activities:

- **Preparation and Planning:**
    - The selected tender will work with ECMWF to understand ECMWF's structure, policies, processes, and procedures related to information security.
- **Documentation Review:**
    - The tender will review existing information security documentation, including policies, procedures, risk assessments, and security controls.
- **On-site and Remote assessment:**
    - Conduct both on-site and remote assessments to evaluate the implementation of information security controls and practices within ECMWF.
- **Gap Identification:**
    - Identify gaps and areas of non-compliance with the ISO 27001 standard and provide detailed assessments of the severity and significance of these gaps.
- **Risk Assessment:**
    - Assess the risks associated with identified gaps and weaknesses in the ISMS.
- **Recommendations:**
    - Provide detailed recommendations and a roadmap for addressing identified gaps and achieving ISO 27001 compliance.

Deliverables:

The following deliverables are expected from the selected tenderer:

- **ISO 27001 Gap Analysis Report:**
    - A comprehensive report outlining the findings, including identified gaps and areas of non-compliance.
- **Risk Assessment Report:**
    - A detailed assessment of the risks associated with the identified gaps.
- **Recommendations Report:**

    - A roadmap for addressing gaps and achieving ISO 27001 compliance, including suggested actions and timelines.
- **Presentation:**
    - A presentation of the findings and recommendations to the ECMWF senior management team.

4.6 Work Package 5 – Consultancy Services

This work package includes optional consultancy services that may be commissioned by ECMWF during the contract based on the resources and rates agreed. The scope of these additional optional services is envisaged to include the following activities:

- Identify and assess potential vulnerabilities within ECMWF IT systems, applications, and networks.
- Conduct controlled and ethical penetration testing to evaluate the security of ECMWF IT systems and applications.
- Assess ECMWF IT security architecture to ensure alignment with best practices and enhance security measures.
- Evaluate ECMWF information security management system for ISO 27001 compliance, identifying gaps and providing recommendations.
- Cybersecurity-related professional services in the following areas:
    - Incident detection and response management
    - Incident response retainer
    - Incident response tabletop exercises
    - Forensic analysis
    - Security awareness training
    - Information security documents review (e.g.: playbooks, policies, guidelines, best practices, etc.).
- Other activities supporting the implementation and improvement of ECMWF's information security programme.

Tenderers should present in their responses the list of the personnel involved in each of the above-mentioned work packages, along with a detailed curriculum, specifying to which work package/services the resource will be considered applicable. Such information should be updated every 6 months, or upon ECMWF request.

5 Scope

The following table contains the list of services (Web Applications, Assets, or Infrastructures) that need to be reviewed as part of the initial scope of the IT Security Review. For each target, the applicable Work Package (WP1, WP2 or WP3) is also specified (see sections above).

ID	Target type	Target	Test position	Test type	# of systems	Webapp - # of pages	Webapp - API # of endpoints	WP1 Vulnerability Assessment	WP2 Penetration Testing	WP3 Architecture Review	Priority
S.1	WebApp	Institutional website	External	Grey Box	1	3650	NO	Y	Y		High
S.2	WebApp	Confluence	External	Grey Box	1	>10.000	Many	Y	Y	Y	High
S.3	WebApp	Jira	External	Grey Box	1	>10.000	Many	Y	Y	Y	High
S.4	WebApp	Copernicus Atmosphere website	External	Grey Box	1	1700	0	Y	Y		High
S.5	WebApp	Copernicus Climate website	External	Grey Box	1	900	0	Y	Y		High
S.6	WebApp	Bitbucket	External	Grey Box	1	Many	1	Y	Y	Y	High
S.7	WebApp	Bamboo	External	Grey Box	1	Many	A few	Y	Y	Y	High
S.8	WebApp	JupiterHUB - Web application for remote access	External	Grey Box	1	5	a few	Y	Y		High

ID	Target type	Target	Test position	Test type	# of systems	Webapp - # of pages	Webapp - API # of endpoints	WP1 Vulnerability Assessment	WP2 Penetration Testing	WP3 Architecture Review	Priority
S.9	Infrastructure	Teleport	External	Grey Box	1	7	0	Y	Y	Y	High
S.10	Infrastructure	Common Cloud Infrastructure and European Weather Cloud service	External	Grey Box	50	N.A..	N.A.	Y	Y	Y	High
S.11	Infrastructure	VPNSSL Remote Access	External	Grey Box	4	4	N.A.	Y	Y		High
S.12	Infrastructure	ADC	External	Grey Box	24	N.A.	N.A.	Y		Y	High
S.13	Infrastructure	DDI & NTP infrastructure	External/Internal	Grey Box	16	N.A.	N.A.	Y		Y	High
S.14	Infrastructure	Storage Data Mover	Internal	Grey Box	1	N.A.	N.A.	Y	Y		High
S.15	Asset	MS Windows 11 image	Internal	Grey Box	1	N.A.	N.A.	Y			High
S.16	Asset	MS Windows 10 image	Internal	Grey Box	1	N.A.	N.A.	Y			High
S.17	Asset	Mac OS image	Internal	Grey Box	1	N.A.	N.A.	Y			High
S.18	Asset	Linux RedHat image	Internal	Grey Box	1	N.A.	N.A.	Y			High

ID	Target type	Target	Test position	Test type	# of systems	Webapp - # of pages	Webapp - API # of endpoints	WP1 Vulnerability Assessment	WP2 Penetration Testing	WP3 Architecture Review	Priority
S.19	Asset	Windows Server image	Internal	Grey Box	1	N.A.	N.A.	Y			High
S.20	Infrastructure	Linux Server image	Internal	Grey Box	1	N.A.	N.A.	Y			High
S.21	WebApp	Corporate websites	External	Grey Box	200	N.A.	1 per site	Y	Y		Medium
S.22	Infrastructure	FTP	External	Grey Box	2	5	0	Y	Y	Y	Medium
S.23	Infrastructure	Keycloack	External	Grey Box	4	5	1	Y	Y		Medium
S.24	Infrastructure	Internet Edge Routers	External	Grey Box	6	N.A.	N.A.	Y	Y	Y	Medium
S.25	Infrastructure	HPC systems	Internal	Grey Box	13	N.A.	N.A.	Y	Y		Medium
S.26	Infrastructure	HPC users facing nodes	External	Grey Box	1	N.A.	N.A.	Y	Y		Medium
S.27	WebApp	Energy Monitoring system	External	Grey Box	1	5	0	Y	Y		Low
S.28	Infrastructure	Vmware Vsphere	Internal	Grey Box	45	N.A.	N.A.	Y	Y		Low
S.29	Infrastructure	Network switches for SAN connection	Internal	Grey Box	1	N.A.	N.A.	Y	Y		Low
S.30	Infrastructure	NAS infrastructure	Internal	Grey Box	40	N.A.	N.A.	Y	Y		Low

ID	Target type	Target	Test position	Test type	# of systems	Webapp - # of pages	Webapp - API # of endpoints	WP1 Vulnerability Assessment	WP2 Penetration Testing	WP3 Architecture Review	Priority
S.31	Infrastructure	Storage infrastructure	Internal	Grey Box	200	N.A.	N.A.	Y	Y		Low
S.32	Infrastructure	Videoconference system	External	Grey Box	1	N.A.	N.A.	Y	Y	Y	Low
S.33	Infrastructure	Tape storage library device	Internal	Grey Box	1	N.A.	N.A.	Y	Y		Low