

RFP-587569-YG –
IT Security Penetration
Testing Services



IAEA
International Atomic Energy Agency

Statement of Work
dated 2022-08-26

Statement of Work

IT Security Penetration Testing Services



Contents

Acronyms.....	3
Definitions	5
Applicable Documents	7
1. Introduction.....	8
2. Scope	8
3. Requirements	9
3.1. Performance Requirements	9
3.2. Functional Requirements	11
3.3. Inputs	13
3.4. Outputs	13
4. Deliverables.....	13
4.1. Deliverable data items.....	13
4.2. Reporting	14
4.3. Logs and packet traces.....	16
4.4. Penetration Test Report Evaluation	17
5. Phases of the penetration tests	17
5.1. Pre-Engagement Activities.....	17
5.2. Engagement Phase (Discovery and Attack/Execution) activities	18
5.3. Post-Engagement Activities	18
6. Qualifications of Contractor and Contractor's Personnel	18
7. Information Handling Requirements	20
Annex I – IAEA Official Holidays.....	21
Annex II – Sample of the Terms of Reference	22



Acronyms

The following acronyms shall apply throughout the Statement of Work (SoW) unless defined otherwise hereinafter:

API	Application Programming Interface
ATT&CK®	Adversarial Tactics, Techniques and Common Knowledge by the company MITRE
BID	Bugtraq ID
CEH	Certified Ethical Hacker
CEPT	Certified Expert Penetration Tester
CET	Central European Time
CICA ITAC	Canadian Institute of Chartered Accountants Information Technology Advisory Committee
CIS V8	Critical Security Controls Version 8
CPT	Certified Penetration Tester
CSSLP	Certified Secure Software Lifecycle Professional
CVE	Common Vulnerabilities and Exposure
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
FISMA	Federal Information Security Modernization Act
GIAC	Global Information Assurance Certification
GPEN	Certified Penetration Tester
GSNA	GIAC Systems and Network Auditor
GWAPT	Web Application Penetration Tester
GWEB	GIAC Certified Web Application Defender
IaaS	Infrastructure as a Service
IAEA	International Atomic Energy Agency



ICT	Information and Communication Technology
iOS	iPhone Operating System
IoT	Internet of Things
ISC ²	International Information System Security Certification Consortium
ISO	International Standards Organization
IT	Information Technology
LAN	Local Area Network
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSBDB	Open-Source Vulnerability Database
OSCP	Offensive Security Certified Professional
OSINT	Open-Source Intelligence
OSSTMM	Open-Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PHP	Hypertext Preprocessor
PTES	Penetration Testing Execution Standard
SaaS	Software as a Service
SOC	Security Operations Center
SoW	Statement of Work
U.S.	United States
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol



Definitions

The following definitions shall apply throughout the Statement of Work (SoW) unless defined otherwise hereinafter:

Application-layer testing	Testing that typically includes websites, web applications, thick clients, or other applications.
Black-box testing	A method of testing where the tester has no inside knowledge of the security design of the tested objects. This method best simulates an external hacker scenario.
Blue team	Defensive security professionals responsible for maintaining internal network defences against all cyber-attacks and threats.
Common Vulnerability Scoring System (CVSS)	Provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
Grey-box testing	A combination of black-box and white-box testing. A method of testing where the tester has limited knowledge of the security design of the tested objects. This method best simulates an internal threat scenario.
IAEA working day	Monday – Friday, from 08:00 a.m. until 18:00 p.m. Central European Time (CET), except IAEA Official Holidays (for the detailed information, refer to Annex I).
National Vulnerability Database (NVD)	The United States (U.S.) government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g., Federal Information Security Modernization Act (FISMA)).
Network-layer testing	Testing that typically includes external/internal testing of networks (Local Area Network (LANs)/Virtual Local Area Network (VLANs)), between interconnected systems, wireless networks.
Penetration tester or team	The individual(s) conducting the penetration test for the entity. They may be internal or external to the entity.
Purple teaming exercise	A security assessment in which red and blue teams work closely together to maximise cyber capabilities through continuous feedback and knowledge transfer.
Red team	Offensive security professionals who are experts in attacking systems and breaking into defences.



Red teaming exercise	a security assessment where a red team is trying to break into systems and a blue team needs to detect and respond to attacks with both teams working in isolation.
Social engineering	Usage of psychological manipulation to gain access to confidential information or bypass technical security controls.
White-box testing	A method of testing where the tester has full knowledge of the security design of the tested objects. This method provides best value for money.



Applicable Documents

The following documents shall be applicable for the work to the extent specified hereinafter:

1. International Standards Organization (ISO) 27001;
2. National Institute of Standards and Technology (NIST) SP 800-115;
3. Penetration Testing Execution Standard (PTES);
4. Open-Source Security Testing Methodology Manual (OSSTMM); and
5. Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) by the company MITRE.

In the event of conflict between the documents listed above and the content of this SoW, the content of this SoW shall take precedence to the extent of the conflict.



1. Introduction

This Statement of Work (SoW) describes the requirements for the procurement of Information Technology (IT) Security Penetration Testing Services (hereinafter referred to as the "Services"). These Services are meant to both complement the International Atomic Energy Agency's (IAEA or the Agency) in-house capabilities where they may already exist and provide additional capabilities where gaps may exist. These Services can also be called upon during periods of high activity, to provide additional capacity.

The Services are instrumental to support the evolving organizational tasks of securing complex IT environments whilst delivering business objectives. To ensure that this process is successfully accomplished, it is essential that the probability of a security weakness being accidentally exposed or maliciously exploited is continually assessed – such as via a penetration test – to ensure that the level of risk is at an acceptable level to the business.

Penetration testing is one of the IT Security assessment techniques, and it involves the use of a variety of manual and automated techniques to simulate an attack on an organization's information security arrangements.

Penetration testing looks to exploit known vulnerabilities but should also use the expertise of the tester to identify specific weaknesses – unknown vulnerabilities – in an organization's security arrangements.

The Agency's Information and Communication Technology (ICT) infrastructure and computing environment consists of state-of-the-art hardware and software platforms.

2. Scope

The following Security Assessment and Security Information Services are within the scope of this SoW:

- Application penetration testing;
- Mobile application penetration testing;
- Infrastructure penetration testing;
- Cloud application penetration testing;
- Cloud environments, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), penetration testing;
- Cloud Application Programming Interface (APIs) penetration testing;
- Cloud Distributed Denial of Service (DDoS) testing;



- Device penetration testing, including workstations, servers, laptops, and mobile devices – tablets and smartphones;
- Wireless penetration testing;
- Telephony or Voice over Internet Protocol (VoIP) penetration testing;
- “Internet of Things” (IoT) device testing;
- Simulated attacks and capture the flag tests/social engineering testing;
- Validation of 3rd party assessment results;
- Red/Blue/Purple Team exercises;
- Ransomware simulation;
- Threat hunting;
- Social Engineering – Insider threat scenario;
- Adversarial simulations; and
- Assessment of Security Operations Center (SOC) detection capabilities.

The IAEA may request the Services for any of the wide range of ICT resources and systems it manages and hosts. Additionally, the Services and deliverables provided by the Contractor may be used by, or shared with, other internal IT groups or project teams within the IAEA.

3. Requirements

3.1. Performance Requirements

- 3.1.1. The Contractor shall provide the Services on an on-call basis. There is a potential need for quick response times to unplanned and short notice service requests.
- 3.1.2. The IAEA understands that there may be circumstances where a Contractor does not have appropriately qualified resources available for a specific Service request on short notice. For these reasons, the IAEA will clearly identify the priority of all service requests.
- 3.1.3. The response times required for this offering are listed in the table below:

Priority	Initial Contractor Response Time	Scheduled Time to initiate work request
High	Three (3) IAEA working days	Two (2) weeks after initial response
Normal	One (1) week	Four (4) weeks after initial response



It is expected that high priority requests form five (5) % of the total services requested.

3.1.4. The Contractor will provide Services on IAEA workdays (Monday – Friday) and during normal business hours (08:00 a.m. – 18:00 p.m. CET). Exceptionally, tests might be performed outside of working hours but only with prior agreement.

3.1.5. Onsite and Offsite Services: The Contractor shall clearly define methodologies and definitions of the onsite and offsite Services. In the case of onsite Services, the schedule time shall be considered as the time for the Contractor to be at the IAEA premises (at this moment Vienna, Austria, Seibersdorf, Austria, Monaco, Toronto, Canada, and Tokyo, Japan). The vast majority of the work (>95%) is expected to take place in Vienna, Austria.

3.1.6. Tools and licenses: The Contractor shall not charge IAEA additional costs for the use of tools, devices, licenses, etcetera.

3.1.7. The Contractor shall be capable of demonstrating adherence to at least one of the following penetration testing methodologies, security standards, and security frameworks:

- OSSTMM;
- Open-Source Intelligence (OSINT);
- Open Web Application Security Project (OWASP);
- Canadian Institute of Chartered Accountants Information Technology Advisory Committee (CICA ITAC);
- ISO 27001/27002;
- ISO 17799;
- NIST SP 800-115;
- Critical Security Controls Version 8 (CIS V8);
- PTES; and/or
- MITRE ATT&CK®.

3.1.8. The Contractor shall be capable of providing “Continuous and scheduled penetration testing capabilities” by performing penetration tests on a per engagement basis and conducting them with various degrees of pre-assessment knowledge (white box/black box/grey box).

- 3.1.9. The Contractor shall be capable of performing code review (static and dynamic) and code disassembly and reverse engineering when expressly requested by the IAEA on code developed within the Agency (mainly .NET and Hypertext Preprocessor (PHP). The Contractor shall clearly define the methodologies of the code review, code disassembly and reverse engineering services.
- 3.1.10. Security testing shall be done at the level sufficient to allow the Agency to adequately measure the effectiveness of security awareness efforts and may be requested to be conducted in the form of active exploitation of undesirable behaviour. For example, creating authorized phishing and spear phishing attacks; creating malicious websites to deliver proof-of-concept malware, social engineering, and other methods to create information breaches, email security testing through phishing attacks and phishing security awareness testing, etc.

3.2. Functional Requirements

- 3.2.1. Application penetration testing: Applications testing may consist of the manual probing of application interfaces, automated fuzzing, development of test datasets and harnesses, and performing manual or automated code review.
- 3.2.2. Mobile Application penetration testing: A general scope of this activity is the same as is outlined in brief in 3.2.1. but relates to mobile iPhone Operating System (iOS) applications.
- 3.2.3. Infrastructure penetration testing: Infrastructure penetration testing may be focused on any elements of the infrastructure. Security assessments may be requested for specific high- value hosts, operating systems, virtual machine configurations, secure communications, domain trusts or entire networks.
- 3.2.4. Cloud application penetration testing: A general scope of this activity is the same as outlined in brief in 3.2.3. but relates to cloud applications.
- 3.2.5. Cloud environments, such as Microsoft Azure or Oracle Cloud including Infrastructure as a Service (IaaS): A general scope of this activity is the same as outlined in brief in 3.2.3. but relates to IaaS.



- 3.2.6. Platform as a Service (PaaS) – Software as a Service (SaaS), penetration testing: A general scope of this activity is the same as outlined in brief in 3.2.3. but relates to PaaS and SaaS. For PaaS, the Contractor shall perform checks on the configuration, versions, and ports. For SaaS, the Contractor shall perform web application vulnerability reviews.
- 3.2.7. Cloud APIs penetration testing: Various analyses related to cloud APIs security, availability, and non-repudiation. Details are provided on a case-by-case basis.
- 3.2.8. Cloud DDoS testing: Various security analyses (e.g., analyse vulnerabilities that can lead to a DDoS) related to cloud DDoS attacks' mitigation. Details are provided on a case-by-case basis.
- 3.2.9. Device penetration testing, including workstations, servers, laptops, and consumer devices (tablets and smartphones). This involves mainly black-box testing but could also include grey-box testing.
- 3.2.10. Wireless penetration testing, telephony, or VoIP penetration testing.
- 3.2.11. Simulated attacks and capture the flag tests/social engineering testing: technical exercises with pre-defined end goals intended to develop and improve real time efficiency of IT Security personnel in situations that are close to real attack scenarios.
- 3.2.12. Validation of 3rd Party Assessment Results: Requests may be made to validate the results and findings of security assessments provided by 3rd parties or internal staff. The requested validation may entail physically reproducing the tests or reviewing the results to determine if the tests were conducted in a reasonable and consistent manner.
- 3.2.13. Adversarial simulations based on real attack scenarios in order to evaluate the effectiveness of the Agency's security controls and the security team's ability to identify and contain an actual attack.
- 3.2.14. Assessment of SOC detection capabilities by simulating attacker techniques and see if these get detected.



3.3. Inputs

- 3.3.1. The Contractor shall conduct a thorough review of the Agency's existing ICT infrastructure as it relates to the scope of each individual security assessment/exercise requested and defined by the Agency on a case-by-case basis.
- 3.3.2. The Contractor shall combine this collected information with the necessary technical expertise and due diligence to design customised targeted security evaluations and conduct them in the best interests of the Agency.

3.4. Outputs

- 3.4.1. The Contractor shall regularly communicate results and outcomes of his/her work both verbally (through regularly scheduled briefings) and in writing. The Contractor will be requested to deliver presentations to targeted audiences (i.e., members of multidisciplinary ICT teams and the management) as required.
- 3.4.2. The Contractor shall work with the technical resolvers in the Agency to review and help prioritize recommendations.
- 3.4.3. The Contractor shall prepare various reporting documents with actionable recommendations as described below.

4. Deliverables

4.1. Deliverable data items

The Contractor shall deliver the following data items:

- 4.1.1. The Contractor shall provide a report on all assessments. Not all assessments require the same level of detail. The type of report required will be identified in the service request.
 - 4.1.1.1. Full report – includes all assessment raw data, summary data and recommendations; and



4.1.1.2. Brief report – includes summary data and recommendations

4.1.2. The Contractor shall be transparent when it comes to reporting and include documentation on the processes, tools and approaches used to complete the services. There will be no ambiguity in what will be delivered at the conclusion of the tasks since deliverables will have been agreed upon in enough detail prior to commencement of the engagement.

4.1.3. The Contractor shall be skilled enough to explain all the identified findings and sufficiently determine the severity of this finding, considering the architecture and security controls existing within the IAEA networks.

4.2. Reporting

4.2.1. The **Full Report** shall contain as minimum:

- 4.2.1.1. Executive Summary: Brief high-level summary of the penetration test scope and major findings;
- 4.2.1.2. Statement of Scope: A detailed definition of the scope of the network and systems tested as part of the engagement;
- 4.2.1.3. Overview of systems tested and explanation of why they are included in the test as targets;
- 4.2.1.4. Statement of Methodology: Details on the methodologies used to complete the testing;
- 4.2.1.5. Statement of Limitations: Document any restrictions imposed on testing such as designated testing hours, bandwidth restrictions, special testing requirements for legacy systems, etc.;
- 4.2.1.6. Testing Narrative: Provide details as to the testing methodology and how testing progressed, document any issues encountered during testing;
- 4.2.1.7. Segmentation Test Results: Summarize the testing performed to validate segmentation controls;
- 4.2.1.8. Findings: Whether/how the findings may be exploited;



- 4.2.1.9. Risk ranking/severity of each finding;
- 4.2.1.10. Compensating controls identified that reduce the likelihood of compromise
- 4.2.1.11. Targets affected;
- 4.2.1.12. References (if available): Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Bugtraq ID (BID), Open-Source Vulnerability Database (OSBDB), etc.;
- 4.2.1.13. Description of finding; and
- 4.2.1.14. Tools Used.

4.2.2. The **Brief Report** shall contain as minimum:

- 4.2.2.1. Executive Summary: Brief high-level summary of the penetration test scope and major findings;
- 4.2.2.2. Statement of Scope: A definition of the scope of the network and systems tested as part of the engagement;
- 4.2.2.3. Identification of critical systems and explanation of why they are included in the test as targets;
- 4.2.2.4. Findings: Whether/how the findings may be exploited Risk ranking/severity of each vulnerability;
- 4.2.2.5. Targets affected; and
- 4.2.2.6. Description of finding.

4.2.3. Reporting – Industry Standard References: Discovered findings should be mapped to well-known industry- standards if applicable:

- 4.2.3.1. National Vulnerability Database (NVD);
- 4.2.3.2. Common Vulnerability Scoring System (CVSS);



4.2.3.3. CVE;

4.2.3.4. CWE;

4.2.3.5. BID; and

4.2.3.6. OSVDB.

4.2.4. Reporting – Retesting Report Outline: To test the remediation of findings, the report shall contain at least:

4.2.4.1. Executive Summary;

4.2.4.2. Date of Original Test;

4.2.4.3. Date of Retest;

4.2.4.4. Original Findings; and

4.2.4.5. Results of Retest.

4.2.5. IAEA may request in special cases to use IAEA reporting standards (e.g., document templates).

4.3. Logs and packet traces

4.3.1. To ensure accountability of actions taken during the engagement, optionally and at the discretion of the IAEA, the Contractor shall undertake to log and trace every network packet sent and received between the Contractor's testing equipment and the IAEA infrastructure (whether on premise or in the cloud). Packet traces shall be provided to the IAEA at the conclusion of the engagement in an agreed upon industry standard format. Packet trace data shall be encrypted at rest and shall be provided via an encrypted digital method to be agreed upon at the start of each engagement and is subject to the same confidentiality and destruction guidelines outlined in section 7 – Information Handling Requirements.



4.4. Penetration Test Report Evaluation

- 4.4.1. Penetration test reports will be evaluated by IAEA specialists and periodically reviewed with the Contractor to assure/improve the quality of the provided services.
- 4.4.2. The report evaluation check list will be provided by the IAEA.
- 4.4.3. For user awareness testing through penetration tests, metrics shall be provided regarding target groups, target success metrics and related statistics and data and as provided at the beginning of the engagement.

5. Phases of the penetration tests

5.1. Pre-Engagement Activities

- 5.1.1. Every engagement shall be preceded by a scheduled kick-off meeting. The kick-off meeting will be used to review the rules of engagement, define the success criteria, and review the methodology to be used in accordance with information system security assessment best practices such as described by the OSSTMM, NIST SP800-115, OWASP testing methodology as defined in the Testing Guide.
- 5.1.2. The Contractor shall review the scope provided by the IAEA to ensure that that the proper assets and targets are part of examination. Any differences in scope shall be noted, investigated, and agreed upon prior to start. The process to assess whether an IAEA asset or target is considered by the IAEA as a proper part of the examination will be defined on a case-by-case basis.
- 5.1.3. The extent to which post-exploitation techniques are performed shall be defined prior to the start of test to prevent the tester from putting production systems at risk of destabilization.
- 5.1.4. The Contractor shall provide a single point of contact with a backup that will be available for near real-time response throughout the duration of the engagement phase. In case a serious vulnerability is identified, the Contractor's point of contact shall be available within one (1) hour. In parallel, the IAEA will provide a point of contact for the Contractor for the duration of the engagement.



- 5.1.5. Transmission methodology (e.g., encrypted email, encrypted chat) of activities status, identified vulnerabilities, reports shall be agreed prior to the engagement phase.

5.2. Engagement Phase (Discovery and Attack/Execution) activities

- 5.2.1. Main findings identified shall be reported in near real time to the appointed IAEA contact point. Please refer to paragraph 4.2 for the reporting requirements.

- 5.2.2. For infrastructure which is not under the control of the IAEA, such as cloud environments, express permission shall be requested and granted by the Agency before penetration testing can commence and schedules shall be agreed and strictly adhered to by the Contractor.

5.3. Post-Engagement Activities

- 5.3.1. The Contractor is responsible for cleaning up the IT environment (i.e., update/removal of test accounts or database entries added or modified during testing, uninstall of test tools or other artefacts, and restoring active protection-system settings).

- 5.3.2. If the Contractor is not able to clean up the changes made in the IT environment anymore (e.g., due to the removal of permissions), they need to provide detailed instructions on how the clean-up should be performed and how to verify security controls have been restored.

6. Qualifications of Contractor and Contractor's Personnel

- 6.1. The following requirements for the Contractor have been defined: The Contractor shall specialize in the penetration testing service areas covered by this SoW.

- 6.2. The Contractor shall employ personnel or sub-contract personnel who fulfil the following qualification requirements:

- 6.2.1. Good command of the English language (written and oral);



- 6.2.2. A minimum of five (5) years of experience in providing penetration testing services;
- 6.2.3. Experience providing penetration testing services in a highly confidential environment (if required for the engagement);
- 6.2.4. A proven record of at least five (5) satisfied customers of similar sized environments as the Agency to whom the relevant service was provided from 2020 to date. This information shall be available in the form of (anonymised) customer references;
- 6.2.5. Industry certifications or similar qualifications appropriate to the services provided, such as one of those listed below:
 - 6.2.5.1. Global Information Assurance Certification (GIAC) Certified Penetration Tester (GPEN);
 - 6.2.5.2. GIAC Web Application Penetration Tester (GWAPT);
 - 6.2.5.3. Certified Ethical Hacker (CEH);
 - 6.2.5.4. GIAC Systems and Network Auditor (GSNA);
 - 6.2.5.5. Certified Penetration Tester (CPT);
 - 6.2.5.6. Certified Expert Penetration Tester (CEPT);
 - 6.2.5.7. GIAC Certified Web Application Defender (GWEB);
 - 6.2.5.8. International Information System Security Certification Consortium (ISC)² Certified Secure Software Lifecycle Professional (CSSLP);
 - 6.2.5.9. Offensive Security Certified Professional (OSCP); and/or,
 - 6.2.5.10. CREST Penetration Testing Certifications.



7. Information Handling Requirements

The following requirements for handling Agency information have been defined:

- 7.1. The Contractor shall sign the IAEA Confidentiality Agreement and ensure that all personnel providing services or having access to information related to the services provided under this contract have signed either the IAEA Confidentiality Agreement or a similarly restrictive Non-Disclosure Agreement with the Contractor;
- 7.2. Transmission of requests for services or reports and other output that contain sensitive information shall be encrypted during transmission between the Contractor and the IAEA. The method of encryption and management of key material shall be agreed upon by both parties;
- 7.3. Storage of sensitive information relating to current or past vulnerabilities or IT security incidents at the Contractor site shall be protected to ensure there is no unauthorized release of information. After providing a copy of all information related to a specific request for services, the Contractor shall provide assurance to the IAEA that all sensitive information related to the service request has been permanently removed; and
- 7.4. Additionally, every engagement will be subject to the IAEA's Terms of Reference (ToR). This document includes the objectives and scope of the assignment, the requirements towards the specific task(s), the timelines, location of work, expected deliverables, the IAEA support provided during the engagement, and the IAEA point of contact. A sample ToR document is available in Annex II.

Annex I – IAEA Official Holidays

Year 2022

No.	Date	Holiday
1.	Monday, 3 January	(in lieu of 1 January) New Year's Day
2.	Friday, 15 April	Good Friday
3.	Monday, 18 April	Easter Monday
4.	Monday, 2 May	(in lieu of 1 May) May Day
5.	Tuesday, 3 May	Eid al-Fitr
6.	Monday, 11 July	(in lieu of 10 July) Eid al-Adha
7.	Wednesday, 26 October	Austrian National Day
8.	Monday, 26 December	(in lieu of 25 December) Christmas Day
9.	Tuesday, 27 December	(in lieu of 26 December) St. Stephen's Day

Year 2023

No.	Date	Holiday
1.	Monday, 2 January	(in lieu of 1 January) New Year's Day
2.	Friday, 7 April	Good Friday
3.	Monday, 10 April	Easter Monday
4.	Monday, 24 April	(in lieu of 22 April) Eid al-Fitr
5.	Monday, 1 May	May Day
6.	Thursday, 29 June	Eid al-Adha
7.	Thursday, 26 October	Austrian National Day
8.	Monday, 25 December	Christmas Day
9.	Tuesday, 26 December	St. Stephen's Day

Source: [United Nations Information Service](#).

Annex II – Sample of the Terms of Reference

Red Team Cybersecurity Attack Simulation

1. Background

The International Atomic Energy Agency (hereinafter referred to as the IAEA), located in Vienna, Austria is widely known as the world's "Atoms for Peace" organization within the United Nations family. Established in 1957 as the world's centre for cooperation in the nuclear field, it works together with its Member States and multiple partners worldwide to promote the safe, secure and peaceful use of nuclear technologies. The IAEA Secretariat is made up of approximately 2,500 international professional and support staff from scientific, technical, managerial and other professional disciplines.

The IAEA Information and Communication Technology (ICT) infrastructure and computing environment consists of hardware and software platforms managed by the Division of Information Technology (MTIT) in the Department of Management.

These Terms of Reference (ToR) describe the IAEA's requirements for an enterprise-wide security assessment of the networks and systems under its control.

2. Objectives and Scope

The assessment should emulate an attack on the IAEA by an external, skilled threat actor, to assess the organization's ability to detect and thwart sophisticated and motivated threats. The Contractor shall:

- 2.1. Emulate the actions and activities of a skilled cyber attacker and attempt to compromise the IAEA's applications, systems and data;
- 2.2. Identify vulnerable systems, missing security controls and potential detection blind spots that an attacker would exploit; and
- 2.3. Provide feedback on the maturity of the IAEA's intrusion detection and incident response.

The scope of the assessment will include the following domains: [iaea.org](https://www.iaea.org) (managed by MTIT). The Contractor shall test scenarios 1 and 2 below, as follows:

Scenario 1: Try to compromise the [iaea.org](https://www.iaea.org) domain and gain Domain Admins and Enterprise Admins privileges using a non-IAEA laptop from within the Vienna International Centre (VIC); and

Scenario 2: Try to compromise the iaea.org domain and gain Domain Admins and Enterprise Admins privileges using an IAEA laptop with the standard MTIT image and a non-privileged MTIT user account.

3. Requirements

The Contractor shall conduct this assignment using experts with a minimum of five (5) years of experience in penetration testing. The Contractor shall ensure that the experts assigned to this assignment do not have any conflicts of interest.

The Contractor shall not share any information related to this assignment with any parties, within or outside the IAEA, without the prior authorization of the Director of MTIT/Chief Information Officer (CIO).

Electronic communication of “sensitive” information between the Contractor and the IAEA shall be properly protected by mutually agreed methods.

The Contractor shall not interact with or probe any systems that are not part of this assessment. The Contractor’s testers shall ensure that all the tests are authorized. The IAEA shall be responsible for gaining authorization from third party suppliers of IT services such as Microsoft’s Azure, should the scope of this engagement exceed the Contractor’s penetration and security testing rules of engagement. For example, those of Microsoft can be found at www.microsoft.com/en-us/msrc/pentest-rules-of-engagement.

The Contractor shall not use social engineering techniques or (distributed) denial of service attacks to achieve the engagement’s objectives.

The Contractor shall be responsible for logging every action and recording, in detail, the tools, techniques, tactics and observables used during the assessment.

The Contractor will be responsible to document changes made in the Agency’s ICT environment. This documentation is provided to the Agency at the end of the engagement so that changes can be reverted to normal.

The Contractor will be responsible to report unavailability of services, that could have been caused by this engagement, to the point of contact.

4. Timeline and Duration of Work

The assessment is expected to start on <DATE>. The final assessment report should be provided no later than two (2) weeks after the completion of the assignment. Any change of the specified date shall be approved by MTIT.

The duration of the assessment should not exceed 30 working days.



5. Location of Work

The Contractor's services shall be conducted on the IAEA's premises in the VIC, Vienna, Austria.

6. Deliverables

The Contractor shall provide the deliverables for the assignment as follows:

- Kick-off meeting: Meet key people; provide background information and hold question and answer session; define targets; identify assets and ground rules of engagement; and make a schedule of authorizations;
- On-site testing: Test the ICT infrastructure on the IAEA premises according to the agreed scope, approach and duration;
- Exit meeting: At the end of the assignment, organize a meeting on the IAEA premises to present a summary of the findings; and
- Report writing: Deliver the Final Report on the assignment.

The Final Report shall include a description of the tests performed, the findings, the risk ratings of the findings and the Contractor's opinion on the assessment results, as defined in the Contract Statement of Work Section 4.2. The report should also contain detailed descriptions of the verified vulnerabilities and the specific risks that these might pose, including by what methods and to what extent they might be exploited. The report should also include an executive summary of the assignment along with any major findings.

For every confirmed vulnerability, the Contractor shall provide the exact scripts, configurations, parameters and step-by-step instructions on how to replicate the findings.

The Contractor shall deliver the Final Report in the English language for review and approval by MTIT. The report shall be delivered encrypted in softcopy. All work products, intermediate and final deliverables are subject to quality review and formal approval by the IAEA.

7. IAEA Support for the Assignment

The IAEA shall provide on its premises at the VIC, the infrastructure requested by the Contractor to carry out the assignment, such as office space, office equipment and internet connectivity, and physical access to the VIC.



8. Point of contact

The following IAEA staff will be the point of contact for this engagement:

<Name>

<Location>

Wagramerstrasse 5

1400 Vienna, Austria

Email: <name@iaea.org>

Phone: <ext.>

Mobile: <number>