IDM UID
APPVAN

VERSION CREATED ON / VERSION / STATUS
13 May 2024 / 1.1 / Approved

EXTERNAL REFERENCE / VERSION

Technical Specifications (In-Cash Procurement)

TECS_2024-02_CFT_IT Security Global Support

TECS_2024-02_CFT_IT Security Global Support

PDF generated on 27 May 2024

DISCLAIMER : UNCONTROLLED WHEN PRINTED – PLEASE CHECK THE STATUS OF THE DOCUMENT IN IDM

SERVICE

Table of Contents

SERVICE

1 Preamble

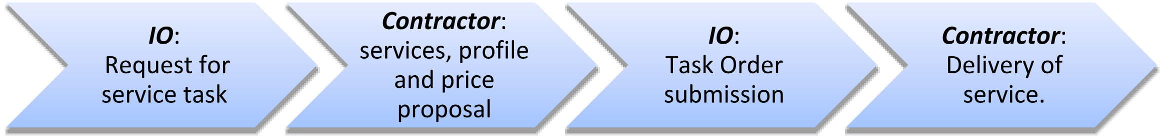
This Technical Specification is to be read in combination with the General Management Specification for Service and Supply (GM3S) – [Ref 1] that constitutes a full part of the technical requirements.

In case of conflict, the content of the Technical Specification supersedes the content of Ref [1].

2 Purpose

These technical specifications define the scope of work under a framework contract(s). The IO/IT (ITER Organization Information Technology) seeks a Contractor(s) to provide consulting and expertise services for assessing, reinforcing and managing the IT Security of its infrastructure.

Once the framework contract(s) is in place, IO IT will set up task orders through the following process for each Lot:



IO: Request for service task

Contractor: services, profile and price proposal

IO: Task Order submission

Contractor: Delivery of service.

Lots

The present technical specifications are divided in 2 lots:

Lot 1: Enhanced Cybersecurity Workforce

Under this lot, we are seeking a Contractor to provide skilled professional services. These services will play a pivotal role in offering Level 2 expertise for the CyberSecurity Operation Center (SOC) operations. Additionally, they will internally lead cybersecurity improvement projects throughout the contract duration. The contractor for Lot 1 is expected to provide full-time involvement, ensuring continuity, and contributing to the proactive enhancement of our cybersecurity capabilities.

Lot 2: High-level Cybersecurity Expertise

Lot 2 is designed for highly skilled cybersecurity services who can contribute on an ad-hoc basis to specific projects. This expertise will form part of project teams engaged in critical initiatives, providing specialized insights and support as required. We seek services with a proven track record in delivering results within specific project scopes.

3 Acronyms & Definitions

3.1 Acronyms

The following acronyms are the main one relevant to this document.

Abbreviation	Description
CRO	Contract Responsible Officer
GM3S	General Management Specification for Service and Supply
IO	ITER Organization
PRO	Procurement Responsible Officer
SIEM	Security information and event management
MFA	Multi Factor Authentication
IoT	Internet of Things
OT	Operational Technology

3.2 Definitions

Contractor: shall mean an economic operator who have signed the Contract in which this document is referenced.

4 Applicable Documents & Codes and standards

This is the responsibility of the Contractor to procure the relevant Codes and Standards applicable to the scope of work described below in 5.

4.1 Applicable Documents

This Technical Specification takes precedence over the referenced documents. In case of conflicting information, this is the responsibility of the contractor to seek clarification from IO.

Ref	Title	IDM Doc ID	Version
1	General Management Specification for Service and Supply (GM3S)	82MXQK	1.4

4.2 Applicable Codes and Standards

This is the responsibility of the contractor to procure the relevant Codes and Standards applicable to the scope of work as described below.

5 Scope of Work

5.1 IO Technical environment

- Servers environment:
  - Windows Server;
  - HyperV clusters;
  - Linux;
  - Kubernetes, Docker.

SERVICE

- Business applications:
  - SAP;
  - .NET VB, C#;
  - SmartPlant, PLM;
  - Catia/Enovia.
- Scientific computing:
  - HPC Linux (RedHat Satellite, 2500 cores, 200 users, 25TB of data).
- Networking:
  - Cisco Networking;
  - Cisco Wifi.
- IT Security:
  - F5 BigIP;
  - Checkpoint FW;
  - PaloAlto FW;
  - Fortinet FW;
  - SIEM: Elastic Search Cluster, Logstash, Kibana, TheHive, Cortex;
  - MS Defender;
  - Sysmon;
  - Security VA: Nessus.
- Cloud services:
  - Azure / Entra ID;
  - Microsoft security, Azure security center, Microsoft Defender.
- Access control and physical security systems.
- Digital instrumentation and control:
  - SCADA systems:
    - EPICS,
    - SIMATIC WinCC Open Architecture, WinCC;
  - RHEV + RHS storage;
  - Plant system slow controller: Siemen Step7 PLC;
  - Plant system fast controllers: industrial grade PC, IO chassis (NI PXIe, NI cRIO, xTCA).

Field device controllers and their fieldbus protocol, such as Modbus, Profibus…

5.2 IO/IT Security

5.2.1 IT Security approach at IO

IO operates its Cybersecurity mainly through the management of an internal CyberSecurity Operation Center (SOC) built on ELK, centralizing all pertinent logs from our servers and security equipment. As of today, IO/IT is not willing to externalize its SOC.

In this context, the Lot 1 Contractor will concentrate on running the SIEM platform (run) to operate early detection, advanced end-point threat detection, malware protection and exploit the detection tools (blue team activities for defensive security). Part of their work will also be dedicated to managing security improvements projects (build) to further reinforce our security posture.

Lot 2 services will provide the necessary audit and remediation actions to certify the compliance with applicable regulations of our critical infrastructures but also the required high-level expertise and experience to facilitate the achievement of the IO/IT Security roadmap.

SERVICE

Also, digital instrumentation and control (I&C) systems and equipment play an important role in the ITER IT ecosystem. ITER operations are highly integrated I&C systems and it is foreseen that some of the tasks ordered on this Lot 2 framework contract will focus on cybersecurity of I&C systems.

Complementary to the main tasks of each Lot, contractors from both Lots might be requested to lead and/or contribute to IT projects enhancing IT Security in ITER.

5.3 Work description

5.3.1 Lot 1 – Enhanced Cybersecurity Services

5.3.1.1 Presentation

The IO/IT seeks professional consulting services to advise, perform, or assist in performing various tasks in IT Security Operations. The requested tasks of this lot are supporting IT Security operations and governance and require a long-term investment in the IO IT infrastructure. It is therefore expected that the Contractor team will be mainly dedicated to the IO (full-time or regular part-time) and will join the IO internal IT Security team. The appointment of a Contractor Project Manager is encouraged for the duration of this contract.

In addition, specific IT Security projects could call for specific expertise for predefined time period. IO/IT could request from the Contractor expertise services to fulfil a specific task delivery in these projects in coordination with an IO representative. In the case project implementation that requires a commercial solution, the IO will conduct separate procurement actions. They are outside of the scope of this Lot 1 Contract.

5.3.1.2 Scope

The requested services will mostly, but not exclusively, comprise the following activities:

- Activity 1 - Regular IT Security operations (run).
  - SOC Analysis:
    - SIEM alert qualification and handling,
    - Security incident handling, incident validation and immediate response (Forensic investigations, suspicious email analysis, …);
  - Handling ServiceDesk tickets for IT security;
  - Vulnerability management (Vulnerability report analysis and bug bounty follow up);
  - IT Security performance reporting;
  - IT Security infrastructure operational maintenance and monitoring;
  - Perform regular IT Security controls;
- Activity 2 - IT Security Improvement program:
  - IT Security infrastructure continuous improvements;
  - IT Security follow up in IT projects;
  - Assistance with the implementation of IO information security management program;
  - IT Security awareness campaigns;
  - Project management and implementation related to the IT Security Roadmap; Eg: *Awareness raising program, MFA roll-out, Bastion, Client & Server hardening, SOC Playbook and ruleset improvement, etc.*
- Activity 3 – IT Security assessments and expertise:
  - Conduct IT Security maturity / risk assessment on IO infrastructure;

- Bring advanced IT Security expertise on cutting edge technologies;
- Perform technical audits and reviews (Web application, internal and physical pentesting, I&C Security).

These activities, including SIEM monitoring, are currently running 8h x 5 days, France time, and not 24/7. However, the Contractor could offer off-site resources in different time zone as to expand the first level monitoring period of the SOC.

5.3.1.3 Profile matching

The final scope of activities assigned to the Contractor's team will depend on their skills and experience. The table below will give an overview of the considered profiles in the Contractor's team for each type of activity:

Activity	**Preferred profiles**
Activity 1 - SOC analysis level 1/2	Junior
Activity 1 - SOC analysis level 2/3	Confirmed
Activity 2 - Projects / build	Confirmed / Senior
Activity 3 - Audit / Expertise	Senior / Expert

5.3.1.4 Deliverables

Operational IT security services updated and maintained IT Security infrastructure, updated project (project initiation document, highlight reports, exception reports, closure report, meeting notes, release notes, etc.), technical (developer guide, administration guide, operations guide) and service (user, internal) documentation; description of tasks as JIRA tickets; updated user documentation; Audit reports, executive summary.

5.3.1.5 Place of execution

Place of execution depends on the type of service requested and shall be agreed with IO/IT before service execution. The three activities can be performed either from ITER site or from a remote location (IO can provide virtual desktop infrastructure access to the contractors).

5.3.2 Lot 2 – High level IT Security Consulting Services

5.3.2.1 Presentation

The objective of this lot is to provide occasional high-level expertise to the IO on some specific issues or lead projects for a short duration but normally with very high level of competency. The Contractor's team shall be consisted of highly qualified and experienced cybersecurity experts who can assist IO in various domains such as cyber incident handling, applied cybersecurity, managed security, IoT, etc.

5.3.2.2 Scope

The tasks that the Contractor may be required to perform include, but are not limited to, the following:

- Conduct proactive threat hunting and analysis; facilitate incident response after significant security event.
- Provide guidance and recommendations on how to improve the detection and response capabilities of the IO security operations centre (SOC).

SERVICE

- Deliver comprehensive security assessments and audits of IO's IT infrastructure, data, identity, and cloud environments.
- Design and implement security solutions for critical resources, such as IoT or OT devices, using advanced technologies and best practices.
- Provide training and awareness programs on cybersecurity topics and trends for the IO staff and stakeholders.
- Support the IO in developing and executing a cybersecurity strategy and roadmap that aligns with its business objectives and compliance requirements.
- Manage and coordinate complex cybersecurity projects, such as migration to a secure cloud, implementation of a zero-trust model, or deployment of a cyber-resilience framework.
- Respond to and mitigate cybersecurity incidents and breaches.
- Provide regular reports and feedback on the performance and quality of the service, as well as the satisfaction and needs of the IO.

The Contractor will be expected to demonstrate a high level of professionalism, flexibility, and responsiveness, as well as a deep understanding of the IO context and challenges. The Contractor will also be expected to adhere to the highest standards of ethics, confidentiality, and security.

5.3.2.3 Deliverables

Audit reports, executive summary, project updated documentation (project initiation document, highlight reports, exception reports, closure report, meeting notes, release notes, etc.).

5.3.2.4 Place of execution

Place of execution depends on the type of service requested and shall be agreed with IO/IT before service execution.

6 Location for Scope of Work Execution

Place of execution depends on the type of service requested and shall be agreed with IO/IT before service execution. The three activities can be performed either from ITER site or from a remote location (IO can provide virtual desktop infrastructure access to the Contractors).

7 IO Documents

No input is expected from IO unless requested by the Contractor.

8 List of deliverables and due dates

The framework contract will be set up for 5 years (3 firm years + 2 times one optional year) with task order(s) to be established according to the needs identified by IO IT.

The deliverables for each activity are described in detail in section 8.1.

8.1 Deliverables

The Contractor shall propose an on-site / off-site team to perform the tasks described in each Task Order.

IO IT provides in-house developed tools to record descriptions of work completed, to log time spent and to record absence. These tools are mandatory to use as they provide a basis for accounting and invoicing:

SERVICE

- Descriptions of work completed: Jira work logs and Confluence pages;
- Logging of time spent: Jira work logs weekly records;
- Records of absence: Confluence Team Calendars.

Monthly activity reports contain qualitative and quantitative detailed information about the issues the Contractor has been confronted to, about the solution proposed and implemented, the innovations introduced in the processes and the ideas to further improve the service. These reports shall be agreed and accepted from IO TRO to release the corresponding payment.

8.2 Acceptance of deliverables

- Coherence with requirements: does the Deliverable correspond to the specifications?
- Coherence with purpose: does the proposed Deliverable meet the objective and purpose?
- Completeness: does the Deliverable address all the required points?
- Level of detail: does the Deliverable address all points with the required level of detail appropriate?
- Consistency with the proposed architecture: the content of the Deliverable must be consistent with the principles of the basis of the system and the objectives requested;
- Formal aspects: Deliverables and their documentation shall be well written, understandable and exempt of language, drafting or typographical mistakes.

8.3 Performance Criteria

IO will evaluate and score the performance of the Contractor regarding Deliverables periodically (at least once a year). IO IT will focus on:

- Timeliness (max. 20 points): Did the Contractor produce Deliverables by the agreed deadline?
- Project execution (max. 20 points): Did the Contractor follow a clear and transparent management process for completion of the Deliverables?
- Quality and demonstrated competence (max. 60 points)

After evaluation, IO will provide a detailed report to the Contractor to give evidence of the performance of the service and eventually to allow the Contractor taking all the necessary measures to improve it, in particular:

- When the performance score is below 45 points, the Contractor will be required to apply urgent improvement measures. If nonetheless the Contractor’s performance remains unsatisfactory, ITER will apply measures that could lead to termination of the current task order or of the whole frame contract.
- If the performance score is not higher than 65 points, the Contractor will be required to apply improvement measures where necessary.
- A performance score of above 66 points will have a positive (above 85 very positive) impact on the decision whether to issue the next task order.

9 Safety requirements

9.1 Nuclear class Safety

No specific nuclear class safety requirements apply.

9.2 Seismic class

No specific safety requirement related to PIC and/or PIA and/or PE/NPE components apply.

10 Specific General Management requirements

Requirement for [Ref 1] GM3S section 6 applies completed/amended with the below specific requirements.

SERVICE

10.1 Specificities (Contract Gates/ Work Monitoring/ Meeting Schedule)

The ITER organization closes for one week around December 25. The Contractor shall include this week in the vacation planning for the on-site staff. Outside of the week of closure, the Contractor shall have at least 50% of its allocated team available, unless previously agreed by both parties to a different arrangement.

At any time of a task order lifecycle, when requested by the IO IT, the Contractor shall be able to provide the current number of the days when the services are provided by its team.

The Contractor obligation is to ensure the service continuity all along the task order validity. IO IT will monitor the quantity and quality of the services provided by the Contractor. Especially, IO IT reserves the right to register and log the time and presence of contractors on site.

The Contractor is required to work in close collaboration with all current and future IO Sub-contractors.

For the execution of services, the Contractor must deploy in reasonable time the Contractor's team with relevant profiles as proposed in the technical offer and agreed by IO IT.

The spoken and written language of all communications between the contractor and the IO is English. Therefore, the Contractor shall deliver all documentation deliverables, reports, drafts and other documents written in English, and conduct or participate in meetings using English language.

The Contractor's staff on-site and off-site shall follow IO IT internal processes using the IO IT tools for these activities:

- Periodic time and activity logging;
- Project management;
- Ticketing follow-up.

The work environment of the off-site team shall be in accordance with the complexity of the tasks in general, and offer especially:

- A strong internet connection at least 20Mb/s download and 5 Mb/s upload with ITER server (You can confirm your internet speed to ITER on this page: http://speedtest.iter.org);
- A workstation station with double screen of at least 22 inches diagonal and processor at least i7 or equivalent (4 core, 3GHz) and memory at least 16GB, 64bit OS, web cam and headset;
- Accessibility to meeting room equipped with white board and projector for 10 persons.

Background check

After the award, the Contractor shall provide certification to the IO that each employee assigned to this project has passed a criminal background check and has not been convicted of any crimes of theft, violence, destruction of property, telecommunications and electronics, fraud, against public administration, etc.

An employee of the Contractor who has been convicted of a crime shall not be permitted to work on this contract.

SERVICE

10.2 Contractor's Team

For each service requested by IO IT, the Contractor will provide detailed resume of the proposed team members to accomplish the task. IO IT will assess the adequacy of the team's skillset with the requested task.

The delivered services should be executed by team members having the proper knowledge of the IO/IT environment elements concerned by the requested service. Proper IT Security expertise shall be demonstrated by suitable experience and certifications (CISSP, OSCP, CEH, GPEN, CASP, GIAC GSEC, etc.).

The Contractor shall appoint a Project Manager (the Contractor Project Manager) who shall lead, manage and supervise the team. The IO shall not supervise the Contractor's team members.

SERVICE

Team members involved in the requested services shall demonstrate proper IT Security skills and demonstrated experience in similar environment. The following qualifications and experiences are expected by the IT Security specialists proposed to perform requested services.

Field of expertise	Indicative Applicable Experience			
	Junior (Lot1)	Confirmed (lot 1 & 2)	Senior (Lot 1 & 2)	Expert (Lot 1 & 2)
IT Security operations *Incident handling* *Management of security systems*	2 years total	5 years total	7 years total	10+ years total
Threat Intelligence *Red team activities, Malware analysis, Proactive defense mechanisms,*		Including 2 years	Including 3 years	
Management of security project *Architecture of security solutions, Project management* *Integration, Deployment, Documentation*		Including 2 years	Including 7 years	
IT Security Audit				4-8 years in one or more field of expertise
Awareness raising				
Risk assessment, Governance				
Recognised IT Security certification(s) e.g.: CISSP, OSCP, CEH, GPEN, CASP, GIAC GSEC, …	Preferred	Mandatory	Mandatory	Mandatory

This table is here to give an overview of our understanding of each profile experience. The missing professional experience can be compensated with extreme proficiency in expected scope. Please refer to the detailed definition of profiles for more information.

10.3 Definition of Roles

10.3.1 Junior profiles

Minimum Qualifications and experience (3 out of 4 required):

- First successful experience or project completion in IT Security, preferably in a SOC team;
- Ability to respond to security incidents, such as investigating security alerts and malicious emails, following the established procedures and protocols, and documenting and reporting the findings and actions taken;
- Be capable of integrating an IT Security solution. They should also be able to test and troubleshoot the solution, and provide support and maintenance when needed.

Knowledge and Skills (3 out of 5 required):

- Basic knowledge in programming (Powershell and/or Python);
- Knowledge in system administration (Active Directory and Microsoft Security);
- Understanding of networking and firewalls (F5 load balancer, Paloalto Firewall and Checkpoint firewall);
- Experienced in SIEM Management (ELK stack);
- Management of a vulnerability scanner (Tenable Nessus).

Examples:

- IT Security Analyst level 1 or 2;
- IT Security vulnerability assessor.

10.3.2 Confirmed profiles

Minimum Qualifications and experience (4 out of 7 required):

- 3-6 years of extensive professional experience in their specialised field;
- Show strong technical skills in using various security tools and technologies (SIEM, Hardening, IDS, etc.);
- Experience in participating in multi-disciplinary team;
- Proficient to respond to security incidents by performing advanced analysis, such as endpoint forensic or malware analysis. They should also be able to perform root cause analysis, and provide lessons learned and improvement actions;
- Be able to perform security assessments, audits, and tests, and provide recommendations and remediation plans.
- Be able to develop, update, and maintain IT security policies, guidelines, and procedures, and ensure compliance with IO requirements. They should also be able to monitor and measure the effectiveness of the security controls and processes, and report on the security status and risks.
- Research and stay updated on the latest IT security trends such as emerging threats, vulnerabilities, and attack techniques, as well as new security solutions and best practices.

Knowledge and Skills (3 out of 6 required):

- Experienced in SIEM Management (ELK stack);
- Knowledge in threat intelligence (MISP, Threat actors);
- Malware analysis and endpoint forensic analysis;
- Knowledge of wide variety of security solutions (IDS, Bastion, Sandbox, EDR);
- Comprehension of ISMS standard (ISO27K, NIST, NIS);
- Web application and internal penetration testing (OWASP and PTES).

Examples:

- IT Security Analyst level 3;
- Incident management Specialist;
- Penetration tester;
- Risk compliance specialist.

10.3.3 Senior profiles

Minimum Qualifications and experience (3 out of 4 required):

SERVICE

- 6-10 years of extensive professional experience in their specialised field;
- Experience in leading complex projects/programmes, involving multiple security functions, such as threat intelligence, vulnerability assessment, incident response, security monitoring, security governance, and security awareness;
- Responsible for leading a high performing team of professionals, including the ability to coordinate contributions of other specialists to complete a joint project. Experience in coaching and mentoring;
- Owner of IT Security certifications.

Knowledge and Skills (3 out of 5 required):

- Experienced in SIEM Management (ELK stack);
- Knowledge in SCADA security;
- Mastering IT Security standard (ISO27K, NIST, NIS);
- Experienced in Project Management (Prince2, Agile methodology);
- Experience implementing security solutions (IAM, Cloud Security, Hardening).

Job title examples:

- IT Security Architect;
- IT Security Manager.

10.3.4 Expert profiles

Minimum Qualifications and experience (4 out of 5 required):

- 10+ years of extensive professional experience in their specialised field;
- Strong theroretical knowledge and practical skills in IT Security, risk management and compliance with the ability to define and apply best practice principles;
- Owner of IT Security certifications;
- Evaluate the design and effectiveness of IT security controls, policies, and procedures, and identify gaps, weaknesses, and improvement opportunities;
- Communicate audit findings, recommendations, and action plans to management and relevant parties.

Knowledge and Skills (2 out of 4 required):

- Mastering IT Security standard (ISO27K, NIST, NIS);
- Experienced in risk assessment and management (EBIOS RM);
- Experienced in web application and internal penetration testing (OWASP and PTES);
- Experienced in SCADA security.

Examples:

- IT Security Auditor

10.4 CAD design requirements

This contract does not imply CAD activities.