ORGANISATION FOR JOINT ARMAMENT COOPERATION

VACANCY NOTICE

Post	A055 - INFORMATION SECURITY MANAGER
Grade	A3
Division	OCCAR-EA Directorate
Section	Security Office
Management of Staff	0
Location	Bonn, DE
Initial Contract Duration	3 years
Closing Date for Applications	07 August 2026
Start Date	01 November 2026
Interview Date	Week commencing on 07 September 2026

1. Background

The OCCAR-EA Security Office is responsible for maintaining the confidentiality of classified information by safeguarding it from espionage, compromise or unauthorised disclosure and by safeguarding installations housing Classified Information from sabotage and malicious wilful damage.

The Security Office is also responsible for ensuring the implementation of security procedures as prescribed in the OCCAR Security Regulations OMP (OCCAR Management Procedures) 11 and 12. It maintains continuous liaison with national and local Security Authorities on all security related matters.

The minimum standards for the handling and protection of classified information, including such information held on communication and information systems are defined in the OCCAR Security Regulations.

OCCAR-EA has furthermore established an integrated business framework covering Information, Risk Management, Quality Management and Information Security Management.

2. Duties and Responsibilities

The Information Security Manager (ISM) is responsible for the development and ongoing review of OCCAR Communication and Information Systems (CIS) Security policies and processes; accreditation of ICT systems, supporting the Information Division in the identification, mitigation, mediation and management of CIS Security risks and vulnerabilities associated with OCCAR-EA CIS; providing advice to OCCAR-EA leadership regarding CIS security issues and topics; and support OCCAR Programmes directly in the same field of expertise. The main focus of the ISM is on the protection of classified information.

The ISM works closely the with the Information Division and the ICT Security Support Engineer in particular, in the definition and execution of appropriate accreditation and Information Security-related risk management strategies for OCCAR-EA CIS, taking particular responsibility for the coordination of any personnel, physical and procedural security measures necessary to counter related threats to information and systems associated with aspects by identified through structured risk management methodology and processes.

In particular, they will:

- Develop and maintain Information Security policies and respective procedures to manage CIS Security risks accordingly;
- Advise Central Office and Programme Divisions regarding Information Security related policy, and support them if Information Security risk-related issues that may arise;
- Support the Information Division in the identification and mitigation of CIS Security risks within or relating to OCCAR-EA systems, and connection to external parties and systems;
- Coordinate Information Security and CIS Security related issues involving third parties;
- Being in lead of the accreditation and continuous re-accreditation of OCCAR-EA CIS systems;

- Coordinate the security monitoring of OCCAR CIS to detect Information Security and cyber threats;
- Investigate CIS Security violations and incidents within OCCAR-EA and support Security Section Leader (SSL) in reporting and impact analysis;
- Management of ICT security incidents within OCCAR and support to Programme, Participating Nations and Industry on OCCAR ICT security matters;
- Support SSL in conducting Information Security training and education of OCCAR personnel;
- Conduct regular phishing-simulation campaigns as well as needs-oriented training to increase the security awareness of OCCAR staff;
- Leading the Expert Working Group of national CIS Security Experts as established by the Security Committee and Future Tasks and Policy Committee;
- Liaise with national CIS Security Authority or other International Organisations in the same field of expertise.

Related to these activities, the ISM will report to the SSL, who is reporting to the Deputy Director while keeping a functional line to the Director of OCCAR-EA in urgent information security matters.

3. Key competences and skills required for the grade

(You must provide evidence of meeting these key competences and skills in your Application, Section 12).

CS 1 The ability to establish and maintain excellent working relationships at all levels in a multicultural context and with respect for diversity;

CS 2 Excellent interpersonal and team working skills with the ability to interact and communicate at all levels within OCCAR as well as with Nations;

CS 3 The ability to work in a changing, developing and demanding environment;

CS 4 The ability to implement clear, efficient and logical approaches to work, to manage assignments, objectives and time;

CS 5 The ability to use Computer and Information Technology (ICT) facilities and be able to demonstrate a good working knowledge of MS Office software.

4. Specialist knowledge and experience required for the post

(You must provide evidence of meeting these specialist requirements in your Application, Sections 10 and 11).

4.1 Essential:

ES 1 Sound knowledge of, and recent experience in, actively leading or significantly contributing to the development and implementation of policies and procedures relating to Information, CIS and Cyber Security within a national or an international organisation;

ES 2 Sound knowledge of, and recent experience in, performing CIS Security risk management tasks in complex, inter-networked CIS environments, including demonstrating the ability to analyse and assess CIS security-related issues;

ES 3 Sound knowledge of, and practical experience in, planning or leading the accreditation of classified complex inter-networked CIS infrastructure with a comprehensive understanding of the physical, personnel, technical and procedural security aspects;

ES 4 Sound knowledge of relevant security policies and procedures governing the protection of classified information of one or more OCCAR Member States as well as of international organisations such as NATO or the EU;

ES 5 Sound knowledge of, and practical experience with, modern cryptographic principles and technologies, including symmetric and asymmetric encryption, key-management practices, digital signatures and secure communication protocols and their application in securing complex inter-networked CIS environments.

4.2 Desirable:

DS 1 Training, certifications or practical experience related Information Security Management System (ISMS) preferably in accordance with ISO/IEC 27001 or a comparable international standard;

DS 2 Experience in direct collaboration with national CIS Security Authorities, including those of foreign nations;

DS 3 Experience working with government-approved cryptographic systems and Public Key Infrastructure (PKI) solutions;

DS 4 Experience with security incident management processes and tools, including participation in incident response activities, investigations or coordination with national/international Computer Emergency Response Teams (CERTs/CSIRTs).

5. Language Requirements

- ADVANCED level[1] of ENGLISH both oral and written.
- Additional knowledge of another OCCAR Member or Participating State's language will be considered as an asset.

6. Qualifications

A university-level education (or equivalent qualification) along with long-standing experience in the activities directly related to the tasks described is highly desirable.

7. Security Clearance

Security clearance at OCCAR Secret level is required for this post - or needs to be obtained within the first 6 months of employment.

8. Applications and Points of Contact

For further information regarding this Post, please contact:

Email: application@occar.int

OCCAR Privacy Statement:

When applying for an OCCAR vacancy, it is necessary for OCCAR to collect and process personal data about you in order to assess and evaluate your suitability for the vacancy, and (if successful) to coordinate with relevant service providers in preparation of your appointment. For further information please visit our web-site: OCCAR Privacy Statement - http://www.occar.int/privacy-data-protection.

[1] The language levels can be found on the OCCAR website, www.occar.int Careers / Applying.