Organisation for Joint Armament Co-operation
Executive Administration

VACANCY NOTICE

Post	A055 – Information Security Manager
Grade	A3
Division	Corporate Support Division
Section	Security
Management of Staff	0
Location	Bonn, Germany
Initial Contract Duration	3 years
Closing Date for Applications	16/07/2020
Start Date	01/10/2020
Interview Date	04/08/2020

1. Background

The OCCAR-EA Security Section is part of the Corporate Support Division (CSD), which is responsible for the provision of essential infrastructure and support to enable the execution units, i.e. the Programme Divisions and Central Office, to carry out efficiently and effectively the core activity of OCCAR-EA. Beside Security, this includes all matters relating to Information and Communication Technology (ICT) and Site Management in each of the OCCAR-EA sites.

OCCAR is entrusted with the management of various programmes concerning complex equipment of high military-strategic significance. OCCAR-EA handles a considerable amount of classified and unclassified information being subject to distribution limitations. Information could be generated by OCCAR-EA or is received from different OCCAR-EA stakeholders like OCCAR Member States, other states participating in an OCCAR Programme, contractors and other cooperation partners such as NATO or EU institutions.

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 Management Procedures, Internal Procedures or Programme Security Instructions.

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

2. Duties and Responsibilities

The Information Security Manager (ISMR) is responsible for the development and ongoing review of OCCAR CIS Security policies and processes; accreditation of ICT systems, supporting the ICT section in the identification, mitigation, mediation and management of CIS Security risks and vulnerabilities associated with OCCAR-EA communication and information systems (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 ISMR works closely the with the ICT section 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 he/she 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 ICT Section 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;
- Support SSL in conducting Information Security training and education of OCCAR personnel;
- 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 ISMR will report to the SSL, who is reporting to the Head of the CSD 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 relations 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 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, Section 11).

4.1 Essential:

ES 1 Sound knowledge of and recent experience with actively leading or significantly contributing to the development and implementation of policies and procedures relating to Information, CIS and Cyber Security for an international organisation such as NATO, EU or others;

ES 2 Sound knowledge of and recent experience of actively performing CIS Security risk management tasks in the context of complex inter-networked CIS; demonstrating the ability to analyse CIS security-related matters; propose solution-centric options for control, drive the implementation of controls, and evaluate their ongoing effectiveness;

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

ES 4 Sound and recent practical knowledge of and experience in establishing and using technical security tools such as log analysis and correlation, to identify and investigate potentially unusual behaviour within complex CIS;

ES 5 Sound knowledge of relevant security policies and procedures for the protection of classified information of one or more OCCAR Member States and of international organisations such as NATO or EU.

4.2 Desirable:

DS 1 CISSP or similar certification(s); continuous participation on respective CIS Security trainings or courses; and experience with implementing ISO 27001;

DS 2 Experience in ICT security auditing and penetration testing;

DS 3 Sound knowledge of and practical experience with Microsoft and CISCO based CIS infrastructure, VEEAM , Vmware vCenter, and IT security tools in particular with McAfee and SPLUNK;

DS 4 Experience in direct collaboration with national CIS Security Authorities of foreign nations;

DS 5 Experience with government approved cryptographic systems and PKI infrastructure.

5. Language Requirements

- Fluency, oral and written, in the English language.
- Adequate knowledge of at least one other OCCAR language would be an asset.

*** The language levels can be found on the OCCAR website, www.occar.int Human Resources / vacancies.**

6. Qualifications

A university-level education (or equivalent relevant experience) 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.

8. Applications and Points of Contact

For further information regarding this Post, please contact:

Geert VANLINTHOUT (Head of Corporate Support Division)

Email: geert.vanlinthout@occar.int

Applications for this Vacancy Notice should be submitted through the appropriate National Administrations.

Applicants who are **not** Ministry of Defence staff wishing to apply for this Post should email the completed application and supporting documentation to B009@occar.int and B010@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.