# JOB DESCRIPTION

| **Post Details:** | | | |
|---|---|---|---|
| Post Title: | **Head, Air Operations Branch** | Organisational Element: | CSU Ramstein |
| Military/Civilian: | CIV | Location: | Ramstein, Germany |

**Organisation context:**

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCIA delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

The Directorate of CIS Support Units (DCSU) is responsible to manage, deliver and maintain assigned Communications and Information System (CIS) products and services for the Agency's customers including NATO Headquarters (NHQ), the NATO Command Structure (NCS), NATO Force Structure (NFS), Nations and internal Agency users. DCSU provides liaison, planning and coordinating functions for Alliance Missions, Operations and Exercises. Services are delivered in coordination with the Enterprise Service Operations Centre (ESOC) and Agency Business Areas/Service Centres under the Enterprise Service Delivery Model (ESDM).

NCIA CIS Support Unit (CSU) Ramstein, located in Ramstein, DEU, is responsible to manage, deliver and maintain assigned Communication and Information Systems (CIS) products and services for the Agency's customers during peacetime, crisis and war throughout its assigned AoR and as otherwise directed. As the local service provider and Service Management Authority (SMA), it supports the NCIA in delivering secure, reliable end-to-end services under the Enterprise Service Delivery Model (ESDM).

**Organisational Element Statement of Functions:**

NCIA CIS Support Unit (CSU) Ramstein, located in Ramstein Germany enables end-to-end CIS services as it installs, operates, maintains and supports the full range of CIS capabilities during peacetime, crisis and war throughout its allocated Area of Responsibility (AOR) and as otherwise directed.

Under the direction of the Head, Air Operations Branch (AOB), the AOB is responsible for the provision of local CIS products and services as required in applicable service agreements. The AOB is responsible to deliver level one and two CIS support to catalogue services as specified in the ESDM under the direction of Agency Service Centres and/or the Enterprise Service Operations Centre (ESOC). The AOB is also responsible to deliver levels one to three CIS support to applicable non-catalogue services as defined in the relevant service agreement(s). The AOB is consulted in relation to the continual improvement programme by reporting on key performance indicators in close coordination with the Service Level Management section.

The AOB is locally responsible for the installation, operation, maintenance and administration of assigned

Information and Communication Technology (ICT) hardware and software. The AOB is responsible, on behalf of the CSU Commander, for the secure operation of all assigned CIS/ICT as directed by the NATO Cyber Security Centre (NCSC). The AOB is accountable for local actions as part of Agency incident management and service request management processes in coordination with the ESOC and Service Management Branch (SMB) and deployment management in coordination with Service Management and Control (SMC) and the SMB. The AOB is consulted in relation to problem management, release management, event management, service validation and testing, configuration and change management, in support of the responsible Agency Service Centre or the SMB.

The AOB comprises the following organizational elements: AOB is constituted of the following functional elements: AirC2 Services Support Section (ASSS), Missile & Space Services Section (MSSS) and Air and Missile Shift (24/7) Support Section (AMSSS)

**Job role description:**

The Head, Air Operations Branch (AOB) is responsible for the leadership and management of all CSU operational support functions for Air-specific Services. This includes overseeing local IT support activities such as Air Command & Control (AirC2), Missile Defence System of Systems (MDSS) and Community of Interests software for Static entities, operations and exercises. The Head of AOB ensures operational continuity across these domains, including 24/7 support readiness, incident response coordination and technical problem resolution.

They supervise a multidisciplinary technical team, manage shift-based service delivery, and coordinate the integration of contractor support to ensure alignment with CSU standards and operational goals. The Head of AOB plays a key role in maintaining the CSU’s cyber defence posture, supporting infrastructure integrity, and ensuring technical compliance with Agency policies and service expectations.

In addition to branch leadership, the Head of AOB contributes to CSU-wide planning and strategic coordination. They collaborate closely with the other branch heads and support CSU governance processes, ensuring that local technical operations support both business-as-usual activities and urgent or crisis-driven demands.

**Duties and Responsibilities:**

**Strategic planning**

- Develops, communicates, implements and reviews the processes which embed strategic management in the operational management of the organisation.
- Leads and manages the creation or review of a strategy that meets the requirements of the business.
- Sets policies, standards, and guidelines for how the organisation conducts strategy development and planning.

**Specialist advice**

- Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations.
- Actively maintains knowledge in one or more identifiable specialisms.
- Recognises and identifies the boundaries of their own specialist knowledge.
- Where appropriate, collaborates with other specialists to ensure advice given is appropriate to the organisation's needs.

**Performance management**

- Forms, maintains and leads workgroups and individuals to achieve organisational objectives.
- Determines and delegates objectives and task responsibilities to individuals or teams — including people management responsibilities as appropriate.
- Sets the quality, performance and capability targets in line with organisational goals.
- Monitors performance and working relationships and provides effective feedback to address individual issues.
- Encourages individual development of skills and capabilities in line with team and personal goals.
- Facilitates the development of individuals by adjusting workload, targets, and team capacity.
- Plays an active role in formal organisational processes such recruitment, reward, promotion and disciplinary procedures.

**Organisational facilitation**

- Facilitates workgroups to deliver defined goals and outcomes.
- Provides support, guidance and suggestions to workgroups and teams to learn collaborative problem solving and improve their team performance.
- Creates shared responsibilities and sustainable agreements with the team.
- Implements and improves agreed team principles, practices, processes & ceremonies.
- Recognises and works with the strengths and constraints of team dynamics.

**Resourcing**

- Plans and manages the acquisition and deployment of resources to meet specific needs and ongoing demand.
- Defines and manages the implementation of resourcing processes and tools.
- Advises on available options and customises resourcing approach to meet requirements.
- Adheres to standards, statutory or external regulations and codes of practice and ensures compliance.
- Engages with external parties in support of resourcing plans.
- Measures effectiveness of resourcing processes and implements improvements.

**Stakeholder relationship management**

- Identifies the communications and relationship needs of stakeholder groups.
- Translates communications/stakeholder engagement strategies into specific activities and deliverables.
- Facilitates open communication and discussion between stakeholders.
- Acts as a single point of contact by developing, maintaining and working to stakeholder engagement strategies and plans.
- Provides informed feedback to assess and promote understanding.
- Facilitates business decision-making processes.
- Captures and disseminates technical and business information.

**Financial Risk Management**

- Updates and implements improvements to risk assessment and management methods.
- Evaluates the benefits and drawbacks of alternative risk management approaches.
- Recommends risk assessment procedures and techniques based on organizational need.
- Consults on a variety of risk assessment approaches and applications.
- Evaluates, recommends, and justifies optimum risk management scenarios.
- Advises others on a variety of risk and reward factors and their relationships.

**HR: Policies, Standards and Procedures**

- Evaluates the impact of standards and policies across functional specialties.
- Collaborates with other functions in establishing and documenting joint standards.
- Manages change and helps organization adjust to unforeseen HR issues that arise.
- Monitors organizational compliance of HR policies, standards and procedures.
- Directs the development of organizational policies and practices.
- Advises on existing and evolving standards and procedures and their impact on HR operations.

**Additional duties for this post:**

- Leads and manages CSU's Air Operations Branch (AOB), overseeing local IT support functions including Air Command & Control (AirC2), Missile Defence System of Systems (MDSS) and Community of Interests services for static entities, operations and exercises.
- Ensures operational continuity within CSU Geographical Area of Responsibility (GAoR) through 24/7 service readiness, shift planning, and structured incident response mechanisms.
- Maintains CSU's cyber defence posture in alignment with Agency security standards, coordinating with enterprise-level cybersecurity stakeholders.
- Manages integration and supervision of external contractor support to ensure alignment with CSU operational procedures and service quality expectations.
- Coordinates the resolution of technical problems and leads root cause analysis efforts to drive service reliability and operational improvement.
- Participates in CSU-wide strategic planning and governance activities, ensuring that service operations are aligned with CSU priorities and Agency mandates.
- Supports surge capacity planning, emergency operations, and high-impact technical response efforts as needed.
- Provides status and reports as required, and ensures that relevant Key Performance Indicators (KPI's) are reported regularly to appropriate Business Areas/Service Centres and SMB.
- Liaises with external technology partners, vendors and local suppliers when required.
- Accountable for the annual training schedule for AOB and its execution in an effective and efficient manner.
- Assists in establishing annual demand forecasts and annual operational budgets for the CSU.
- Collaborates closely with the Heads of SMB and Enabling Services Branch (ESB) to ensure unified CSU service execution and branch coordination.
- Interprets complex technical issues and presents them concisely in briefings to management.
- Represents the CSU in various NATO Committees, Steering Groups/Boards and Conferences with authority to commit CSU resources.
- Contributes to the Service Level Management process and ensures coherence between agreed and delivered services; provides relevant input to SLAs, OLAs, Underpinning Agreements (UA) and other agreements.
- Participates in the recruitment and selection of CSU staff.
- Deputises for CSU Commander, if required.
- Performs other duties as may be required.

**Education, Experience and Training (essential):**

**Education:**

- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 3 years post-related experience.
- Or exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to NCIA, that is, at least 10 years extensive and progressive expertise in duties related to the function of the post.

**Experience:**

- The incumbent must have a minimum of three years of CIS engineering experience and 3 years of experience in the management of CIS systems either as a Project Manager or Service Operations Manager;
- Experience leading multi-disciplinary technical teams in areas such as desktop support, telecom, network, or cybersecurity.
- Possess demonstrable leadership characteristics and extensive experience in leading teams of CIS professionals under challenging circumstances and in complex environments.
- Knowledge and experience in the preparation and implementation of new or changed services.
- Knowledge in the management of performance of systems and services.
- Knowledge and experience of requirements' identification, and their analysis and validation.
- Demonstrated experience in service continuity, incident response, and infrastructure support.
- Proven ability to manage shift-based or 24/7 operations and on-call support.
- Experience coordinating internal teams and contractor-delivered services.
- Experience contributing to risk management, operational planning, and technical governance.
- Knowledge of cybersecurity best practices and service operations frameworks.

**Training/Certifications:**

- Certification in a formal Project Management methodology (PRINCE2, PMP, PMBOK etc.).
- ITIL V3 or ITIL 4 Intermediate Qualification within Service Transition, Service Operation and Continual Service Improvement (CSI).

**Education, Experience and Training (desirable):**

**Experience:**

- Working knowledge of NATO political and organizational structure.
- Experience in geographically distributed IT operations or support environments.
- Experience managing crisis response and post-incident improvement initiatives.
- Experience contributing to or leading technical audits, business continuity testing, or cyber defence exercises.
- Knowledge and experience about the operation and control of IT infrastructure (typically hardware, software, data stored on various media, and all equipment within Wide and Local Area Networks) required to deliver and support IT services and products to meet business needs.
- Knowledge of the maintenance of regulatory, legal and professional standards.
- Knowledge about building and management of systems and components in virtualized computing

environments, including their security and their sustainability.

- Prior experience of working in an international environment comprising both military and civilian elements. Demonstrable evidence in maintaining knowledge of advances in Information Technology.

**Training/Certifications:**

- Formal Management Qualification such as the NCIA is Leadership Programmes, or the NATO-wide Executive Development Programme (NEDP).
- Advanced ITIL certification (e.g., ITIL Managing Professional or equivalent).
- Certification in cybersecurity (e.g., CISSP, CISM).
- NATO Resource Management Education Programme (RMEP).
- Formal training in risk management or operational resilience.

**Behavioral competencies:**

- Deciding and Initiating Action - Takes responsibility for actions, projects and people; takes initiative and works under own direction; initiates and generates activity and introduces changes into work processes; makes quick, clear decisions which may include tough choices or considered risks.
- Adhering to Principles and Values - Upholds ethics and values; demonstrates integrity; promotes and defends equal opportunities, builds diverse teams; encourages organisational and individual responsibility towards the community and the environment.
- Leading and Managing - Provides others with a clear direction; motivates and empowers others; attracts and develops staff of a high calibre; provides staff with development opportunities and coaching; sets appropriate standards of behaviour.
- Achieving Personal Work Goals and Objectives - Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities.

| | |
|---|---|
| **Language:** | A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.<br>**NOTE:** Most of the work of the NCIA is conducted in the English language. |