NATO
NORTH ATLANTIC TREATY ORGANIZATION
INTERNATIONAL STAFF

OTAN
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
SECRÉTARIAT INTERNATIONAL

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

Officer, Accreditation Support – 261179

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 06-Sep-2026
Salary (Pay Basis): 8,273.12 (EUR) Monthly
Grade NATO Grade G17
Clearance Level CTS

Description

1. SUMMARY

The Cyber and Digital Transformation Division (CDT) oversees all aspects of cyber and digital transformation across the NATO Enterprise, advancing the Alliance's agenda in these areas. As a fully integrated civilian-military Division, CDT combines the strategic insight of the International Staff (IS) with the operational expertise of the International Military Staff (IMS), enabling coherent, credible, and actionable advice to NATO's senior decision-making bodies.

Within the Cyber Operations Section (CYOP), the Officer, Accreditation Support is responsible for tracking the accreditation backlog and monitoring the status of unaccredited systems across the NATO Enterprise. The incumbent contributes to the security accreditation process for traditional and cloud-based CIS solutions by coordinating and prioritising Security Audits (Type 3 and 4), applying a risk-based approach to prioritisation, performing gap analysis, and supporting remediation planning in accordance with NATO risk management frameworks. The incumbent also provides strategic advisory support to senior stakeholders, contributing to decision-making related to enterprise cybersecurity posture, accreditation readiness, and risk acceptance.

2. QUALIFICATIONS AND EXPERIENCE

The incumbent must:

- possess a university degree relevant to the position;

- have at least 5 years of experience in the cyber operations field, including experience in leading remote teams effectively;
- demonstrate strong experience in cybersecurity risk assessment, compliance frameworks (ISO 27001, NIST, GDPR), and security accreditation processes for both traditional and cloud-based solutions, including the aspects to be addressed during cybersecurity inspections;
- have experience designing, implementing, and improving cybersecurity governance programmes, including ISMS, audit readiness, and enterprise security controls within traditional and cloud-based CIS capabilities and services;
- have the following minimum levels in NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other.

The following are considered an advantage:

- professional certifications relevant to the position, such as: security certifications (CISSP, CCSP, CISM, etc), audit certifications based on international standards (ISO 27001 Lead Auditor, etc.), project management and IT service management certifications (PRINCE2, ITIL v4, etc.);
- experience providing executive-level reporting and cybersecurity briefings, and coordinating multi-stakeholder environments across large organisations; and
- experience developing, executing, coordinating, and improving accreditation processes for a large organisation.

3. MAIN ACCOUNTABILITIES

Policy Development: Contribute to the development of policies, directives, and guidance documents related to enterprise security accreditation. Advise the section head on NATO Enterprise security accreditation processes and procedures. Support and contribute to policy changes related to CIS security and its management, in coordination with the Security Accreditation Authority (SAA) and the Communication and Information Systems Provider (CISP). Assess and verify risks, and develop proposals to strengthen existing CIS security policies related to accreditation at the enterprise level. Develop high-level strategic documents and advice to enhance enterprise security accreditation and support interoperability within the Alliance.

Project Management: Participate in project management boards as required, contributing to accreditation and cybersecurity risk perspectives. Maintain and contribute to enterprise-level cybersecurity programme execution within assigned responsibilities. Identify, monitor, and proactively mitigate cybersecurity and accreditation-related risks across programmes; provide expertise and leadership to resolve exceptions and issues. Coordinate and lead accreditation and risk management activities, including remediation planning and prioritisation based on business impact, across traditional and cloud-based CIS solutions for classified and unclassified capabilities and services. Coordinate and develop mitigation and remediation actions with other members of the Cyber Operations Section to ensure a coherent and consistent approach.

Stakeholder Management: Establish and maintain a network of key experts across the NATO Enterprise, with a specific focus on enterprise-wide security accreditation. Develop close cooperation with the NATO operational community across the lifecycle of enterprise

security processes and practices, with emphasis on accreditation management. Provide advisory support to senior leadership on enterprise cybersecurity risk posture, accreditation readiness, and accreditation-related decisions.

Knowledge Management: Draft background briefs, progress reports, presentations, and other materials for high-level meetings. Track accreditation status and support enterprise situational awareness by contributing relevant information to appropriate NATO bodies and boards (e.g., CyOC, CRMG, BCISOAs). Based on briefings, discussions, and security accreditation outcomes, provide advice on evolving security programmes across NATO nations, NATO civilian and military bodies, and non-NATO entities. Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

Reporting Line: Reports to the Team Lead, Cybersecurity Risk Management.

Interactions: Interacts with staff across the NATO Enterprise and works in close cooperation with CDT staff.

Direct Reports: N/A

Indirect Reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking: sees multiple relationships.
- Flexibility: adapts to unforeseen situations.
- Impact and Influence: takes multiple actions to persuade.
- Initiative: is decisive in a time-sensitive situation.
- Organizational Awareness: understands organisational climate and culture.
- Teamwork: cooperates.

6. CONTRACT

Contract to be offered to the successful applicant (if non-seconded): Definite duration contract of three years; possibility of renewal for up to three years, during which the incumbent may apply for conversion to an indefinite duration contract.

Contract clause applicable:
In accordance with the contract policy, this is a post in which turnover is desirable for political reasons in order to be able to accommodate the Organisation's need to carry out its tasks as mandated by the Nations in a changing environment, for example by maintaining the

flexibility necessary to shape the Organisation's skills profile, and to ensure appropriate international diversity.
The maximum period of service foreseen in this post is 6 years. The successful applicant will be offered a 3-year definite duration contract, which may be renewed for a further period of up to 3 years. However, according to the procedure described in the contract policy the incumbent may apply for conversion to an indefinite contract during the period of renewal and no later than one year before the end of contract.
If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period of up to 3 years subject also to the agreement of the national authority concerned. The maximum period of service in the post as a seconded staff member is six years.
Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Régulations.

7. USEFUL INFORMATION REGARDING APPLICATION AND RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries. Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (link);
- For all other applications: www.nato.int/recruitment

Before you apply to any position, we encourage you to click here and watch our video providing 6 tips to prepare you for your application and recruitment process.

Do you have questions on the application process in the system and not sure how to proceed? Click here for a video containing the information you need to successfully submit your application on time.

When submitting your application, please ensure that your Taleo Candidate Profile is updated and that your CV is correctly uploaded in the Taleo attachments section.

More information about the recruitment process and conditions of employment, can be found at our website (http://www.nato.int/cps/en/natolive/recruit-hq-e.htm)
Appointment will be subject to receipt of a **security clearance** (provided by the national Authorities of the selected candidate), approval of the candidate's **medical file** by the NATO Medical Adviser, verification of your study(ies) and work experience, and the successful completion of the **accreditation** and notification process by the relevant authorities.

NATO will not accept any phase of the recruitment and selection prepared, in whole or in part, by means of reference documents without proper quotes (plagiarism), or any tools available on internet, including but not limited to translation facilities, or generative artificial-intelligence (AI) tools. NATO reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such tools will be rejected without further consideration, and NATO reserves the right to take further steps in such cases as appropriate.

8. ADDITIONAL INFORMATION

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations, and strongly encourages women to apply.

NATO is committed to fostering an inclusive and accessible working environment, where all candidates living with disabilities can fully participate in the recruitment and selection process. If you require reasonable accommodation, please inform us during your selection process.

Candidates will be required to provide documented medical evidence to support their request for accommodation.

Building Integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

Due to the broad interest in NATO and the large number of potential candidates, telephone or e-mail enquiries cannot be dealt with.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

The nature of this position may require the staff member at times to be called upon to travel for work and/or to work outside normal office hours.

The organization offers several work-life policies including Teleworking and Flexible Working arrangements (Flexitime) subject to business requirements.

Please note that the International Staff at NATO Headquarters in Brussels, Belgium is a non-smoking environment.

For information about the NATO Single Salary Scale (Grading, Allowances, etc.) please visit our website. Detailed data is available under the Salary and Benefits tab.

NATO does not charge any application, processing, training, interviewing, testing or other fee in connection with the application or recruitment process. For more info please click here.

Administratrice/Administrateur (soutien homologation) - 261179

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 06-sep-2026
Salaire (Base de paie) : 8,273.12 Euro (EUR) Mensuelle
Grade NATO Grade G17
Niveau de l'habilitation de sécurité CTS

Description :

1. RÉSUMÉ

La Division Cyber et transformation numérique (CDT) supervise toutes les questions relatives au cyber et à la transformation numérique au sein de l'entreprise OTAN et fait avancer les travaux de l'Alliance sur ces dossiers. En tant qu'entité civilo-militaire pleinement intégrée, elle combine l'acuité stratégique du Secrétariat international (SI) et l'expertise opérationnelle de l'État-major militaire international (EMI), ce qui lui permet de formuler des avis cohérents, crédibles et exploitables à l'intention des organes décisionnels de haut niveau de l'OTAN.

Au sein de la Section Opérations cyber (CYOP), la personne titulaire du poste assure le suivi des dossiers d'homologation en souffrance et de l'état de conformité des systèmes non homologués en usage au sein de l'entreprise OTAN. Elle contribue aux processus d'homologation de sécurité des solutions SIC traditionnelles ou faisant appel au cloud en coordonnant les audits de sécurité (de type 3 ou 4) et en définissant leur degré de priorité sur la base d'une approche fondée sur les risques, en analysant les insuffisances et en aidant à planifier la mise en œuvre de mesures de remédiation sur la base des cadres OTAN relatifs à la gestion des risques. La personne titulaire du poste offre aussi un soutien consultatif de niveau stratégique aux hauts responsables et contribue ainsi aux processus de prise de décision concernant la posture de cybersécurité de l'entreprise OTAN, la préparation du processus d'homologation et l'acceptation du risque.

2. QUALIFICATIONS ET EXPÉRIENCE

La personne titulaire du poste doit :

- posséder un diplôme universitaire dans un domaine pertinent pour le poste ;
- avoir au moins cinq ans d'expérience dans le domaine des opérations cyber et notamment une expérience probante de l'encadrement d'équipes à distance ;
- avoir une solide expérience de l'évaluation des risques cyber, des cadres de conformité applicables (ISO 27001, cadre du NIST, RGPD) et des processus d'homologation de sécurité à suivre pour les solutions traditionnelles et pour les solutions cloud, ainsi que des aspects sur lesquels doivent porter les inspections de cybersécurité ;
- avoir une expérience de la conception, de la mise en œuvre et du perfectionnement de programmes et instruments de gouvernance pour la cybersécurité (système de

management de la sécurité de l'information (SMSI), préparation à l'audit, contrôles de sécurité internes applicables aux capacités et services SIC faisant appel à des solutions traditionnelles ou à des solutions cloud) ;
- avoir au minimum les niveaux de compétence ci-après dans les langues officielles de l'OTAN (anglais/français) : V (« avancé ») dans l'une ; I (« débutant ») dans l'autre.

Seraient considérés comme autant d'atouts :

- le fait d'avoir obtenu des certifications professionnelles dans des domaines pertinents pour le poste, par exemple : certifications de sécurité (CISSP, CCSP, CISM, etc.) ; certifications dans le domaine de l'audit répondant à des normes internationales (Auditeur principal ISO 27001, etc.) ; certifications en gestion de projet et en gestion de services informatiques (PRINCE2, ITIL v4, etc.) ;
- une expérience de l'établissement de rapports à l'usage des parties prenantes au niveau exécutif et de la présentation d'exposés de cybersécurité ;
- une expérience de l'élaboration, de l'exécution, de la coordination et du perfectionnement de processus d'homologation au sein d'une grande organisation.

3. RESPONSABILITÉS PRINCIPALES

Élaboration des politiques – Contribue à l'élaboration des politiques, des directives et des documents d'orientation relatifs aux processus d'homologation de sécurité de l'entreprise OTAN. Rend des avis à la/au chef de la Section en ce qui concerne les processus et procédures d'homologation de sécurité. Accompagne et alimente l'évolution des politiques relatives à la sécurité des SIC et à sa gestion, en concertation avec l'autorité d'homologation de sécurité (SAA) et le prestataire de services SIC (CISP). Fait un travail d'évaluation des risques et de vérification et propose des moyens de renforcer les politiques relatives à la sécurité des SIC dans leurs aspects ayant trait aux processus d'homologation au niveau de l'entreprise OTAN. Établit des documents stratégiques de haut niveau et remet des avis en vue d'améliorer les processus d'homologation de sécurité et de renforcer l'interopérabilité au sein de l'Alliance.

Gestion de projet – Contribue aux travaux des comités de gestion des projets, s'il y a lieu, en proposant un éclairage sous l'angle de l'homologation et des risques de cybersécurité. Soutient l'exécution des programmes liés à cybersécurité menés à l'échelle de l'entreprise et y contribue, dans le périmètre de ses responsabilités. Repère, suit et atténue activement les risques liés à la cybersécurité et à l'homologation des systèmes qui pourraient peser sur les programmes ; met son expertise et sa capacité d'impulsion à profit pour résoudre des problèmes ou traiter des cas particuliers. Coordonne et dirige les activités liées à l'homologation et à la gestion des risques, en s'occupant en particulier de planifier la mise en œuvre des mesures de remédiation et de hiérarchiser les priorités au regard de l'impact potentiel de tel ou tel élément sur les activités, et ce pour l'ensemble des solutions SIC traditionnelles ou solutions cloud sur lesquelles reposent les services et capacités classifiés et non classifiés. Travaille en concertation avec d'autres membres de la Section Opérations cyber, notamment aux fins de l'élaboration de mesures d'atténuation et de mesures correctives, de manière à assurer la cohérence et l'homogénéité de l'approche d'ensemble.

Gestion des parties prenantes – Établit et entretient un réseau d'experts OTAN disposant de compétences clés, notamment en ce qui concerne les processus d'homologation de

sécurité à l'échelle de l'entreprise OTAN. Travaille en coopération étroite avec les parties OTAN intervenant au niveau opérationnel à toutes les étapes des processus et pratiques de sécurité de l'entreprise, en se concentrant en particulier sur la gestion des homologations. Formule des avis à l'usage des hauts responsables sur la posture de cybersécurité de l'entreprise OTAN, sur la préparation du processus d'homologation et sur l'acceptation du risque.

Gestion des connaissances – Rédige des notes d'information et des rapports d'activité et prépare des présentations et d'autres documents pour des réunions de haut niveau. Suit l'état de l'homologation des systèmes et aide à dégager une vue d'ensemble de la situation à l'échelle de l'entreprise OTAN en communiquant les informations pertinentes aux organes et comités compétents (Centre des cyberopérations, Groupe de gestion du risque cyber, Comité des autorités opérationnelles des SIC, etc.). Sur la base d'exposés, de débats et des résultats de processus d'homologation de sécurité passés, formule des avis sur l'évolution des programmes de sécurité dans les pays membres et les organismes civils et militaires de l'OTAN ainsi que dans des entités non OTAN. S'acquitte de toute autre tâche en rapport avec ses fonctions qui pourrait lui être confiée.

4. STRUCTURE ET LIAISONS

Hiérarchie – La personne titulaire du poste relève de la/du chef de l'équipe Gestion des risques de cybersécurité.

Relations de travail – Elle entretient des contacts avec des membres du personnel de toute l'entreprise OTAN et travaille en coopération étroite avec les agents de la Division CDT.

Nombre de subordonné(e)s direct(e)s : sans objet.

Nombre de subordonné(e)s indirect(e)s : sans objet.

5. COMPÉTENCES

La personne titulaire du poste doit faire preuve des compétences suivantes :

- Réflexion analytique : discerne les relations multiples.
- Flexibilité : s'adapte à des situations imprévues.
- Persuasion et influence : prend différentes mesures à des fins de persuasion.
- Initiative : fait preuve de décision dans les situations où il faut agir sans attendre.
- Compréhension organisationnelle : comprend le climat et la culture de l'Organisation.
- Travail en équipe : coopère.

6. CONTRAT

Contrat proposé (hors détachement) : contrat d'une durée déterminée de trois ans ; renouvelable pour une période de trois ans maximum, au cours de laquelle le/la titulaire pourra demander qu'il soit transformé en contrat de durée indéterminée.

Clause contractuelle applicable :
Conformément à la politique des contrats, il s'agit d'un poste auquel il est souhaitable, pour des raisons politiques, d'assurer une rotation de manière à pouvoir répondre au besoin qu'a l'Organisation d'exécuter les tâches qui lui sont confiées par les pays dans un environnement en constante évolution, notamment en préservant la souplesse nécessaire à l'adaptation de son profil de compétences, et de veiller au degré de diversité approprié à son caractère international.
La durée de service maximale prévue à ce poste est de six ans. La personne retenue se verra offrir un contrat d'une durée déterminée de trois ans, qui pourra être reconduit pour une période de trois ans maximum. Toutefois, conformément à la procédure décrite dans la politique des contrats, elle pourra demander, au plus tard un an avant l'expiration de la deuxième période, que son contrat soit transformé en contrat de durée indéterminée.
Si la personne retenue est détachée de l'administration d'un État membre de l'OTAN, elle se verra offrir un contrat d'une durée déterminée de trois ans, qui, sous réserve de l'accord des autorités nationales concernées, pourra être reconduit pour une période de trois ans maximum. À ce poste, la durée de service d'un agent détaché n'excède pas six ans.
Les agents en fonction se verront offrir un contrat conforme aux dispositions du Règlement du personnel civil de l'OTAN.

7. INFORMATIONS UTILES CONCERNANT LA PROCÉDURE DE CANDIDATURE ET DE RECRUTEMENT

On notera que seules les candidatures de ressortissant(e)s de pays de l'OTAN pourront être acceptées. Les candidatures doivent être soumises comme suit :

- pour les seuls agents civils de l'OTAN : via le portail de recrutement interne (lien) ;
- pour toutes les autres candidatures : via le lien www.nato.int/recruitment.

Il est recommandé de commencer par regarder ici une vidéo proposant six conseils destinés à aider les candidat(e)s à préparer leur dossier.

En outre, on trouvera ici une vidéo expliquant la marche à suivre sur le portail pour introduire son dossier de candidature et s'assurer de sa réception par l'OTAN dans les délais fixés.

Lors de la soumission de votre candidature, veuillez vous assurer que votre profil de candidat Taleo est à jour et que votre CV est correctement téléchargé dans la section des pièces jointes de Taleo.

On trouvera de plus amples informations concernant le processus de recrutement et les conditions d'emploi sur le site web de l'OTAN (http://www.nato.int/cps/fr/natolive/recruit-hq-e.htm).
La nomination se fera après vérification des diplômes et des antécédents professionnels de la/du candidat(e) retenu(e) et sous réserve de la délivrance d'une **habilitation de sécurité** par les autorités du pays dont la/le candidat(e) retenu(e) est ressortissant(e), de l'approbation de son **dossier médical** par la/le médecin-conseil de l'OTAN et de l'achèvement du processus d'**accréditation** et de notification par les autorités compétentes.

Dans le cadre de ses procédures de recrutement et de sélection, l'OTAN n'acceptera aucune réponse qui aura été produite, en tout ou en partie, sur la base de documents de référence non explicitement cités (plagiat) ou au moyen d'outils disponibles sur Internet, y compris, entre autres, d'outils de traduction ou d'outils d'intelligence artificielle (IA) générative. Elle se réserve le droit de vérifier si la personne candidate a eu recours à de tels outils. L'OTAN pourra rejeter sans autre examen tout dossier de candidature élaboré, en tout ou en partie, à l'aide de ces outils. Elle se réserve également le droit de prendre toute autre mesure qu'elle jugerait nécessaire.

8. INFORMATIONS COMPLÉMENTAIRES

L'OTAN est déterminée à promouvoir la diversité et l'inclusion, et elle s'attache à assurer l'égalité de traitement en matière d'emploi, d'avancement et de fidélisation indépendamment de toute considération liée au genre, à l'âge, à la nationalité, à l'origine ethnique, à la religion ou aux croyances, à la culture, à l'orientation sexuelle, ou au handicap. L'Organisation examinera les candidatures de ressortissant(e)s de tous les pays membres, et encourage vivement les femmes à postuler.

Attachée aux principes d'inclusivité et d'accessibilité, l'OTAN prend toutes les dispositions nécessaires pour que les personnes porteuses d'un handicap puissent participer au processus de recrutement. Si vous avez besoin d'aménagements spécifiques, veuillez le préciser pendant votre processus de sélection.

Toute demande d'aménagement doit être étayée par une attestation médicale.

Le développement de l'intégrité est un élément clé des tâches fondamentales de l'Alliance. En tant qu'employeur, l'OTAN attache une grande importance au respect des principes d'intégrité, de transparence et de redevabilité, conformément aux normes et aux pratiques internationales établies pour le secteur de la défense et de la sécurité s'y rapportant. Les candidat(e)s sélectionné(e)s doivent être des modèles d'intégrité et s'employer en permanence à promouvoir la bonne gouvernance dans le cadre de leur travail.

En raison du vif intérêt suscité par l'OTAN et du nombre élevé de candidatures potentielles, il ne pourra pas être donné suite aux demandes de renseignements adressées par téléphone ou par courrier électronique.

Les candidat(e)s qui ne seront pas retenu(e)s pour ce poste pourront se voir offrir un poste analogue, au même grade ou à un grade inférieur, pour autant qu'ils/elles remplissent les conditions requises.

De par la nature du poste, le/la titulaire peut parfois être amené(e) à voyager pour le travail et/ou à travailler en dehors des heures normales de service.

L'Organisation, en application de plusieurs politiques sur l'équilibre entre vie professionnelle et vie privée, propose notamment des possibilités de télétravail et d'horaire flexible sous réserve des exigences liées à la fonction.

Le Secrétariat international de l'OTAN est un environnement sans tabac.

Pour en savoir plus sur l'échelle unique de rémunération mise en place à l'OTAN (grades, indemnités, etc.), veuillez consulter notre site web. Des informations détaillées sont fournies sous l'onglet Salaires et allocations.

L'OTAN ne vous réclamera jamais de frais dans le cadre d'une procédure de recrutement, que ce soit pour le dépôt de votre candidature, le traitement de votre dossier, les ressources mises à disposition, les entretiens, les épreuves, ou autre. Pour plus d'informations, cliquez ici.