Internship Notice: IT related posts (Cyber & Information Security; Transition Management; Network & Communications Infrastructure; Software Engineering; IT Product Management; Reporting and ITSM Processes; Operations Services)
Ref. eu-LISA/24/INTERN/IT

Posts	Internships in IT functions (Cyber & Information Security; Transition Management; Network & Communications Infrastructure; Software Engineering; IT Product Management; Reporting and ITSM Processes; Operations Services)
Internship duration:	6 months (with the possibility of extension, 12 months total)
Monthly grant[1]:	2,193.84 EUR
Place of assignment:	Strasbourg, France
Working model	Hybrid working arrangements – relocation to the place of assignment required
Targeted Starting Dates:	16 October 2024 16 November 2024
Level of Security Clearance[2]	SECRET UE/EU SECRET
Deadline for applications	15 July 2024[3] 11:59 am (Strasbourg, France) / 12:59 pm (Tallinn, Estonia)

[1] Indicative calculation for Strasbourg, France in 2024.
[2] Decision nr 2019-273 of the Management Board on the Security Rules for Protecting EU Classified Information in eu-LISA: https://eulisa.europa.eu/AboutUs/Documents/MB%20Decissions/2019-273_EUCI%20rules.pdf
[3] Date of publication: 11 June 2024

1. ABOUT THE AGENCY

We are eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. We are proud to design, develop and operate large-scale information systems at the heart of Schengen, in the area of internal security, border management and judicial cooperation. Our core mission is to keep Europe safe through technology, operating IT systems and providing services related to EU Justice and Home affairs policies. We aim to help the EU Citizens feel safe, protected, free, fairly treated and part of a united Europe.

Join us to become part of our organisational culture, an inclusive and diverse people centric environment. We believe in 'Together as one, we are making it happen'. We want our people to feel respected, valued and empowered. With a workforce consisting of more than 24 different nationalities, we embrace the international work environment and collaborate with colleagues from diverse backgrounds. It is our policy to provide equal employment opportunities for all applicants regardless of gender, race, disability, age, religion or belief, political views, sexual orientation, marital status or family situation, language, social origin, ethnicity or being part of a national minority.

We believe in creating a positive and enjoyable work environment for our people and we take pride in nurturing a work environment that values and recognises the contributions of our team members. As an organisation, we understand the importance of employee recognition in driving motivation and creating a fulfilling workplace.

Please visit our website and discover more about eu-LISA's core activities.

2. INTERNSHIP DESCRIPTION

The internship aims at enhancing your educational and professional experience through meaningful work assignments in your specific area of competence. During your internship, you will have the opportunity to be introduced to the EU professional world, learn from experts of different parts of Europe and contribute to a mission that has a direct impact on the daily life of millions of EU citizens.

Depending on your area of interest and suitability, you can express your interest in **ONE** of the following profiles. (Nevertheless, based on the recruitment needs of the Agency, you may be contacted or offered a post related to other profile(s) for which you are suitable.)

Profile A: Cyber Security & Information Security
Profile B: Transition Management - Release and Deployment Management
Profile C: Network and Communications Infrastructure
Profile D: Software Engineering
Profile E: IT Product Management
Profile F: Reporting and ITSM Processes
Profile G: Operations Services

The description of each profile can be consulted in the Annex.

All internship profiles require a security clearance. Therefore, all selected candidates will need to have, or be in a position to apply for a valid Personnel Security Clearance Certificate at the SECRET UE/EU SECRET level, immediately after signing the internship agreement.

A Personnel Security Clearance Certificate (PSCC) is defined as a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid national or EU PSCC, which shows the level of EU Classified Information (EUCI) to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET), the date of validity of the relevant PSC and the date of expiry of the certificate itself.

Candidates who hold a valid security clearance must provide a copy of their security clearance and specify the issuing authority, level and date of expiry. In case the validity of their security clearance expires within six months, the renewal procedure will be initiated expeditiously.

Kindly note that the necessary procedure for obtaining a PSCC shall be initiated by eu-LISA, and not by the individual candidate.

No appointment will be fully confirmed until the security clearance has been received by eu-LISA from the competent National Security Authority.

3. ELIGIBILITY CRITERIA

Candidates will be considered eligible for the selection on the basis of the following formal criteria to be fulfilled by the deadline for applications:

- You are a national of the Member States of the European Union or Schengen Associated Countries;
- You have completed at least three (3) years [six (6) semesters] of higher education course (university education or studies equivalent to university) or obtained the relevant degree (minimum a Bachelor or its equivalent) by the closing date for applications[4];
  N.B. Only qualifications that have been awarded in the Member States of the European Union or that are subject to the equivalence certificates issued by the authorities in the said Member States of the European Union shall be taken into consideration.
- You must have knowledge of the working language of eu-LISA (English) at least at level C1[5].
- You are covered in the event of illness or accident by a national social security scheme or a private insurance policy.[6] (The European Health Insurance Card is accepted).

[4] The selected candidate(s) must provide copies of certificates or declarations from the relevant University.
[5] Cf. Language levels of the Common European Framework of reference: http://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr
[6] Interns are covered by accident insurance for non-statutory staff only while working in the eu-LISA premises. eu-LISA does not cover health or general accident insurance.

4. SELECTION CRITERIA

Professional experience and knowledge:

- Have a degree in a field relevant to one or more of the internship profiles advertised (e.g., Information Technology, Computer Science, Cyber Security, Data Science, etc);
- Knowledge and/or experience related to the tasks of the internship profiles(s);
- Knowledge of Microsoft Office applications (Excel, Word, PowerPoint, Outlook);

Personal qualities:

- Ability to act upon eu-LISA's values and guiding principles (We get the job done - We take ownership - We are all role models - We act together as one).
- Good communication and interpersonal skills, including flexibility, ability to multitask and service-oriented approach;
- Ability to work as part of a team in a multicultural environment;
- Interest and willingness to learn.

5. EQUAL OPPORTUNITIES

eu-LISA guarantees equal opportunities and accepts applications without distinction on grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

6. CONFIDENTIALITY

The intern must exercise the greatest discretion regarding facts and information that come to his/her knowledge during the course of the internship. He/she must not, in any matter at any time, disclose to any unauthorised person any document or information not already made public. To ensure this discretion, the intern will be requested to implement and sign the eu-LISA Declaration of Confidentiality before starting the internship and will also be required to attend a security briefing immediately after having started the internship.

7. SELECTION PROCEDURE

Your application will be assessed on the basis of the eligibility and selection criteria specified above.

The shortlisted eligible candidates will be contacted to confirm their interest and availability for one or more assessment exercises (e.g., a pre-recorded video interview, a remote written test and/or interview, etc).

A talent pool (reserve list) of candidates may be established and used for the selection of similar internship positions depending on the needs of the Agency.

As English is eu-LISA's working language, the selection procedure will be fully conducted in English.

At any time prior to the start of the internship, candidates may withdraw their applications by informing eu-LISA HRU via e-mail: eulisa-INTERNS@eulisa.europa.eu

8. INTERNSHIP CONDITIONS: REMUNERATION AND BENEFITS

The internships are expected to start on 16 October 2024 and 16 November 2024. The initial internship period is offered for six (6) months, with a possibility of extension up to a total of twelve (12) months.

You will receive a monthly grant of 2,193.84 EUR which is 1/3 of the basic gross remuneration received by an official at the grade AD5 step 1 weighted by the correspondent correction coefficient[7] of 119,5% for Strasbourg, France.

Interns are solely responsible for the payment of any taxes due on the grant received from eu-LISA by virtue of the laws in force in their country of origin. The grant awarded to interns is not subject to the tax regulations applying to officials and other servants of the European Union.

Subject to budget availability, interns whose places of residence amounts to at least 50 km distance from the place of assignment are entitled to the reimbursement of their travel expenses incurred at the beginning and at the end of the internship.

eu-LISA's interns are entitled to annual leave of two (2) working days per each complete calendar month of service. Moreover, there are on average 19 eu-LISA Public Holidays per year.

9. PROTECTION OF PERSONAL DATA

eu-LISA ensures that applicants' personal data is processed in accordance with Regulation (EC) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

The legal basis for the selection procedures of interns is defined in eu-LISA's internship policy.

The purpose of processing personal data is to enable the selection procedure.

The selection procedure is conducted under the responsibility of eu-LISA's Human Resources Unit, within the Corporate Services Department. The controller for personal data protection purposes is the Head of the Human Resources Unit.

The information provided by the candidates will be accessible to a strictly limited number of HR staff of eu-LISA, to the Selection Panel, and, if necessary, to the Executive Director, Security and/or the Legal Officer of eu-LISA.

Almost all fields in the application form are mandatory; the answers provided by the candidates in the fields marked as optional will not be taken into account to assess their merits.

eu-LISA will keep applicants' files for no longer than two (2) years. Beyond this period, aggregate and anonymous (scrambled) data on internship applications will be kept only for statistical purposes.

All applicants may exercise their right of access to, rectification or erasure or restriction of processing of their personal data. Personal data such as contact details can be rectified by the candidates at any time during the procedure. In the case of data related to the admissibility criteria, the right of rectification cannot be exercised after the closing date of applications' submission.

[7] The correction coefficient is subject to a regular update.

Any substantiated query concerning the processing of his/her personal data can be addressed to the Human Resources Unit at eulisa-INTERNS@eulisa.europa.eu.
Applicants may have recourse at any time to the European Data Protection Supervisor (edps@edps.europa.eu).

10. APPLICATION PROCEDURE

In order for your application to be valid and considered eligible, you must create an account on eu-LISA's e-Recruitment tool, complete the personal and CV information as well as eligibility and selection criteria checklists.
If you wish to apply for a position at eu-LISA, you must apply via the e-Recruitment tool.
eu-LISA does not accept applications submitted by any other means (e.g., e-mail or post), or any spontaneous applications.

Please make sure you indicate your desired role profile as part of the professional competencies' criteria section when preparing your application in the eRecruitment platform.

The closing date for submission of applications is 15 July 2024 at 12:59 pm Tallinn time/11:59 am Strasbourg time.
Candidates are strongly advised to not wait until the last day to submit their application, since heavy internet traffic or a fault with the internet connection could lead to difficulties in submission. eu-LISA cannot be held responsible for any delay due to such difficulties.
Once the application has been successfully submitted to eu-LISA's e-Recruitment tool, candidates will be notified by email.
Please note that if at any stage of the selection procedure it is established that any of the requested information provided by a candidate is false, they will be disqualified.
In case of any queries about the selection process, please contact us via email:
eulisa-INTERNS@eulisa.europa.eu
If a candidate reaches the reserve list stage, they will be requested to supply documentary evidence in support of the statements that they made for this application.

ANNEX

Profile A: Cyber Security & Information Security

You will contribute to the work of two of the four sectors within the Security Unit: Cyber Security Sector and Information Security and Assurance Sector.

The Security Unit is responsible for the Agency's end-to-end security tasks. This includes the security of the IT systems the Agency operates, the physical security of its premises, the security of its personnel and assets, as well as security related to its outsourced activities.

Under the supervision of a Tutor and with the overall reporting capacity to the Head of Unit, you are expected to provide support in:

- Drafting security policies, standards and guidance documents;
- Security risk management based on the ITSRM2 methodology and tools;
- Security monitoring and event analysis, including the drafting of procedures and playbooks;
- Security incident management processes, including the drafting of procedures and playbooks;
- Technical vulnerability management, including the drafting of procedures and playbooks;
- Secure configuration and hardening, security engineering and security solution management activities, including the drafting of security documentation;
- Security and business continuity awareness and training activities for the current year;
- Eliciting security requirements from the applicable regulations for eu-LISA;
- All activities related to the tasks performed in the relevant Sectors, as instructed by the Head of Sectors.

Profile B: Transition Management - Release and Deployment Management

The Transition Management Sector is one of the two sectors of the Transition and Automation Unit. The mission of the sector is to ensure a controlled and exhaustive transition of systems and services to Operations and to deliver new functionalities required by the business while protecting the integrity of existing services.

Under the supervision of a Tutor, you are expected to carry out the following duties:

- Supporting the coordination at technical and business level of all the releases and patches concerning the systems under the Agency's responsibility by detecting and resolving any technical dependency or business constraints;
- Assisting in the improvement and final definition of the overall Transition Plan (document) for any changed product or service in cooperation with the Project teams;
- Contributing to outline the team's involvement in the DevOps pipeline (for non-production environments) and in standardizing the Software Development Plan deliverable across all new systems while clarifying the scope of the Sprints;
- Supporting the creation and improvement of a sector's Wiki (utilizing market-leading tools such as Confluence) while replacing the current document-dependant knowledge management system (SharePoint) and contributing to the simplification and maintenance of the existing system until it is decommissioned;
- Assisting in the creation of a standardized "introduction/welcome package" for the team's newcomers;

- Contributing to the identification of all the Release Management team's interfaces with other sectors' (and teams) as well as in the definition of the roles and responsibilities for all release related activities (e.g., RACI matrix);
- Assisting in the Transition related requirements elicitation process by liaising with other stakeholders and agreeing on their final ownership while improving their quality;
- Supporting the improvement of the release process/policy and its template documents in order to avoid information duplication and improve clarity;
- Engaging proactively in all team's activities and suggest improvements of processes and tools.

Profile C: Network and Communications Infrastructure

The Network and Communications Infrastructure Sector (NCIS) is under the Platforms and Infrastructure Unit (PIU) and is responsible for supporting and maintaining the seamless operation of large-scale Justice and Home Affairs solutions entrusted to eu-LISA. This encompasses overseeing the delivery and management of network infrastructure and communication services. The activities include operation, maintenance and evolution of the running solutions, Product Management of TESTA network, EUWS Port service delivery, Serena network service delivery. In addition, NCIS provides network related consultancy supporting the development of Solutions and Platforms, to ensure the collaboration and appropriate interface among the Sectors of PIU.

Under the supervision of a Tutor, you are expected to carry out the following duties:

- Providing support in the daily operational tasks of the Sector, such as Incident Management and Request Fulfilments;
- Supporting internal research activities by conducting data gathering and analysis to develop network operations tools solutions to integrate AI techniques;
- Assisting in tasks related to document review of contractors' deliverables;
- Contributing to the drafting and review of internal guidelines and procedures;
- Supporting the management and development of the intranet Sector's page;
- Maintaining effective information sharing and co-operation with relevant stakeholders;
- Undertaking other support tasks as necessary.

Profile D: Software Engineering

The Software Engineering Sector is part of the Technology and Software Engineering Unit and its mission is to ensure the quality of the large-scale IT systems' software, providing subject matter expertise on the software design, including software code quality. The sector is also responsible for designing, operating and maintaining the in-house build and deployment pipelines with the DevOps tools.

Under the supervision of a Tutor, you are expected to conduct the following duties:

- Configuring and using Continuous Integration (CI) pipelines on Core Business System (CBS) projects;
- Researching on Cloud solutions for CI;
- Assisting in the creation and maintenance of a "lab" environment for testing and experimenting with existing and planned technologies and tools complying with the platform and security requirements.

Profile E: IT Product Management

The Programme and Solutions Management Unit encompasses three sectors: the Home Affairs Programmes Sector, the Justice Programmes Sector and the Solutions Expertise Hub. The mission of the unit is to deliver all Programmes and Projects for the Operations Department of eu-LISA within set tolerances of scope, time, budget and quality, to ensure that approved projects and programmes related to large-scale information systems are organized and executed in a consistent manner and within established standards.

Under the supervision of a Tutor in the Solutions Expertise Hub Sector, you are expected to carry out the following tasks:

- Developing and improving strategies: You will work on product and business strategies, recommending new strategies and improvements. You may also collaborate with policy units to capture user needs;
- Collaborating with key stakeholders: You will communicate with all solution-related parties, developing a communication system for instant feedback. You identify market trends, stakeholder behaviour, and solution reception patterns, and determine stakeholder-specific solution features. You will also collaborate with architects to derive product requirements documents;
- Working on the Solution roadmap and lifecycle: You will learn about the solution vision, roadmap, and lifecycle, creating and managing a feature backlog. You will also assist with roadmap planning and can recommend changes and improvements. As part of the assignment, you will deliver solution requirement documents to program/project teams for implementation;
- Market research and analysis: You may conduct thorough market research to understand stakeholders needs, trends, and competitive landscape. You may analyse data to support decisions and strategy;
- Documentation and training materials: You may develop and maintain solution documentation and training materials, creating user guides, FAQs, and training manuals;
- Supporting Solution launches: You may be involved in the coordination with internal teams to plan and execute solution launches, in creating launch plans, in preparing and organizing launch events or webinars.

Profile F: Reporting and ITSM Processes

The Transition and Automation Unit consist of the Automation and Tooling Sector and the Transition Management Sector. The mission of the unit is to ensure well managed and controlled transition to operation of new or modified components or systems by running one of the three processes: release management, operational change management or transition operations and by administering and supporting the operational tools. Additionally, the unit enables the availability and up-to-date of operational documentation and the provision of the tools that support and allow more efficiency in Operations.

Under the supervision of a Tutor in the Automation and Tooling Sector, you are expected to carry out the following tasks:

- Providing support in the migration of the report templates from Crystal Reports into the new CRRS (Central Repository for Reporting and Statistics) System established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes;
- Providing support with the new CRRS system administration and configuration;
- Providing assistance for SIS II (Schengen Information System version 2) statistics report;

- Running data quality check reports;
- Assisting with the execution of reporting and communication activities;
- Supporting all activities related to the tasks performed in the Sector.

Profile G: Operations Services

The mission of the Operations Unit is to ensure the operational management of the Digital Solutions with the business systems functioning within the Service Level Agreements. This is executed via the monitoring of the operations and the performances of the large-scale IT systems, the coordination of operational processes (incidents, problems etc.), the detection and first response to incidents (including security incidents), the provision of technical support and expertise on the Digital Solutions from an applications and databases perspective and the maintenance of the systems in Operations. In Particular, the Operations Services Centre delivers the 24/7 Service Desk, Solutions Monitoring & Incident Response and Cyber Defence capability.

Under the supervision of a Tutor in the Operations Services Centre, you are expected to carry out the following tasks:

- Supporting the execution of security monitoring, event analysis, and security incident response, including drafting procedures and playbooks;
- Providing process maturity improvement for incidents and improving training materials;
- Developing a customer engagement framework and enhancing customer satisfaction scores;
- Ensuring continuous improvement activities for monitoring, detection, defence and response activities;
- Contributing to the definition and development of the unified logging, monitoring and detection approach;
- Developing operational intelligence and AIOps strategies;
- Preparing reporting and communication;
- Contributing to the drafting and review of internal guidelines and procedures;
- Supporting the management and development of the intranet Sector’s site;
- Supporting all activities related to the tasks performed in the Sector.