Internship Notice: IT related posts (Cyber & Information Security; Transition & Release Management; IT Service Management; IT Network Infrastructure; IT Project Management; Software Quality Assurance)
Ref. eu-LISA/25/INTERN/IT

CORRIGENDUM TO VACANCY NOTICE (pages 2 and 4)

Posts	Internships in IT functions (Profile A: Cyber & Information Security; Profile B: Transition & Release Management; Profile C: IT Service Management; Profile D: IT Network Infrastructure Administration; Profile E: IT Project Management; Profile F: Software Quality Assurance)
Internship duration:	6 months (with the possibility of extension, 12 months total)
Monthly grant[1]:	~~2,247.97 EUR~~ 2,273.89 EUR
Place of assignment:	Strasbourg, France
Working model	Hybrid working arrangements – relocation to the place of employment required
Targeted Starting Date:	October 2025
~~**Level of Security Clearance**[2]~~	~~SECRET UE/EU SECRET~~
Deadline for applications	01 July 2025[3] 11:59 am (Strasbourg, France) / 12:59 pm (Tallinn, Estonia)

[1] Subject to a regular update.
[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: 01 April 2025

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 help implement the European Union's policies by designing, developing, and operating large-scale information systems in internal security, border management, and judicial cooperation.

Our teams develop and manage the technological architecture of the Schengen area and the EU justice domain. By equipping law enforcement and border management operators and juridical practitioners with cutting-edge technological infrastructure, we help ensure security and justice for citizens.
With a workforce of more than 24 nationalities, eu-LISA embraces an international work environment and values collaboration among colleagues from diverse backgrounds, and is committed to provide a positive and enjoyable work environment.

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

2. INTERNSHIP DESCRIPTION

We are looking for motivated young talents who can bring a fresh perspective to our tech teams. Whether you are a recent university graduate, an early-career professional or pursuing a master's degree, if you have a passion for IT, we want to hear from you!

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 are welcome to express your interest for one of the following six 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 and Information Security
Profile B: Transition Management – (Junior) Release Manager
Profile C: IT Service Management
Profile D: IT Network Infrastructure Administrator
Profile E: IT Project Management
Profile F: Software Quality Assurance

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

Repealed:

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.

Replaced with:

Internship positions do not require a security clearance. Therefore, none of the 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.

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.

[4] The selected candidate(s) must provide copies of certificates or declarations from the relevant University.

- You must have knowledge of the working language of eu-LISA (English) at least at level C1[5].

4. SELECTION CRITERIA

Key competencies:

- Have a degree in a field relevant to one or more of the internship profiles advertised (e.g., Information Technology, Computer Science, Cyber Security, Engineering, Data Science, etc.);
- Demonstrated ability or potential to perform the tasks of the internship profiles(s);

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, and a service-oriented approach;
- Ability to work as part of a team in a multicultural environment;
- Eagerness to learn and proactive attitude.

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 sign and implement 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.

[5] Cf. Language levels of the Common European Framework of reference: http://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr

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 in October 2025. The initial internship agreement 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 ~~2,247.97 EUR~~ 2,273.89 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 of 114.2% for Strasbourg, France[6].

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.

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. The intern is solely responsible to arrange such insurance prior to the start of the internship at eu-LISA. Proof of this insurance shall be submitted to eu-LISA prior to the beginning of the internship. Not presenting respective proof may be a reason to refuse the internship. The European Health Insurance Card is accepted.

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.

[6] Subject to a regular update.

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.

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, applicants 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 profile as part of the professional competencies' criteria section when preparing your application in the eRecruitment platform.

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 and Information Security

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.

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

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

- 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 Sector(s), as instructed by the Head of Sector(s) and/or the designated Tutor.

Profile B: Transition Management – (Junior) Release Manager

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;
- Supporting the coordination on technical, business and organisational level of transition to operations, including support to eu-LISA customers;
- 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;
- 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);

- 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: IT Service Management

The Automation and Tooling Sector is part of the Transition and Automation Unit. The Automation and Tooling Sector's main responsibilities include: the automation for operations, the user support for the ITSM (Information Technology Service Management) tools, the preparation of the operators' manuals and the support for the operational procedures for new systems.

Under the supervision of a Tutor, you are expected to carry out some of the following potential tasks:

- Providing support to the preparation of the Operators' manual for the new business systems and interacting with all relevant stakeholders;
- Becoming familiar with the functionalities of the central business systems, their scope and the expected support model after entry-into-operation;
- Gaining hands-on experience with the Agency's ITSM framework and supporting tools, potentially participating in the implementation, testing and maintenance of those tools;
- Providing support to the execution of reporting and running data quality checks, using Crystal Reports and SQL Developer, or any other tools in use at the Agency;
- Providing support with the new CRRS (Central Repository for Reporting and Statistics) system administration and configuration, and helping in the migration of the report templates from Crystal Reports into CRRS;
- Gaining hands-on experience on the event management and monitoring system of the Agency, participating in the monitoring and observability standard definition;
- Supporting various activities related to the tasks performed in the Sector, as instructed by the Head of Sector and/or the designated Tutor.

Profile D: IT Network Infrastructure Administrator

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 for the Network Infrastructure of the operated Systems.
- Supporting internal research activities by conducting data gathering and analysis to develop network operations tools solutions, such as integration to 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 E: IT Project Management

The Programmes Management Unit (PMU) is responsible for the management of all programmes addressing the implementation of all large-scale IT systems and digital solutions entrusted to eu-LISA in the Justice and Home Affairs (JHA) domain; this includes the evolution of all existing large-scale IT systems. PMU operates in compliance with the respective system-specific legal bases, as well as stakeholder expectations and milestones agreed at the political level.

PMU's Programme and Project Management Teams oversee and coordinate all associated activities until the developed products are ready for operational use. PMU is supported by the Project Practices and Methodologies Sector (PPMS), responsible for facilitating the implementation of all projects, in an agile and efficient manner, through appropriate tools and project management practices. PMU comprises three sectors: Home Affairs Programmes Sector (HAPS), Justice Programmes Sector (JUPS) and Interoperability Programmes Sector (IOPS).

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

- Performing quality assessments of projects delivered in the Agency;
- Processing documentation in order to keep it aligned with internal control standards, relevant internal processes and needs of the Agency;
- Organizing and performing necessary quality assurance tasks of projects within their lifecycle;
- Ensuring that project managers in the Agency receive adequate support and have necessary toolset to implement their duties;
- Providing support with the extraction and collection of data from different sources. Assist in the analysis and structuring of data, and compiling periodic updates to management;
- Facilitating the Project Management process by acting as central point for lessons learned, templates, best practice and estimation techniques;
- Supporting project managers in resource planning ensuring that resource dashboard(s) are updated regularly.
- 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 project requirements documents;
- 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;
- 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: Software Quality Assurance

The Technology and Software Engineering Unit (TSU) is responsible for overseeing the successful technical implementation of all IT core business systems and solutions managed by eu-LISA. TSU contributes to the technical delivery of large-scale IT development projects by providing subject matter expertise and hands-on capabilities in the following engineering domains: system and solution architecture, software design and development, DevOps, testing and quality assurance.

To that end, TSU provides a detailed framework, guidance and hands-on expertise on building large-scale IT systems and digital solutions, while also ensuring the software quality of those systems. To ensure that all new systems and releases are fit for purpose and in compliance with relevant quality expectations, TSU oversees comprehensive testing for software solutions and integrating services for all IT systems delivered for the EU's JHA community. TSU comprises four sectors: Solutions and Architecture Design Sector (ARCS), Software Development Sector (SODS), Continuous Software Delivery Sector (CSDS) and Solutions Quality Assurance Sector (SQAS).

As a Software Quality Assurance Intern, you will assist the test team in ensuring the quality of our software. You will learn the basics of software testing and contribute to making sure our applications work as expected. This role is a great opportunity to gain hands-on experience in a real-world software development environment and learn from more experienced QA professionals.

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

- Assist in Test Case Execution: Execute pre-written test cases and document results and bug reporting.
- Test Documentation: Help maintain and organize test documentation.
- Basic Test Planning: Assist in creating simple test plans.
- Learning Test Tools: Become familiar with basic testing tools and understand their added value and limitations.
- Team Collaboration: Work with QA engineers and developers in a constructive and positive environment.

What's in it for you?

- Become a Quality Expert: Learn the fundamental skills of software testing and see firsthand how your work impacts the final product.
- Unlock the Secrets of Software Development! Get a real-world look at the software development lifecycle and gain invaluable experience in a collaborative team environment.
- Master the Tools! Get hands on exposure to testing tools, and build a foundation for a future in tech.