Internship Notice: IT related internship posts
Ref. eu-LISA/26/INTERN/IT

Posts	Internships in IT functions (Profile A: Cyber & Information Security; Profile B: Business Analysis; Profile C: Information and Communication Technology; Profile D: IT Network Infrastructure Administration; Profile E: Service Transition & Release Management; Profile F: IT Service Management; Profile G: Application Management; Profile H: Enterprise Architecture; Profile I: Software Delivery Engineering; Profile J: Software Quality Assurance; Profile K: Project Administration Support; Profile L: IT Project Support (Home Affairs domain); Profile M: IT Project Support (Judiciary domain)
Internship duration:	6 months (with the possibility of extension, 12 months total); full-time, 40 hours/week
Monthly grant[1]:	2,329.80 EUR
Place of assignment:	Strasbourg, France
Working model	Hybrid working arrangements –relocation to the place of assignment required
Targeted Starting Date:	01 October 2026
Deadline for applications	30 April 2026[2] 11:59 am (Strasbourg, France) / 12:59 pm (Tallinn, Estonia)

[1] Subject to a regular update.
[2] Date of publication: 06 March 2026

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. As an equal opportunity employer, we are committed to providing a positive and enjoyable work environment. We welcome applications from all suitable candidates, irrespective of age, gender, ethnicity or social origin, disability, religion or belief, and sexual orientation.

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 background, area of interest and suitability, you may express your interest for any of the below profiles by indicating your order of preference. Please note, however, that in line with the Agency's recruitment needs, you may also be contacted or offered a position in another profile for which you are considered suitable.

Profile A: Cyber Security and Information Security
Profile B: Business Analysis
Profile C: Information and Communication Technology
Profile D: IT Network Infrastructure Administration
Profile E: Service Transition and Release Management
Profile F: IT Service Management
Profile G: Application Management
Profile H: Enterprise Architecture
Profile I: Software Delivery Engineering
Profile J: Software Quality Assurance
Profile K: Project Administration Support
Profile L: IT Project Support (Home Affairs domain)
Profile M: IT Project Support (Judiciary domain)

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

3. ELIGIBILITY CRITERIA

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

- You are national of one of the European Union Member States or Norway, Iceland, Liechtenstein, or Switzerland and you enjoy full rights as a citizen[3];

- 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];

Only qualifications awarded in an EU Member State or that are subject to an equivalence certificate issued by an authority in a said EU Member State shall be taken into consideration.

- 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, Business Informatics, Cyber Security, Engineering, Data Science, etc.);
- Demonstrated ability or potential to perform the tasks of the internship profiles(s);
- Strong communication skills in English at least at level C1;

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

5. 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 prior to starting the internship and will also be required to attend a security and cybersecurity briefing immediately after having started the internship.

6. SELECTION PROCEDURE

[3] Prior to hiring, the successful candidate will be asked to provide a certificate of absence of any criminal record issued by the competent authority.
[4] The selected candidate(s) must provide copies of the diploma, or certificates 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

Applications will be assessed on the basis of the eligibility and selection criteria specified above. Only shortlisted candidates will be contacted and invited to the next stage of the selection process, which may involve various assessments.

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, any communication related to the selection procedure, including the assessments during 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

7. INTERNSHIP CONDITIONS: REMUNERATION AND BENEFITS

The internship positions are expected to be filled on 01 October 2026. 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 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 113.6% 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.

Interns shall observe the regular working hours at eu-LISA: working forty (40) hours per week, from Monday to Friday, eight (8) hours per day respecting the core hours of eu-LISA.

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 18 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

[6] Subject to a regular update.

beginning of the internship. Not presenting respective proof may be a reason to refuse the internship. The European Health Insurance Card is accepted.

8. 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.

Any substantiated query concerning the processing of his/her personal data can be addressed to the Human Resources Unit (eulisa-INTERNS@eulisa.europa.eu)**.**

Applicants may have recourse at any time to the European Data Protection Supervisor (edps@edps.europa.eu).

9. APPLICATION PROCEDURE

In order for your application to be valid and considered eligible, applicants must create an account on eu-LISA's e-Recruitment platform, complete the personal and CV information as well as eligibility and selection criteria checklists and submit it by to the deadline for applications.

If you wish to apply for a position at eu-LISA, you must apply via the e-Recruitment platform. 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 (SCU) is responsible for safeguarding eu-LISA's assets, in particular the large-scale IT systems and data entrusted to the Agency. By ensuring the secure and continuous operation of large-scale IT systems, together with an appropriate level of data and physical security, SCU contributes to compliance with the provisions of Article 2 of eu-LISA's establishing Regulation.

In order to ensure uninterrupted service availability to the EU's Justice and Home Affairs community, SCU's scope of activities covers security governance and assurance, risk management, information security, business continuity and disaster recovery. This task includes overseeing eu-LISA's security and continuity management system (SCMS) and operating the Computer Security Incident Response Team (CSIRT). SCU is also responsible for the protection of classified information, as well as ensuring the physical security of eu-LISA premises and staff in three locations: Tallinn, Estonia; Strasbourg, France; and Brussels, Belgium.

The unit comprises the Security Policy and Coordination Sector (SPCS), Information Security and Resilience Sector (ISRS), the Cyber Security Sector (CYBS) and the Protective Security Sector (PSCS).

The **Information Security and Resilience Sector (ISRS)** is responsible for providing comprehensive information security, business continuity and assurance services to ensure operational resilience and uninterrupted operation of both corporate and JHA information systems/services, as well as the underlying infrastructure hosting the systems.

In order to effectively mitigate vulnerabilities and threats to eu-LISA's assets and systems, ISRS upholds the highest standards of security compliance through robust security building blocks and comprehensive security assurance measures. This task includes proactive risk assessments, customised security and business continuity plans (incl. for each JHA system managed by eu-LISA), vulnerability management, penetration tests, and security reviews.1 In addition, ISRS collaborates closely with stakeholders across the EU to address emerging security challenges and implement proactive solutions.

To ensure the continuous improvement of eu-LISA's security and business continuity processes, ISRS organises trainings and regular business continuity exercises to test operational processes and procedures during disruptive incidents and to identify areas for improvement. Additionally, ISRS coordinates the implementation of recommendations gleaned from exercises, inspections and audits, incl. drafting action plans and subsequent reporting.

The **Cyber Security Sector (CYBS)** is responsible for safeguarding the integrity of eu-LISA's digital assets, in particular EU's JHA information systems, infrastructure and data entrusted to the Agency. The main objective is to ensure the integrity, confidentiality and availability of systems and services to stakeholders in the EU's JHA community.

In order to identify and mitigate cyber threats, CYBS applies proactive and robust cybersecurity measures in accordance with best practices in threat detection and incident management. This includes access management and the continuous monitoring of the entire IT ecosystem to ensure swift response to security incidents, such as attacks, intrusions, data breaches or security policy violations.

Incident response is coordinated by a dedicated Computer Security Incident Response Team (CSIRT) in accordance with established processes and protocols, incl. isolation, eradication, mitigation, and recovery. CSIRT's mandate also includes security information and event management (SIEM), vulnerability management, crisis management support and incident follow-up, incl. proposing improvements.

To ensure the continuous improvement of eu-LISA's defensive capabilities, CYBS focuses on maintaining threat hunting capability that covers eu-LISA's entire spectrum and conducts exercises to assess and improve established cybersecurity measures. In this regard, CYBS collaborates closely with stakeholders in the EU's CSIRT network by sharing threat intelligence, and supporting cybersecurity exercises.

Additionally, CYBS provides subject matter expertise for the design and deployment of systems and applications to facilitate robust security engineering practices, in particular for integration with existing cybersecurity tools and services. CYBS also contributes to the improvement eu-LISA's overall security posture and resilience by organising awareness sessions and provides training on topics related to cybersecurity and incident management.

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

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- 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;
- Undertaking other support tasks as necessary.

Profile B: Business Analysis

The Business and Stakeholder Relations Unit (BSU) is responsible for managing eu-LISA's external relations by overseeing the management of business, stakeholder and institutional relations, as well as communication and public relations activities. In this role, BSU's core objective is to maintain and reinforce the Agency's reputation as a trusted and reliable partner in its areas of expertise.

Under the business relations management function, BSU's Business Relations Management Sector (BRMS) acts as the main interface between eu-LISA and its stakeholders in the EU's Justice and Home Affairs (JHA) domain. In this role, BRMS is responsible for ensuring structured interfacing with stakeholders, as well as overseeing the implementation of stakeholder demands and legal/business requirements that feed into the design and development of all IT systems entrusted to eu-LISA.

The stakeholder relations management function includes the provision of administrative support to all eu-LISA's governance bodies. To that end, BSU operates the eu-LISA Management Board Secretariat (MBS) who also supports the work of Advisory Groups (AG) and Programme Management Boards (PMB) that provide guidance for the development of JHA information systems entrusted to eu-LISA. BSU is also responsible for the policy function within the Agency and for coordinating relations with other EU agencies and networks, primarily in the JHA domain.

As for institutional relations management, BSU hosts the Agency's Liaison Office team who are responsible for cultivating efficient information exchange and working relations with eu-LISA's key stakeholders based in Brussels, in particular EU institutions and bodies.

As a separate task, BSU oversees eu-LISA's corporate communication and public relations function by managing internal and external communication activities, with a view to upholding the Agency's image as a trusted and valuable partner to its stakeholders in the EU's JHA community.

The unit comprises the Business Relations Management Sector (BRMS), the Governance and Stakeholder Management Sector (GSMS), the Communication Sector (COMS) and the Liaison Office team.

The **Business Relations Management Sector (BRMS)** is the business interface between eu-LISA and its stakeholders, i.e., Member State authorities (incl. Schengen associated countries) from all business areas (borders, visa, immigration, law enforcement and justice), EU institutions and agencies, international organisations, and on the industry side, passenger carriers operating at air, land and sea.

BRMS objective is to earn and retain the trust of all stakeholders by creating and maintaining the conditions for a trustful relationship between them and the Agency.

Under the portfolio management function, BRMS oversees three interconnected processes: business relationship management, demand management and requirements management. The portfolio management function performed by BRMS oversees the policy implementation and drives from strategic perspective the approach for the implementation of stakeholder demands and business requirements for all JHA domain products entrusted to eu-LISA.

In this regard, BRMS is involved in two strategic initiatives: (1) the Demand Management Initiative (DMi), and the Business to Build (B2B) initiative. Via the Demand Management Initiative (DMi), BRMS ensures that all stakeholder demands are properly captured, recorded, analysed and converted, if approved, into business requirements that feed into the systems development lifecycle. The latter allows BRMS to analyse the impact of any demand from resource (human and financial) and planning perspectives, which is a major contribution to the preparation of the legislative financial statements (LFS) by the European Commission. In addition, BRMS plays a major role in the Business to Build (B2B) initiative, ensuring a structured transition of business demands, as well as continuous control and monitoring of their implementation in the build phase.

As the main interface for eu-LISA's stakeholders, BRMS plays a key role in the work of eu-LISA's governance bodies: Management Board, Advisory Groups, Programme Management Boards and the Working Group for Carriers. In this role, BRMS is responsible for chairing the meetings and coordinating discussions to provide internal/external guidance for all information systems and digital solutions entrusted to eu-LISA. In addition, BRMS participates in the work of various other groups at EU level, i.e., committees and working parties of the European Commission, Council and the Parliament.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- Provide transversal and practical support to the business analysis activities, in particular by fostering the efficient and coordinated use of existing tools for agile projects (i.e. JIRA, Confluence, SES Reuse).
- Assessing and proposing improvements in the use of tools for business analysis activities (documenting requirements, business use cases, business process modelling, etc).
- Contribute to the preparation and consolidation of information relevant for stakeholders, such as analysing statistical data or collect and compile data from multiple stakeholders;
- Working closely with other colleagues on the different business areas;
- Assist the sector in the organisation of meetings with stakeholders and the preparation of the associated material;
- Undertaking other support tasks as necessary.

Profile C: Information and Communication Technology

The Corporate Services Department (CD) is responsible for managing and coordinating eu-LISA's resource administration to ensure the Agency's smooth, compliant and efficient operation at all sites across the EU, i.e., Tallinn, Estonia; Strasbourg, France; Brussels, Belgium, and St Johan im Pongau, Austria. This task includes the management of facilities and physical assets, as well as human and financial resources. In addition, the department coordinates the provision of the following support services: ICT, procurement, missions, logistics, supplies, and document management.

The department comprises three units: the Budget and Finance Unit (BFU), the Procurement and Contract Management Unit (PCU) and the Human Resources Unit (HRU). In addition, the department hosts two sectors: the General Services Sector (GESS) and the ICT Services Sector (ICTS).

The **Information Communication Technology Services Sector (ICTS)** is responsible for corporate ICT services needed for the Agency's daily operation, ensuring that the corporate IT infrastructure is reliable, flexible, highly available, and integrated in the areas of ICT systems, networks communication, and IT applications.

To that end, ICTS is responsible for the development, evolution and maintenance of the corporate IT infrastructure and applications, as well as providing support to staff via dedicated corporate helpdesk. The Agency's corporate IT function is also responsible for improvement projects aimed at increasing the efficiency and agility of the organisation, including the implementation of the Information Technology Infrastructure Library (ITIL), and the migration of IT services to the cloud.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- Review and validate the monthly reports (Service Level Agreements compliance, ticket resolution times, etc.);
- Track trends in incident and request to identify anomalies or emerging patterns;
- Monitor the quality and relevance of the Knowledge Base (checking for outdated or duplicate articles, etc.);
- Collect end-user feedback and complaints, categorize and summarize patterns;
- Support compliance checks;
- Help facilitate regular review meetings (agenda, scheduling, minutes);
- Contribute to service documentation updates, especially around onboarding new team members or transitioning services;
- Assist in change and release coordination by tracking calendar events and checking if service desk is informed/involved as needed;
- Review ICTS Inventory and check and monitor the meeting rooms inventory and meeting rooms usage;
- Undertaking other support tasks as necessary.

Profile D: IT Network Infrastructure Administrator

The Platforms and Infrastructure Unit (PIU) is responsible for the engineering, operation and maintenance of the underlying networks, infrastructure and platforms that host the applications of the Justice and Home Affairs (JHA) information systems, solutions and services entrusted to eu-LISA. PIU ensures that these components are managed in a secure, reliable, and scalable manner, providing a robust foundation for the Agency's IT operations. These tasks are delivered via core infrastructure services in the Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) model. In addition, PIU is also responsible for the configuration management process, which includes maintaining eu-LISA's Configuration Management Database (CMDB).

As product owner, PIU is responsible for eu-LISA's core infrastructure and platform products: common shared infrastructure (CSI), communication network (TESTA-ng), common shared platform (CSP), comprehensive cloud platform (CCP), and end-user workstations (EUWS) for operational management, including its secure remote access solution SERENA. In addition, PIU will be responsible for the National Uniform Interface (NUI) and Internet Zone (IZ) platforms, after their completion and takeover from the contractor.

In this capacity, PIU provides infrastructure-related expertise and engineering support throughout the system development cycle, working closely with application owners, service managers, project managers, software developers, architects, technical teams and contractors, to ensure that eu-LISA designs and delivers well-functioning systems in compliance with established requirements, as well as applicable regulations, and service-level agreements.

Although eu-LISA's data centre facilities are managed by the General Services Sector (GESS), PIU is responsible for the technical specifications, installation and maintenance of IT equipment housed within these facilities. In addition, PIU manages external partnerships by providing hosting services to Frontex and the EU Agency for Asylum (EUAA).

The unit comprises the Infrastructure Maintenance and Support Sector (IMSS), the Network and Communications Infrastructure Sector (NCIS) and the Smart Hosting Platforms Sector (SHPS).

The **Network and Communications Infrastructure Sector (NCIS)** is responsible for the engineering, operation and maintenance of the underlying network and communication infrastructure services that support the JHA information systems, solutions and services entrusted to eu-LISA. Under this task, NCIS provides the communications network TESTA-ng that ensures secure and reliable communication between the central systems of large-scale IT systems managed by eu-LISA and their end-users in the EU's JHA community, i.e., the Member States and EU agencies.

In the process of network and communications infrastructure maintenance, NCIS contributes its expertise and engineering support for the corrective, adaptive and evolutive maintenance of network components underpinning the JHA information systems.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- 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 page of the Sector;
- Maintaining effective information sharing and co-operation with relevant stakeholders;
- Undertaking other support tasks as necessary.

Profiles E and F

The Transition and Automation Unit (TAU) is responsible for ensuring that all new or modified IT systems or components developed by eu-LISA for the JHA community are ready for smooth operational management, and undergo a well-managed transition into operation. In addition to onboarding new systems and releases, TAU must

ensure they remain fit for purpose throughout their lifetime. To that end, TAU is responsible for three processes – operational change management, release management, and transition into operation.

Throughout, TAU supports eu-LISA's operational efficiency through the delivery, administration and maintenance of operational tools that facilitate all eu-LISA's ITSM processes, and provides support to internal users. In addition, to ensure uninterrupted availability of all JHA systems managed by eu-LISA, TAU staff perform stand-by duty at the backup site in Austria (BCU), and contribute to 24/7 systems support as Critical incident Coordinators (CiC) or Managers on Duty (MoD).

The unit comprises the Transition Management Sector and the Automation and Tooling Sector.

Profile E: Service Transition & Release Management

The **Transition Management Sector (TRMS)** is responsible for overseeing the transition into operation process for all large-scale IT systems, solutions and services developed or managed by eu-LISA. The main goal is to deliver new functionalities as per established business requirements, while also safeguarding the integrity of existing systems and services. To that end, TRMS oversees three processes – operational change management, release management, and transition into operation.

An important component of the smooth handover to operations is knowledge transfer from development teams to operational and support staff, enabling them to effectively and efficiently deliver, support and maintain the product or service in compliance with relevant requirements and service level agreements.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- 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;
- 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;
- Undertaking other support tasks as necessary

Profile F: IT Service Management

The **Automation and Tooling Sector (AUTS)** is responsible for the administration of eu-LISA's transversal operational service tools (i.e., tools for system monitoring, reporting, event management, etc.) and ITSM processes that enable the efficient operation of JHA information systems. These tools are used for the delivery of 24/7 end-user support via the External Service Desk and they also facilitate operational resolution processes, ensuring the EU's JHA community with well-functioning systems in compliance with the legal basis and service-level agreements. This task also includes the corrective, adaptive and perfective maintenance of the tools, providing related user support, as well as contributing to operational ITSM quality management.

As a separate task, AUTS is also responsible for advancing intelligent business process automation, an approach that combines artificial intelligence (AI) and process automation. The objective is to improve efficiency and

optimise costs by automating repetitive and time-consuming tasks, allowing staff to focus on more complex and engaging tasks that yield higher value. In the long term, intelligent automation will boost end-user satisfaction thanks to improved quality, operational efficiency, and faster response times.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- Main Objective: Develop an interactive e-learning onboarding module for new users of the eu-LISA ServiceNow platform and perform reporting on metrics, SLAs, KPIs and processes.
- IT Area: IT Service Management (ITSM), based on the ITIL V4 standard and implemented in the eu-LISA ServiceNow platform.
- Content Inputs:
  - Feedback from users and process owners
  - Existing workshop materials, demos, and training recordings
  - Access to the system(s)
- Collaboration: Work closely with users, process owners, and ITSM stakeholders to validate learning content, Learning and HR to ensure alignment for e-learning standards.
- IT Technologies:
  - ServiceNow® (ITSM processes), JIRA/Confluence;
  - Articulate software, which includes Articulate Storyline, for creating interactive learning content;
  - Moodle LMS;
  - SQL developer (Oracle);
  - Crystal Reports/Power BI.
- Undertaking other support tasks as necessary.

Profile G: Application Management

The Operations Unit (OPU) is responsible for the 24/7 operational management of Justice and Home Affairs (JHA) information systems and services entrusted to eu-LISA, with a view to ensuring uninterrupted systems availability and high-level performance for the EU's JHA community. To that end, OPU staff monitors the operation and performance of JHA systems on a 24/7 basis and provides round-the-clock end-user support via a dedicated service desk, while also performing stand-by duty at the backup site (BCU) in Austria.

To ensure high-level performance and high-quality services, OPU coordinates eu-LISA's operational resolution processes related to incidents and problems, while also providing technical support and expertise for systems maintenance.

The unit comprises the Operations Services Centre (OPSS) and the Solutions Operations and Maintenance Sector (SOMS).

The **Solutions Operations and Maintenance Sector (SOMS)** is responsible for providing second-level support for JHA systems and solutions, in particular applications and databases, to ensure high-level system performance as per respective Service Level Agreements (SLA). To that end, SOMS is tasked with investigating and resolving incidents and problems that affect service-level quality or could potentially disrupt operations. Through its service owners, SOMS oversees the entire lifecycle of the solutions in operation, ensuring that all services are delivered in compliance with service-level agreements and performance targets.

As process owner, SOMS is responsible for the following processes: problem management, capacity management, availability management, and service level management. Under the service level management

process, SOMS is responsible for ensuring the proper support and maintenance of solutions by contractors, in particular TOF Lot 1.

Working closely with other Units under the Digital Solutions Operations Department, SOMS contributes to release management and operational change management processes overseen by the Transition and Automation Unit (TAU).

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- Develop and enhance internal tools to improve efficiency and visibility:
  - Analyse existing manual or semi-automated processes and propose technical improvements.
  - Design, develop and maintain small-scale tools or scripts aimed at automating recurring operational tasks.
  - Contribute to the development of dashboards or reporting mechanisms to improve visibility over business and technical activities.
  - Depending on the selected topic, technologies involved may include:
    - Scripting languages and automation (e.g. Bash, Python, Ansible)
    - SQL and database systems (e.g. Oracle, Postgres, Elasticsearch)
    - Orchestration Platform (e.g. OpenShift)
    - Version control systems (e.g. Git)
    - Advanced interaction with middleware or application environments (e.g. WebLogic, Linux-based systems)
- Facilitate information sharing and stakeholder cooperation:
  - Support coordination with internal stakeholders (e.g. business teams, technical teams, operations).
  - Contribute to structured information exchange and documentation updates following meetings or technical activities.
  - Assist in preparing technical or operational presentations for internal audiences.
- Contribute to daily operational and business support activities:
  - Support document lifecycle management (drafting, updating, structuring and version control of technical and operational documentation, procedures and guidelines).
  - Contribute to the analysis and optimisation of internal workflows and operational processes, identifying opportunities for simplification and standardisation.
  - Assist in the preparation of reports, dashboards and internal briefings related to sector activities.
  - Support knowledge management initiatives to ensure continuity, traceability and accessibility of information.
- Contribute to additional sector support tasks:
  - Provide ad hoc technical or operational assistance as required, in line with sector priorities.
  - Support testing, validation or small-scale deployment activities related to internal tools or improvements.
- Undertaking other support tasks as necessary.

Profiles H, I and J

The Technology and Software Engineering Unit (TSU) is responsible for overseeing the successful technical implementation of all large-scale IT systems and solutions entrusted to eu-LISA. To support increasing eu-LISA's ownership of software development, TSU is responsible for implementing the Software Factory (SoFa) approach

to ensure better consistency, scalability and quality in the development and evolution of software applications for the EU's JHA domain.

As eu-LISA's internal SoFa hub, TSU provides a standardised pipeline for agile and iterative software development, together with a framework of tools and practices covering the entire software development lifecycle (SDLC) to streamline production and accelerate delivery, while also ensuring consistency, scalability and quality across projects. This task includes overseeing continuous improvement by capturing proven best practices and reusable assets, enabling teams to build upon accumulated knowledge. In this role, TSU provides 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 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.

The unit comprises the Solutions and Architecture Design Sector (ARCS), the Software Development Sector (SODS), the Continuous Software Delivery Sector (CSDS) and the Solutions Quality Assurance Sector (SQAS).

Profile I: Software Delivery Engineering

The **Continuous Software Delivery Sector (CSDS)** is responsible for the design, implementation, and the maintenance of eu-LISA's software delivery pipeline. This includes automating the build and deployment of software solutions, as well as selecting and integrating appropriate tools for continuous integration (CI) and continuous delivery (CD).

In this role, CSDS drives deployment readiness by ensuring that the software is always in a deployable state and that deployments are predictable and repeatable. To improve efficiency, speed and reliability, CSDS is committed to continuous optimisation of the delivery pipeline and drives the continuous improvement of software delivery practices across the Agency. Additionally, CSDS drives DevSecOps best practices to integrate security checks and practices throughout the software delivery pipeline.

To ensure smooth and continuous delivery of software releases, CSDS collaborates with other key teams across the Agency, in particular with TSU's Software Development Sector (SODS) to integrate code changes and build results. To ensure reliable deployments, CSDS works closely with teams under the Digital Solutions Operations Department, in particular Solutions Operations and Maintenance Sector (SOMS) under the Operations Unit (OPU) and partners with Platform and Infrastructure Unit (PIU) teams on issues related to infrastructure and platform management.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- Team Collaboration: Work with DevSecOps experts in a constructive and positive environment.
- Learning DevSecOps methodology: Become familiar with DevSecOps tools (RedHat Openshift, Gitops, Kafka, Service Mesh, Sonarqube, Artifactory, Jenkins, Github, Ansible) and understand their added value and limitations.
- Assisting in DevSecOps Execution: Execute and Configure CI/CD pipelines, help during troubleshooting.
- Compiling documentation: Help maintain and organize documentation for CI/CD pipelines, development environments, automations.
- Undertaking other support tasks as necessary.

Profile J: Software Quality Assurance

The **Solutions Quality Assurance Sector (SQAS)** is responsible for conducting comprehensive testing for all software solutions and integrating services for all IT systems developed and managed by eu-LISA.
SQAS is responsible for overseeing the testing process in its entirety, from requirements verification, test planning and design to test execution, risk assessment, defect management and test support, thereby verifying and validating the quality of systems and services entering into operation. This is done in close collaboration with respective contractors, as well as product owners and project managers in the Programme and Solutions Management Unit (PMU), based on approved requirements and change requests. In addition, SQAS offers continuous support to stakeholders in their individual testing activities, e.g., Member States during national system test campaigns.
Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- Assist in test case execution: execute pre-written test cases and document results;
- Bug reporting: identify and report software defects clearly;
- Test documentation: help maintain and organize test documentation;
- Basic pest planning: assist in creating simple test plans;
- Learning test tools: become familiar with basic testing tools;
- Team collaboration: work with quality assurance engineers and developers in a constructive and positive environment;
- Undertaking other support tasks as necessary.

Profile K: Project Administration Support

The **Programme and Engineering Department (PED)** oversees the development, technical implementation and evolution of all information systems and digital solutions entrusted to eu-LISA in the Justice and Homa Affairs area, as the SIS, VIS, Eurodac, EES, ETIAS, e-CODEX, JITs CP, ECRIS as well as various Interoperability components, in compliance with the respective legal basis and stakeholder requirements. The department oversees the solutions development lifecycle from planning and design to development, testing and validation, ensuring that all evolutive releases and new systems are fit for purpose and are developed in an efficient way, within the timeline, budget and scope agreed.
The department comprises two units and one sector: 1) The Programme and Solutions Management Unit (PMU) in charge of programme and project management and coordination 2) the Technology and Software Engineering Unit (TSU) in charge of the actual software development and testing of the IT solutions and 3) the **Project Practices and Methodologies Sector (PPMS)** responsible for facilitating the implementation of all projects, in an agile and efficient manner, through appropriate practices and governance.
Under the supervision of a Tutor, you are expected to support the Head of Department as well as the PPM sector as needed in the following transversal tasks:

- Supporting the quality checks and assessments of ongoing or closed projects;
- Processing documentation and keep it aligned with internal standards, relevant internal processes and the needs of the department;
- Supporting basic financial planning and monitoring as well as preparation of simple financial summaries with regards to the financial resources allocated/ consumed within the projects' implementation;
- Providing support with the extraction and collection of data from different sources. Assist in the analysis, structuring and presentation of data;

- Helping in the collection of lessons learned and in the follow up of agreed action plans in relation to the Department's work;
- Perform various communication tasks within and beyond the department in accordance with the above duties;
- Undertaking other support tasks as necessary.

Profiles L and M

The Programme and Solutions Management Unit (PMU) is responsible for the management of all programmes addressing the implementation of all IT systems entrusted to eu-LISA in the EU's Justice and Home Affairs (JHA) domain; the latter includes the evolution of all existing JHA information systems under the Agency's scope. In this capacity, PMU operates in compliance with the respective 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. This entails close collaboration with practically all eu-LISA subdivisions, in particular the sectors under the Programme and Engineering Department's Technology and Software Engineering Unit (TSU). To ensure seamless engagement and business understanding of stakeholders needs, PMU collaborates closely with the Business Relations Management Sector (BRMS) under the Business and Stakeholder Relations Unit. In the process of development and delivery, PMU and TSU are 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. When it comes to reporting on the implementation of IT programmes and projects, respective PMU programme and project teams deliver regular progress reports and status updates to the Agency's governance bodies (i.e., Advisory Groups, Programme Management Boards, eu-LISA Management Board), and also to the EU Institutions.

PMU comprises three sectors: Home Affairs Programmes Sector (HAPS), Justice Programmes Sector (JUPS) and Interoperability Programmes Sector (IOPS).

Profile L: IT Project Support (Home Affairs domain)

The **Home Affairs Programmes Sector (HAPS)** is responsible for the management of all programmes addressing the implementation of IT systems entrusted to eu-LISA in the EU's home affairs domain, including the evolution of existing IT systems operating in that domain. In this role, HAPS operates in compliance with the respective legal bases, as well as stakeholder expectations and milestones agreed at the political level.

In the EU's home affairs domain, HAPS manages programmes for the EU's IT systems supporting the areas of internal security, border control, visa, migration and asylum: SIS, VIS, Eurodac, EES, ETIAS (incl. web services) that make up the cornerstones of the Schengen area and the new JHA interoperability architecture. This includes their recast and revised versions, as well as evolutions stemming from Screening Regulations and the EU's Artificial Intelligence Act.

As for new initiatives, HAPS manages the programmes for the EU's visa application platform (EU VAP) and the central router for police cooperation (Prüm II). Going forward, HAPS will also manage all programmes for the development of new solutions and products entrusted to eu-LISA in the EU's home affairs domain.

All HAPS programmes and projects are managed by dedicated programme and project teams who coordinate all activities related to the delivery and evolution of both new and existing IT systems managed by eu-LISA. In this role, HAPS teams provide leadership and coordinate the work of cross-functional eu-LISA teams to ensure successful delivery of systems and releases. As per statutory requirements, HAPS teams are also responsible

for delivering regular progress reports and status updates to the Agency's governance bodies (i.e., Advisory Groups and Programme Management Boards) on the implementation of their respective programmes and projects.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- 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 internal stakeholders: You will communicate with all solution-related parties, developing a communication system for instant feedback. You will also collaborate with architects to derive project requirements documents;
- Undertaking other support tasks as necessary.

Profile M: IT Project Support (Justice domain)

The **Justice Programmes Sector (JUPS)** is responsible for the management of all programmes addressing the implementation of IT systems entrusted to eu-LISA in the EU's justice domain, including the evolution of existing IT systems operating in that domain. In this role, JUPS operates in compliance with the respective legal bases, as well as stakeholder expectations and milestones agreed at the political level.

In the EU's justice domain, JUPS manages programmes for the EU's IT systems supporting cooperation between national and other relevant authorities in cross-border judicial proceedings. Currently, eu-LISA is responsible for the operational management of the following systems: European Criminal Records Information System reference implementation (ECRIS RI) and the e-CODEX system. In addition, JUPS is developing the ECRIS supplement for third-country nationals and stateless persons (ECRIS-TCN), together with the Joint Investigation Teams (JITs) collaboration platform for facilitating cross-border investigations and prosecutions. Going forward, JUPS will also manage programmes for the development of new solutions and products entrusted to eu-LISA in the EU's justice domain.

All JUPS programmes and projects are managed by dedicated programme and project teams who coordinate all activities related to the delivery and evolution of both new and existing IT systems managed by eu-LISA. In this role, JUPS teams provide leadership and coordinate the work of cross-functional eu-LISA teams to ensure successful delivery of systems and releases. As per statutory requirements, JUPS teams are also responsible for delivering regular progress reports and status updates to the Agency's governance bodies (i.e., Advisory Groups and Programme Management Boards) on the implementation of their respective programmes and projects.

Under the supervision of a Tutor, you are expected to contribute to the following tasks:

- 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;
- Undertaking other support tasks as necessary.