Opportunity for an Information Security & Risk Analyst

Join the dynamic and multicultural team behind one of the largest top-level domains in the world, .eu (also available as .ею and .ευ).

Our human-sized, tech-oriented, not-for-profit organization is dedicated to managing, operating and promoting the .eu TLD with a mission to provide high-quality, secure, and accessible services to millions of users across the EU and beyond. Operating .eu, since its creation in 2003, EURid has built a very strong technical expertise in the top-level domain industry.

We are seeking an Information Security & Risk Analyst to strengthen our Security Office. As an Information Security & Risk Analyst working in EURid's Belgium (Diegem) office, you will contribute to implement and maintain security processes, take ownership of IT asset lifecycle management, and ensure compliance with relevant frameworks and regulations, including ISO/IEC 27001, 22301 and NIS2. Directly reporting to EURid's Security Officer this position is ideal for someone with a solid grounding in information security, ready to take ownership of operational responsibilities, contribute to strategic initiatives, and ensure efficient, secure, and sustainable management of IT assets.

Key responsibilities:

- Support the Security Officer in the development, implementation, and maintenance of the organization's information security program (ISMS).
- Contribute to ISO/IEC 27001 implementation and maintenance, including security controls, policies, procedures, and continuous improvement activities.
- Maintain a high-level understanding of NIS2 requirements and support alignment of internal security processes with regulatory expectations.
- Support the implementation of information security and risk management processes and standards across IT.
- Participate in risk assessments, audits, and internal reviews to support compliance and security assurance activities.
- Collaborate closely with enterprise architecture, software development, system operations and internal IT teams to align projects with security principles and support operational security tasks.
- Take ownership of IT asset lifecycle management from procurement to retirement and IT supplier management, with support from the Security Officer and IT leadership and system operations, ensuring cost efficiency, security compliance, and sustainability.
- Maintain and update the CMDB / asset register, ensuring data accuracy and proper classification of information assets.
- Monitor and report on recurrent security tasks, including control plan execution, patch management, security configuration, quality control execution, exception management…
- Support security awareness initiatives across the organization, building a strong security culture.
- Report regularly on risks, issues, and corrective actions.
- Document security procedures and processes, ensuring consistency and clarity.
- Stay current with emerging threats, technologies, and regulatory changes to provide relevant input to the Security Office.

Qualifications:

Education & experience:

- University degree in Information Security, Computer Science, Information Systems, Engineering, or a related field, or equivalent professional experience.
- 2-4 years of professional experience in information security, GRC, SecOps, or a related field.
- Security related certifications (e.g., ISO 27001 Lead Implementer, …) is a plus.

Technical proficiencies:

- Knowledge of ISO/IEC 27001, and its practical implementation as well as NIS2 Directive, and Cybersecurity Fundamentals.
- Experience supporting regulatory compliance or audit activities.
- Experience with security process design and implementation in operational environments.
- Understanding of IT infrastructure, networks, and application development practices (DevOps experience is a plus).
- Willingness to take ownership of IT asset procurement, supplier management, and lifecycle management.
- Understanding of identity and access management concepts in Microsoft Active Directory and Microsoft 365 environments.
- Prior exposure to security automation or monitoring tools is a plus.
- Experience with the Atlassian tool stack (Jira, Confluence, Jira Service Management) for issue tracking, documentation, and service workflows is an advantage.

Soft Skills:

- Strong communication and stakeholder management skills, with the ability to build effective relationships across teams and with external parties.
- Strong organizational skills and attention to detail.
- Ability to work collaboratively in a cross-functional team environment.
- Good communication skills in English.

What we offer:

- A dynamic and international work environment.
- A competitive compensation package that includes a competitive salary, a company car, meal vouchers, a comprehensive group and health insurance plan and additional holidays.
- Healthy work-life balance including hybrid work.
- Opportunities for growth and development.
- A role that supports a high-impact, high-visibility European digital initiative.

You will join a highly skilled, mission-driven team working on projects that matter for Europe's digital future. So don't miss this exciting opportunity to take your information security career to the next level and help build the future of the Internet in Europe.

Send your details or contact us via jobs[at]eurid[dot]eu