Security, Risk & Compliance (SRC) Analyst
40 hours/week

Are you an experienced Security, Risk & Compliance (SRC) Analyst and currently looking for a new challenge? Would you like to work in a socially responsible industry? At Digidentity you're at the right address. We're looking for a Security, Risk & Compliance (SRC) Analyst to join our team immediately.

The Security, Risk & Compliance (SRC) Analyst at Digidentity is tasked with maintaining Digidentity information security policies, processes and procedures and implementing them within Digidentity. The SRC Analyst will translate and communicate compliance requirements between SRC and other stakeholders within Digidentity. Furthermore, the SRC Analyst will assist in various assessments and consult on remediation actions.
The SRC Analyst will work in cross-functional capacity to extend the communication capabilities of SRC to other stakeholders within Digidentity. The SRC Analyst will work together with and reports to the Chief Security Officer (CSO).

About Digidentity

Everybody should be able to identify, authenticate and authorize themselves online in a simple and secure manner. That is our mission! Digidentity develops and provides solutions for secure digital communication between individuals, companies and Governmental agencies.
For this purpose, we are continually developing new services and improving existing ones, such as 'Virtual Smartcard Technology'. This is to provide a unique digital identity, which a user keeps complete control of.

Digidentity is specialized in the delivery of certificates, authentication services and digital signatures. We work on systems which are currently being used by millions of users.

What can you expect?

- Monitor, perform or participate in information security assessments, tests, reviews and audits (internal and external);
- Oversee remediation of deficiencies identified in reviews, assessments (self- and automated) and audits (internal and external);
- Monitor current threats and trends and determine their possible impact including communication to relevant stakeholders;
- Define the Digidentity information security policies;
- Document and deploy security training specific to Digidentity (e.g. PKI);
- Define and implement processes and procedures linked to information security;
- Ensure the quality of information security assessments, tests, reviews and audits;
- Inform the CSO about information security status and incidents and present improvement proposals;
- Contribute to forensic investigation;
- Test elements of the information security incident, response and/or continuity plan;
- Articulate information security needs of Digidentity into concrete security measures.

- Support the CSO with identification of newly identified IT risks and issues;
- Analyze IT risks and issues including rating, periodic reporting, tracking, and validation of IT controls effectiveness;
- Ensure cross-department collaboration and communication to ensure appropriate processes, procedures and tools are installed, monitored, and effectively operating and alerting;
- Ensure adequate registration, analysis and reporting of information security incidents;
- Participate in vulnerability and penetration assessments, monitor endpoint protection solutions and tools;
- Maintain compliance baseline and participate in enforcement of compliance baseline;
- Participate in creation and maintenance of security documentation to meet compliance requirements;
- Document and conform to processes related to security monitoring and detection;
- Interface with technical personnel and other teams as required.

What do we expect?

- Experience in performing assessments and reviews;
- 5+ years of experience in Information Security;
- Experience with Electronic Identification and Public Key Infrastructure;
- Experience with analyzing and accurately documenting processes and procedures;
- Capable to analyze various information security standards, frameworks and regulations;
- Able to execute risk assessments and implement remediation plans;
- Experience in detail orientation, research, compilation, and reporting on data;
- Experience working effectively as a member of a cross-functional team;
- Able to prioritize own workflow;
- Ability to handle multiple priorities on tight deadlines without compromising quality.

Knowledge and Experience required

We will welcome contact from you if you can meet these criteria:

- Bachelor's Degree in Information Technology or equivalent required;
- CISSP, CISA or CISM information security certification required (or equivalent);
- Knowledge of information security design concepts and principles;
- Expertise and advanced consultative skills including building collaborative relationships;
- Excellent interpersonal, written and verbal communication skills;
- Knowledge of IT regulatory requirements (e.g. GDPR and eIDAS regulations);
- Knowledge of IT control frameworks (e.g. ISO, ETSI, COBIT or NIST frameworks);
- Knowledge of IT infrastructure and security;
- Self-motivated and comfortable with working in a close knit team;
- Fluent in both English and Dutch.

Interested? Send your motivation and your CV to recruitment@digidentity.com with the subject "*Security, Risk & Compliance (SRC) Analyst* & Your Name". For questions regarding this position you can call Paul van Os on +31 6 51 57 82 90.