Informatikai termékek és elektronikus információs
rendszerek biztonsági értékelése
https://www.valilab.hu

jelentkezés: info@valilab.hu

VALILAB Kft.
IT Biztonsági Vizsgálólaboratórium

Keresünk jelentkezőket az alábbi munkakör jövőbeli betöltésére:

CYBERSECURITY AUDITOR (Kiberbiztonsági vizsgáló)

Előnyös személyi tulajdonságok egy auditori / értékelői munkához:

- Jó megfigyelő/érzékelő képesség
- Magabiztosság, egyúttal diplomatikusság
- Határozottság, egyúttal rugalmasság
- Etikus viselkedés
- Titoktartási képesség

Az egyetemi oktatásban megszerzett minden (az informatikához és az informatika biztonsághoz kapcsolódó) ismeret hasznos alap lesz.

A konkrét értékelési módszerek csoportos munka közben elsajátíthatók.

A kiberbiztonsági vizsgálókhoz kapcsolódó rész az ECSF-ből
(European Cybersecurity Skills Framework,
https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles):

Profile Title	Cybersecurity Auditor
Alternative Title(s)	Information Security Auditor (IT or Legal Auditor) Governance Risk Compliance (GRC) Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst
Summary statement	Perform cybersecurity audits on the organisation's ecosystem. Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.
Mission	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.
Deliverable(s)	• Cybersecurity Audit Plan • Cybersecurity Audit Report
Main task(s)	• Develop the organisation's auditing policy, procedures, standards and guidelines • Establish the methodologies and practices used for systems auditing • Establish the target environment and manage auditing activities • Define audit scope, objectives and criteria to audit against • Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests • Review target of evaluation, security objectives and requirements based on the risk profile

Profile Title	Cybersecurity Auditor
	• Audit compliance with cybersecurity-related applicable laws and regulations • Audit conformity with cybersecurity-related applicable standards • Execute the audit plan and collect evidence and measurements • Maintain and protect the integrity of audit records • Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports • Monitor risk remediation activities
Key skill(s)	• Organise and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques • Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls • Decompose and analyse systems to identify weaknesses and ineffective controls • Communicate, explain and adapt legal and regulatory requirements and business needs • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent
Key knowledge	• Cybersecurity controls and solutions • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Conformity assessment standards, methodologies and frameworks • Auditing standards, methodologies and frameworks • Cybersecurity standards, methodologies and frameworks • Auditing-related certification • Cybersecurity-related certifications
e-Competences	Testing Documentation Production Risk Management Quality Management