Senior Cyber Resilience Professional:
Do you want to change your career by being a key member in a new Cybersecurity Company bringing fresh thought and innovative ideas?

For those who come on board, we offer significant career advancement, big challenges and a runway for positive growth.

CYBERFLIP SA (www.cyberflip.eu) provides state-of-the art Cybersecurity Consulting Services in the following domains:

- Cyber Security Office as a Service
- Cyber Risk Management
- Cybersecurity Framework Design and Implementation
- Cyber Resilience, Incident Response and Crisis Management
- Maturity assessments
- Compliance Services and IS/IT Certification preparation
- Technical Security Assessments
- Cyber Security Awareness Trainings

…and more to come…

Our main differentiating points are:

- We provide industry-specific services, tailored to each Organization's unique requirements, needs and budget.
- We are bridging the gap between technology and business objectives. Through our techno-economic approach, we guide the Organization to implement cost-effective security controls targeting the maximum possible ROI.
- We prioritize the recovery and response capability of the Organization through specialized Incident Response and Recovery playbooks and Crisis Communication Plans, involving all necessary functions (Tech, Business, Legal, Executive, Externals)
- We are always applying the latest international good practices combined with our professional industry experience – we have been on the other side!

Responsibilities

- Design and implementation of programs to improve Cyber Resilience through Incident Management, Crisis Management, Disaster Recovery and Business Continuity.
- Translate cybersecurity risk into business risk through Cyber Risk Quantification
- Identify risks, propose, design and implement controls in order to ensure an effective and secure Information Security Governance and Risk framework, tailored to Customers needs and budget.
- Design and conduct Cyber Maturity assessments
- Integrate modern security trends into traditional approaches to address real security challenges
- Design and Implementation of data protection and privacy programs

Requirements:

- Bachelor's Degree in Computer Science or Information Security fields (Master's degree in Information Security would be considered an asset)
- At least 3-4 years hands-on experience in Information Security domain focusing on Risk Management, Incident Management and Cyber Resilience.
- Experience on design and implementation of Cybersecurity and Risk Management frameworks utilizing globally accepted good practices and frameworks, such as COBIT, ISO2700X, NIST, ISO 22301, ISO 31000, ISO 20000 etc. Experience in Risk quantification methods will be considered a plus.
- Experience in security operations, i.e. incident handling, vulnerabilities management and incident reporting;
- Knowledge of current and modern security technology trends (zero trust, cloud security, AI) and experience in their adoption as to address real security challenges.
- Strong problem solving and communication skills
- Commitment to teamwork and able to demonstrate strong client relationships
- Ability to maintain professionalism and strive for high ethical standards at all time
- Demonstrated ability to write clearly, succinctly, and in a manner that appeals to a wide audience (in both Greek and English)
- One or more Information Security related certifications is considered an asset. Indicatively: ISO 27001:2013 LA, ISACA and/or ISC2 certifications

Benefits

- Competitive remuneration package
- A challenging job in a fast developing company;
- Friendly work environment where you can thrive, develop your skills and see your ideas become real practice
- Continuous learning and training opportunities
- Career advancement possibilities