Cyber Information Security Officer

Niveau : Intermediate
Activité : Group
Bureau : Geneva

If you are passionate about meeting client needs, want to challenge the status quo and be part of an innovative environment and future, the Syz Group can bring you what you are looking for. Working at Syz takes a blend of collaboration, entrepreneurial spirit and willingness to pull together. In return for your talent and dedication, you can expect a fast-paced, stimulating work environment, a flat hierarchy with direct access to senior leaders, a culture hungry for innovation and the opportunity for your voice to be heard and your ideas to be listened to.

Do you have a key interest and demonstrable experience in Information Security with expertise in Cyber Security?

We are currently looking for a Cyber Information Security Officer to join our Security department and reporting tothe Chief Security Officer (CSO). The incumbent will be responsible for enforcing policies and procedures, ensuring protection for our organization's information system from all forms of security breaches or cyber-attacks from both outside and inside the organization.

She/He will ensure compliance of our cyber security framework working with our Information Technology and Cyber security teams and will be mainly operating as 2nd line of defense.

Responsabilités principales

- Review and monitor the organizational security compliance against current frameworks and regulation (FINMA 2023/1, NIST, LPD and ISO 27001)
- Provide key inputs and collaboration with various risk/compliance departments (i.e., Quality Management, Data Integrity, Ethics & Compliance, Cyber Security, Privacy/Legal, Records Management)
- Provide subject matter expertise to Contract Managers, Business Unit Managers, and third-party relationship Managers to ensure third party risk management program is compliant with applicable regulations or policies
- Contribute to develop, maintain, and publish up-to-date information security directives, procedures, standards, and guidelines
- Develop and ensure effective disaster recovery policies and standards to align with enterprise business continuity management program goals
- Perform internal investigations, forensic investigations and assist with any inquiry related to the usage of our data
- Collaborate in insider threat prevention activities, such as performing or evaluating background checks on individuals when required
- Provide regular reporting on the status of the information security program
- Actively participate in security, data management, forensic investigations, and security Governance
- Monitor or ensure the oversight external threat environments for emerging threats
- Plan and oversee penetration tests to find any flaws
- Collaborate with management and the IT departments to improve security
- Document any security breaches and assess their damage
- Educate colleagues about security software and best practices for information security
- Collaborate and maximize partnership with external providers
- Assess whether new technologies are appropriate for the company to implement
- Ensure technologies currently in use are efficient and propose/make changes wherever necessary
- Maintain/develop network and relationship with pairs in the industry and with local companies

Profil

Professional experience & competencies:

- 5-7 years' experience in information security of which at least 2 years in a similar role within the Swiss finance industry (banking industry an asset)
- Strong understanding of Microsoft Cloud technologies, especially Azure and Office 365 with successful track record of min. 2 years
- 1 year experience on operating Data Loss Prevention technologies (Purview and or Forcepoint)
- Good knowledge of IT production frameworks such as ITIL as well as technological trends
- Solid knowledge of various information security frameworks (NIST, CIS…)
- Ability to conduct technological analyses and research
- Good knowledge in mobile technologies and change management
- Good understanding of Private Banking sector and of FINMA operational risk framework

Personal competencies:

- Excellent problem-solving and analytical skills
- Good communication skills with the ability to popularize security matters to a non-technical audience and to educate them
- Result, client solution and team oriented
- Ability to maintain excellent quality standards in high stress situations
- Excellent problem-solving and analytical skills with the ability to balance business interests with risk
- Organization, rigor and attention to details

Language requirements:

- Excellent verbal and written command in French and English, German an asset

Education:

- Bachelor's degree in computer science, Management or equivalent
- Current relevant professional certification such as CISSP, Microsoft Azure, Microsoft 365

Specific requirements:

- **Mandatory Swiss residency** (for the last 12 months at least)