Information Security Officer

- Experience level : Intermediate
- Activity : Group
- Office : Geneva

-
  - Tweet
  - Share
  - Share
  -
  -
-
-

The Information Security Officer (hereinafter ISO) reports to the Chief Security Officer (CSO) and is responsible for implementing and controlling information systems security processes, working actively with the CSO on the management of Information Security related projects according to SYZ Cybersecurity strategy, supporting Business lines and IT department in cybersecurity aspects of various projects within the bank as well as ensuring technology monitoring and regulatory watch of the Group's information systems security.

Your missions

Key responsibilities

The ISO has operational responsibility for verifying the effective enforcement of the Information Systems Security Policy (ISSP), more particularly:

- Implementation of controls and concrete action plans, defined by the CSO to mitigate or address cybersecurity related risks, including :
  - Track regulatory and technical changes to ensure that the ISSP is in line with the latest trends
  - Monitor the necessary updates to guarantee the overall logical and physical security of the information systems
  - Keep up with technological changes that may have an impact on threats and the means of protecting information systems
- Monitoring of effective implementation of the agreed action assigned to business lines or to IT department
- Ongoing surveillance of the relevance and adequacy of security measures related to these action plans
- Prevention of risks related to the information systems from the early stages of development of any project involving these systems. Under CSO supervision, coordination of security activities of delegated functions such as TISO (Technical Information Security Officer) and operations teams. As permanent member of the Security Committee, active participation to its preparation and to the application of actions decided by the committee
- Support to the CSO for the reporting of information security incidents and other events influencing SYZ cybersecurity framework

Main activities

- Technology intelligence and foresight:
  - Track regulatory and technical changes to ensure that the ISSP is in line with the latest trends
  - Monitor the necessary updates to guarantee the overall logical and physical security of the information systems
  - Keep up with technological changes that may have an impact on threats and the means of protecting information systems
- Diagnosis and analysis of risks related to the security of information systems:
  - Choose an appropriate risk analysis methodology for the information systems security environment
  - Assess risks based on threats to the information systems security, the impacts, and consequences of these threats
- CSO support in definition and application of the Information Systems Security Policy (ISSP):
  - Collect ISSP stakeholders (Executive Committee, CSO, IT, etc.) input as part of Business objectives to be achieved by the policy.
  - Implement ISSP related security standards under Information Security team responsibility and supervise the ones assigned other departments.
- Employee training and awareness-on IT risks and security issues.
- Manage the IT controls portfolio:
  - Review periodically security and IT controls catalogue to reduce the Group's operational risk.
  - Execute cybersecurity related controls to be done by Information Security team and supervise the ones assigned other departments.
  - Implement appropriate action plans for the remediation of any anomalies detected by the controls.
- Projects and assessments:
  - Information Systems Security Project Manager
  - Responsible for the security aspects of business and IT projects
  - Assist CSO while conducting risk assessments for projects and initiatives
  - Propose security concepts for some IT and business projects

Your profile

Professional experience

- Bachelor's degree in computer science or equivalent
- Advanced training and 5 years' experience in information systems security (ISS)
- Certifications in ISS (CISSP, CISA, CISM) highly appreciated
- Technical executive with proven experience in project management and complex security concepts

Professional competencies

- Knowledge of technical concepts and security mechanisms:
  - Knowledge of technical concepts and security mechanisms:
  - System and network architecture concepts and techniques
  - Operating procedures and data exchange standards
  - Knowledge of operating systems and related programming languages
  - Application functionalities, in particular, the authorization and data access principles
  - Security of database management systems
- Technical expertise as an IS architect and a thorough knowledge of the processes
- Knowledge of ISO 2700x security and ISO 3100x risk management standards

- Experience in managing organizational and technical projects
- Knowledge of the regulatory texts applicable to the banking sector, in particular, the FINMA circulars dealing with the security of information systems, data protection and operational risk

Personal competencies

- Demonstrated ability to balance business interests with risk
- Ability to anticipate
- Ability to manage resources (budget, consultants, systems, etc.)
- Ability to organize and lead change
- Ability to deal with crisis situations
- Good writing skills in French and English (ability to conceive and document clear governance principles)
- Teaching and communication skills (ability to lead working groups, awareness raising and training sessions)
- Results focused, with the energy and commitment to drive delivery
- Rigor and attention to details
- Solution-oriented
- Curiosity: technological changes are frequent. The CISO must have an interest in all areas (applications, programming languages, hardware, virtualization, operating systems) because security is a cross-disciplinary issue

Language requirements

French mother tongue with good level in English

Apply for this position

If this position is of interest to you, send us your complete application by filling in the Internet form.

Apply online Return to job offers

Why join us?

- Find out more

Follow us on LinkedIn

- See more