**Job Description Cyber Security Manager**

As one of the world’s leading and largest graduate business schools, INSEAD brings together people, cultures and ideas to change lives and to transform organisations. A global perspective and cultural diversity are reflected in all aspects of our research and teaching. With campuses in Europe (France), Asia (Singapore) and the Middle East (Abu Dhabi), INSEAD’s business education and research spans three continents.   
  
The primary role of Cyber Security Manager is to drive, implement and maintain INSEAD’s cybersecurity management program to ensure information assets are adequately protected. He or she is also responsible for identifying, evaluating, reporting and mitigating information security risks in a manner that meets regulatory and compliance requirements. This role requires close liaison with business units to implement security best practices that meet defined policies and standards for information security. He or she will also oversee a variety of IT-related risk management activities and cybersecurity projects.   
  
The ideal candidate is an up and coming Cyber Security professional, a consensus builder, and an integrator of people, technologies, data and processes. The position holder must be able to coordinate disparate priorities & constraints while maintaining the balance between security control and technology enablement of business activities.   
  
Main Accountabilities

* Formulating information security goals and establish policies, standards and procedures in line with the school’s overall cyber security strategy.
* Implementation of a strategic comprehensive information security and IT risk management program, driving towards ISO 27001 certification by 2021.
* Manage the school’s information security organization, consisting of a direct report and about 20 project assigned reports. This includes training, staff development and annual performance reviews for the direct report(s).
* The position holder facilitates the IT Security Steering Committee meetings.
* Develop, maintain, publish and control the adherence to up-to-date information security policies, standards and guidelines. Oversee the approval, training, and dissemination of security policies and practices to about 1000 employees, and about 1400 students globally.
* Development and execution of the school’s overall cybersecurity strategy. Identify emerging trends in the industry and establish strategic guidance related to best practices in cybersecurity.
* Implementation of a strategic comprehensive information security and IT risk management program based on ISO 27001 standard. This includes work with IT teams to ensure implementation of security controls in software development life cycle and new technology adoption. This include discussions with technical leads, to ensure alignment across the security, technology and business architectures.
* Work directly with the business units to facilitate IT risk assessment and to determine acceptable levels of residual risks.
* Develop the culture of appropriate cyber security risk assessment and risk acceptance across from stake holders to end users and IT professionals. Lead the implementation, development, training and awareness for information security.
* Provides regular reporting on the status of the information security program to the Executive Committee and the Board of Directors as part of the enterprise risk management program.
* Manages security incidents and events to protect INSEAD’s IT assets, including intellectual property, regulated data and the school’s reputation.
* Monitors the external threat environment for emerging threats and provides recommendations for appropriate courses of action.

Experience

* Bachelor’s Degree in Information Systems/Computer Science of equivalent
* More than 10 years of technical experience, with at least 3 years in related fields (IT Risk management, IT Audit and IT Security management).
* Certifications in CISSP, CISA, CISM, C-CISO preferred
* Excellent knowledge of ISO 27001 and COBIT
* Good understanding of ITIL, NIST, data security standards, personal data protection laws of Europe (GDPR), and Singapore is an advantage.
* Excellent up to date understanding of latest Cybersecurity threats and preventive measures