CareerCross by JAC Recruitment

【新着】 Senior Cyber Security Manager

Please do not hesitate to contact us.

Job Information

Recruiter
ACS Japan

Job ID
1516683

Industry
Insurance

Company Type
Large Company (more than 300 employees) - International Company

Non-Japanese Ratio
About half Japanese

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
12 million yen ~ 15 million yen

Refreshed
January 22nd, 2025 16:44

General Requirements

Minimum Experience Level
Over 6 years

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Business Level

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

Senior Cyber Security Manager (ICAT)

【The opportunity】

- The Senior Manager, Information Risk Management Control Assurance Testing (ICAT) will play a vital role in the 2nd Line of Defense global ICAT team responsible for assessing the information risk management activities to provide independent and objective control assurance against the company's information risk appetite.

【Key Responsibilities】

- Perform information risk assurance assessments and controls testing according to the company's policies and standards, e.g. Identity and Access Management, vulnerability management, network security, application security, IT asset inventory etc.
- Provide risk management services and advisory initiatives for information and technology risks
- Collaborate with different lines of defense, subject matter expertise, to carry out assurance project planning and keep pace with both internal drivers (IRM standards and Technology processes) and external drivers (technology, regulations, risks, and control standards)
- Ensure that all assurance procedures executed are conducted in accordance with Global IRM Methodologies
- Collaborate with regional, market Information Risk Officers, Governance & Control teams to ensure process assurance of key risks and gaps identified from assurance engagements, and to define, track and report on management corrective action plans
- Develop relationships with teams across the globe, regionally, and locally, e.g. IT, Audit Services, Global Information Risk Management, Operational Risk Management, and other risk and control groups to develop integrated strategies to manage our most key areas of risk
- Commit to and contribute to the ongoing evolution of assurance processes, standardization of procedures, and continuous improvement
- Stay abreast of evolving information and technology risks, as well as new regulations, laws, and requirements for technology, information security, cybersecurity, and privacy across the company's jurisdictions

Required Skills

【Job Requirements】

- Minimum 5 years of progressive experience in the areas of Information Security / Business Resiliency / Technology Risk strategies, principles, processes, and deliverables within a large enterprise
- University degree in Risk Management, Business Information Systems, Computer Science or related discipline is preferred
- Relevant work experience in financial services and technology operations, e.g. information risk management, or audit function
- In depth knowledge of system development methodologies, cyber and network security processes, and regulatory requirements (CA OSFI, US SOX, JP FSA, HK SFC, SG MAS etc.)
- Sound knowledge of best practices of various aspects of information risk management Previous risk advisory consulting experience is preferred

【Competencies】

- Fluency in both Japanese and English, including speaking, reading, and writing
- Results oriented with a keen focus on quality and delivering value; ability to balance multiple priorities and projects; strong attention to detail while retaining focus on the "big picture" and top risks; flexible and organized with the ability to oversee multiple projects concurrently
- Strong communication, stakeholder management, and presentation skills
- Problem solving, analytical, innovative, and strategic thinker
- Ability to work independently and effectively collaborate with teammates around the globe
- Ability to quickly comprehend business processes and identify the risk implications, analyze complex situations, reach appropriate conclusions, and make value-added and practical recommendations.
- Recognized professional designations in Information Security, Audit and Business Continuity (e.g., CISSP, CISA, CISM, CEH, CRISC, FAIR)
- Demonstrated ability to work effectively in diverse environments and cultures, over multiple office locations
- Ability to identify opportunities to utilize data analytics for enhanced depth and breadth of assurance coverage

★If you have any questions or need more information, please do not hesitate to contact us.
★Jing Liu ｜E-mail: jing.liu@acsjapan.jp

Company Description