VP – Security Advisory Services

Global Firm / Up to 16M JPY

Job Information

Recruiter
Skillhouse Staffing Solutions K.K.

Job ID
1608034

Industry
Insurance

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

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
Negotiable, based on experience ~ 16 million yen

Work Hours
9:00 - 18:00 (Mon - Fri)

Holidays
Sat, Sun, National Holidays, Paid Holidays, etc.

Refreshed
August 19th, 2026 16:33

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
Technical/Vocational College

Visa Status
Permission to work in Japan required

Job Description

A Global Financial firm is seeking a **Vice President – SAS Function regional lead.** The ideal candidate will support the activities related to the Security Service Desk (SSD) as well as support the business within the SAS Japan function and collaborate closely with regional Security Advisory Services (SAS) teams.The primary focus of the role is to ensure that the Business as Usual (BAU) or Run the Bank (RTB) activities are being running in a smooth and well manner.

Responsibilities:
- Be a point of contact and perform a SAS function lead role and provide oversight on Business requests, security awareness and Third-party cyber risk assessment (TPCRM) for vendors, suppliers, and service providers
- Work with procurement, legal, regional stakeholders including resilience (TPRM) and platform teams to embed security requirements into vendor contracts
- Act as trusted Security advisor to business units and project teams, ensuring that security requirements are integrated into project/technology initiatives
- Review and assess software, network and cloud solutions for security compliance and recommend mitigation strategies where required
- Maintain strong governance on the third-party cyber risk assessment (TPCRM) process for Japan in terms of complying with regional requirements and synergy with Wealth management team
- Liaise with internal security teams such as global TPCRM, SOC, Vulnerability Management, Security Architecture, Threat Intelligence and others to enhance the overall TPCRM cybersecurity control framework
- Proactively attend and contribute to Japan TPRM Working Group meetings and participate in ServiceNow VRM implementation
- Manage regular reporting to the SAS management about the status of the third-party cyber risk assessment (TPCRM) for the Japan region
- Conduct security awareness programs on third-party cyber risks and compliance requirements
- Participate in third-party security incidents and data breaches, ensuring compliance with regulatory reporting requirements
- Support Cyber Culture and Learning initiatives (on ground activities, translation and content review) locally for Japan
- Assist in the translation of business communications / Security Reports from English to Japanese and vice a verse

Why should you apply:
- Highly diverse and inclusive team
- Exposure to global financial systems and compliance technologies
- Opportunity for high impact contribution to Nomura team
- Work under an internationally integrated organization (London HQ, Japan sub-structure)

Company Details:
Headquartered in Tokyo with offices in Hong Kong, London, and New York, it is Japan's largest securities firm, employing approximately 26,000 staff worldwide and offering a full range of equity, fixed income, foreign exchange, and other investment products and services.

Working Hours: 08:40 – 17:40
Workstyle: 5 days in office.
Benefits: Social insurance, pension, transportation, etc.
Interview Process: 1-2 round

Required Skills

- 10+ years of experience in information security, with strong experience of cyber risk management, technology risk, knowledge regulatory frameworks, risk mitigation
- In-depth understanding of information security principles, current cyber threats, and mitigation strategies, including hands-on knowledge of network security, firewall rules, cloud connectivity, and technology risk.
- Good communication skills

Company Description