Information Security Manager - Up to 16M

Working with the APAC region

Job Information

Recruiter
Skillhouse Staffing Solutions K.K.

Job ID
1607968

Industry
Insurance

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

Non-Japanese Ratio
Majority Japanese

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
10 million yen ~ 16 million yen

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

Holidays
Saturday, Sunday, National Holidays, Year-end and New Year, etc.

Refreshed
October 28th, 2026 02:00

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

A leading global insurance company is seeking an experienced **Information Security Manager** to join its APAC Information Security team and lead cybersecurity governance, risk management, and security initiatives across Japan.

You will serve as the Information Security leader for Japan, representing the Global Information Security organization locally. The successful candidate will drive cybersecurity governance, risk management, regulatory compliance, and security transformation initiatives across the business.

Responsibilities:
- Lead Information Security activities across Japan
- Represent the Global CISO function as Japan's Information Security leader
- Assess cyber risks, controls, and compliance against security frameworks and KPIs
- Provide security advisory and technical guidance to business and technology stakeholders
- Drive adoption of security policies, standards, and transformation initiatives
- Support regulatory assessments and security governance activities
- Manage security reporting, governance, and exception tracking
- Partner with executives, business leaders, and technology teams on cybersecurity matters
- Oversee security incident management in collaboration with regional and global teams
- Drive security awareness, training, and security culture initiatives

Why should you apply:
- Long term work opportunity, plus WFH available
- Straightforward, get going culture
- Flexibility working time
- Users/ team are logical and easy to change
- Great team dynamics and learning opportunity
- Opportunities to learn/brush-up English/Japanese language

Company Details:
A leading global provider of property and casualty insurance, this company is known for its commitment to innovation, diversity, and employee development. With a strong presence in over 50 countries, employees have the opportunity to work in a dynamic and inclusive environment where personal and professional growth is encouraged. The company values collaboration, integrity, and excellence, offering comprehensive training, career development programs, and competitive compensation packages. A culture of respect and inclusivity is promoted, ensuring that employees feel empowered to contribute, grow, and make a difference in their roles while helping the organization deliver world-class insurance products and services globally.

Working Hours: 9:00 - 18:00 (Mon-Fri)
Working Style: 3 days' work in office, and 2 days' work from home
Holidays: Saturday, Sunday, National Holidays, Year-end and New Year Holidays, Paid Holidays
Services/Benefits: Transportation expenses up to 20,000 yen per month, plus Paid leave, plus social insurance (health insurance, welfare pension, and work-related accident insurance), Periodic health examination, and Employment insurance

Required Skills

- Proven experience managing Information Security requirements within a global Financial Services or Insurance organization
- Strong cybersecurity leadership experience across multiple security domains
- Strong knowledge of security frameworks such as ISO 27001, NIST CSF, or similar
- Knowledge of Japanese cybersecurity regulations and regulatory expectations
- Experience in Cyber Incident Response and Incident Management
- Experience supporting security transformation and security control improvement programs
- Understanding of cloud technologies and cloud security principles
- Experience with Data Loss Prevention (DLP) controls and security governance
- Strong stakeholder management and executive communication skills
- Ability to communicate security risks effectively to technical and non-technical audiences

Company Description