IT Director, Information Security & Cyber Risk

Urgent Hiring

Job Information

Recruiter
Skillhouse Staffing Solutions K.K.

Job ID
1609218

Industry
Automobile and Parts

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

Non-Japanese Ratio
About half Japanese

Job Type
Permanent Full-time

Location
Kanagawa Prefecture

Salary
10 million yen ~ 20 million yen

Work Hours
8:00-17:00 / 9:00-18:00 No Core Time, flexible working hours

Holidays
Saturday, Sunday, and National Holidays, etc

Refreshed
August 24th, 2026 13:43

General Requirements

Minimum Experience Level
Over 10 years

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Daily Conversation

Minimum Education Level
High-School

Visa Status
Permission to work in Japan required

Job Description

A Global Insurance firm is seeking an experienced and visionary **IT Director, Information Security & Cyber Risk** to lead cybersecurity strategy, governance, and risk management across the organization.

In this highly visible leadership role, you will be responsible for establishing, implementing, and continuously enhancing enterprise information security and cyber resilience capabilities. You will play a critical role in protecting the organization's information assets, technology infrastructure, customers, and reputation while ensuring compliance with regulatory requirements and industry standards.

Responsibilities:
- Develop and execute enterprise-wide cybersecurity strategies aligned with business objectives
- Maintain and enhance information security policies, standards, and governance frameworks
- Lead cybersecurity governance forums and provide regular reporting to executive management, risk committees, and the Board
- Drive cybersecurity roadmaps, strategic initiatives, and investment planning
- Monitor emerging cybersecurity regulations and ensure timely compliance and response
- Partner closely with regional and global CISO organizations to align with enterprise cybersecurity risk management frameworks
- Assess, monitor, and report cyber risks across business operations, applications, infrastructure, and third-party environments
- Ensure effective identification, evaluation, mitigation, and tracking of cybersecurity risks
- Oversee security exception management and risk acceptance processes
- Provide executive oversight of security monitoring, threat detection, and response capabilities
- Collaborate with regional security teams to manage major cyber incidents and crisis response activities
- Ensure lessons learned from security incidents are translated into stronger controls and improved resilience
- Strengthen cyber resilience and business continuity capabilities across the organization
- Ensure ongoing compliance with applicable regulations, industry standards, and internal control requirements
- Act as the primary cybersecurity liaison for regulatory examinations and external audits
- Lead the remediation of audit findings and regulatory observations
- Provide strategic direction for secure technology architecture, cloud security, and cybersecurity engineering initiatives
- Oversee implementation of security controls across applications, infrastructure, endpoints, and networks
- Ensure security requirements are embedded throughout technology projects and digital transformation programs
- Sponsor emerging technology risk assessments, including AI and Generative AI-related security risks
- Foster a security-first culture throughout the organization
- Lead enterprise-wide security awareness and education initiatives
- Partner with business and executive leaders to strengthen cyber risk ownership and accountability

Why should you apply:
- Lead enterprise-wide information security and cyber risk strategy for one of the world's leading financial services organizations
- Gain high visibility and influence by partnering with executive leadership, regional and global CISO teams, regulators, and Board-level stakeholders
- Play a critical role in driving cybersecurity transformation, digital innovation, cloud security, and emerging technology risk management, including AI and GenAI initiatives

Company details:
Our client is a leading global financial services organization serving millions of customers across more than 20 countries and territories. The company is recognized as one of the insurance industry's leaders in Artificial Intelligence adoption, consistently investing in Generative AI, Machine Learning, and enterprise digital transformation initiatives. Its AI organization works closely with regional and global teams to develop innovative, production-ready AI solutions that enhance customer experience, improve business operations, and accelerate innovation across the enterprise.
The company offers a collaborative international environment, strong investment in employee development, flexible working arrangements, and long-term career growth opportunities while fostering a culture of innovation, responsible AI, and continuous learning.

Working Hours: Monday–Friday, 9:00–17:00
Working Style: Hybrid (2 days remote work per week)
Work Location: Tokyo
Holidays: Weekends, national holidays, year-end holidays, paid leave, and additional special leave.
Benefits: Comprehensive social insurance, retirement plan, professional training programs, language learning support, childcare and family care programs, wellness benefits, and other employee support initiatives.

Required Skills

- Extensive experience in cybersecurity, information security, technology risk, or related disciplines, ideally within complex enterprise environments
- Proven experience in highly regulated industries such as Insurance, Banking, or Financial Services, with strong knowledge of governance, risk, and compliance requirements
- Strong executive stakeholder management skills, including experience presenting security strategy, risks, and recommendations to senior leadership and/or Boards of Directors

Company Description