PR/160315 | Information Security Resilience Lead (Manufacturing)

Job Information

Recruiter
JAC Recruitment Malaysia

Job ID
1584347

Industry
Other (Manufacturing)

Job Type
Permanent Full-time

Location
Malaysia

Salary
Negotiable, based on experience

Refreshed
March 31st, 2026 10:25

General Requirements

Minimum Experience Level
Over 3 years

Career Level
Mid Career

Minimum English Level
Fluent

Minimum Japanese Level
None

Minimum Education Level
Associate Degree/Diploma

Visa Status
No permission to work in Japan required

Job Description

A global manufacturing group specializing in high-precision interconnect solutions and high-reliability assemblies across industries such as automotive, data communications, industrial equipment, and consumer electronics is seeking an Information Security Resilience Lead.
In this role, you will be responsible for the end-to-end governance, implementation, and continuous improvement of ICT continuity and cyber crisis readiness across global operations. Your mission is to ensure the organization can withstand, respond to, and recover from major digital disruptions, safeguarding uninterrupted business operations and production environments.

Key Responsibilities

- Develop, implement, and maintain the corporate ICT Business Continuity Management System (BCMS) and Cyber Crisis Management framework in alignment with ISO 22301 and ISO 27031.
  Lead comprehensive Business Impact Analyses (BIA) across business units and manufacturing sites to identify critical processes, Allowable Interruption Windows (AIW), Maximum Tolerable Outages (MTO), and minimum Service Level Objectives (SLOs).
- Collaborate with IT teams to design, validate, and optimize backup and recovery strategies, ensuring Disaster

Recovery (DR) plans meet business-defined RTO/RPO targets—particularly for production-critical systems.
- Design and facilitate scenario-based Cyber War Rooms, tabletop exercises, and full-scale crisis simulations to assess readiness and strengthen organizational resilience.
- Assess the resilience and recovery capabilities of third-party service providers, cloud partners, and key operational technology (OT) vendors, ensuring alignment with internal resilience standards.
- Serve as the subject matter expert for customer audits, supplier assessments, security questionnaires, and ISO 22301 certification activities related to ICT-BCP, DR, and Cyber Resilience.
- Partner with the Information Security GRC team to ensure the resilience framework meets regulatory and contractual requirements, including emerging standards such as NIS2.
- Prepare formal resilience dashboards, maturity assessments, and executive-level reporting outlining risks, gaps, and recommended improvements.

Key Requirements & Technical Skills

- Minimum 3 years of experience in Information Security with strong emphasis on ICT Business Continuity, Disaster Recovery, or Cyber Resilience.
- Solid understanding of ISO 22301 (Business Continuity) and ISO 27031 (ICT Readiness for Business Continuity).
- Proven experience designing or managing Cyber War Rooms and leading cross-functional teams through simulations or real-world incidents.
- Deep technical knowledge of modern backup solutions, immutable storage, replication methods, and architectures designed to meet stringent RTO/RPO objectives.
- Ability to translate technical recovery and resilience concepts into clear business-risk language for non-technical stakeholders.
- Strong ability to work independently while collaborating effectively with global teams.
- Analytical mindset with the capability to identify single points of failure within business or operational processes.
- Experience supporting external audits, customer assessments, or certification programs.
- Ability to evaluate the resilience and recovery posture of external cloud, SaaS, and critical OT/IT service providers.
- Bachelor’s degree in Information Security, Computer Science, Engineering, or a related discipline.
- Relevant certifications such as CBCP, CISM, CISSP, ISO 22301 Lead Implementer, or willingness to obtain them.

Company Description