BFCHRJ - 128 – IT Security Manager| Managed Services | Bahrain

About the role:

Reporting to the CIO, the Information Security Manager is responsible for understanding, communicating, and addressing the risks impacting the company's critical business processes and sensitive business information in its various forms of digital, physical and knowledge.

The Information Security Manager will be tasked with devising strategies to mitigate information security risks and mange IT security threats, which, if materialized, can cripple the Company's ability to execute normal business operations and have direct negative impacts the Company's profitability, reputation, client confidence, and regulatory compliance standing.

Your Responsibilities:

- Develop and own a customized Information Security Management Systems (ISMS) and the consequent frameworks, manuals, policies, procedure, forms, etc.
- Conduct and maintain an inventory of business information assets and assign owners, classification, criticality levels, and other relevant information to such assets.
- Conduct business impact analysis to define and map RTO and RPO to business processes.
- Conduct a risk analysis to identify, valuate, justify, and prioritize the controls to be adopted in order to preserve the confidentiality, integrity and availability of information.
- Propose and document technical and procedural controls to protect information flows across internal, external, and public networks.
- Introduce solutions and tools for continuous monitoring of accountability and traceability and the performance of adopted information security controls.
- Supervise analyzing the current technology environment to identify deficiencies and recommend solutions and areas of improvement.
- Engage with external parties to conduct regular and independent evaluation of the company's information security posture including internal vulnerability scanning, P&P evaluations, penetration testing, and others.
- Meet with departments' heads to gather business requirement and transform such requirement to executable projects.
- Play a leading role in developing the Company's disaster recovery and business continuity plans in order to ensuring that such plans adequately cover business operations contingencies and incident response.
- Establish an information security culture within the company.
- Prepare and deliver information security awareness training sessions and campaigns.

About You

- College degree, preferably in a related discipline
- Specialized certifications such as CISA, CISM, ISO27001, COBIT, etc.
- Exceptional English communication skills – both written and verbal.
- Minimum 10 years work experience.

Other skills required for the job:

- Strong knowledge of IT operations, technical controls, and latest technologies.
- Ability to read and understand regulations related to information protection.
- Understanding of online banking and payment processing.
- Exposure to the risks and opportunities of international E-Commerce is a plus
- Strong technical skills in Telecoms, Networks, Security, Applications and Database.
- A solid understanding of change management process.
- Able to work effectively at all levels in an organization.
- Strong analytic and decision-making abilities.
- Understanding of security incident management.
- Ability to influence others and move toward a common vision or goal.