BFCHRJ - 123 – IT Security Office | Managed Services | Bahrain

About the role:

The IT Security Officer (ITSO) is part of the information security assurance function responsible for helping to protect the integrity, confidentiality, and availability of the company's business data.

The ITSO role is a technical one which requires advanced knowledge and hands-on experience with data protection methodologies, tools, and standards, and being abreast with latest server, networking, and IT security technologies.

Your Responsibilities:

- Support the Information Security Manager in devising strategies to mitigate IT security risks and manage threats which, if materialized, would compromise sensitive business data, and obstruct the Company's ability to execute normal business operations.
- Assist the Information Security Manager in conducting and maintaining information security risk analysis and asset inventories, and in drafting policies and procedures.
- Advise on the design and data protection controls to imbed in e-Commerce websites, online financial transaction systems, VPNs, and web-based communication.
- Advise on the design of LAN, WAN, and parameter networks, and on the internal technical controls to adopt to protect data against internal and external threats.
- Work with the IT department to effectively deploy security devices such as firewalls, IPS, systems monitors, web filers, DLP, and end-point devices controls.
- Monitor implemented technical controls, procedural controls, and systems logs and produce regular reports on security breaches, incidents, and nonconformities.
- Analyzes network traffic and alerts to assess, prioritize and differentiate between potential intrusion attempts and false alarms.
- Take part in the software development process by advising on the security control to incorporate into new systems.
- Take part in projects with potential consequences on information security and advice on the controls to imbed in such projects.
- Participate in DR and BC planning to ensure that information security incident response capabilities are imbedded within such plans.
- Participate in assessing the IT environment and addressing vulnerabilities through systems inspections, internal vulnerability scanning, penetration testing, etc.
- Advise on the selection and procurement of IT security products and services.
- Participates in investigating IT security incidents and identifying and implementing appropriate corrective and preventive actions.

About You:

- College degree in Computer Science, Computer Engineering, or a related field of study
- Security certifications – CISA, CISM, CISSP, SSCP, CEH, SANS Security certifications (GIAC / GSEC)
- Certifications and training in cyber security, cloud security is preferred
- Strong knowledge of data security best practice and international standards
- Specialized technical certifications such as CISSP and CEH V7
- Strong knowledge of networking technologies: TCP/IP, firewalls, VPNs and proxies
- Strong knowledge of the PCI DSS standard and related technical controls including SEIM, HIPS, and encryption;
- Excellent knowledge of ISO27001, NIST RMF, OWASP

Minimum 3-5 years of hands-on technical work experience in similar environment / industry, which includes:

- Security incident management and investigations
- Security monitoring
- Vulnerability management
- Cloud security
- Cyber security
- Applications security
- Implementation and management of industry security standards

Other skills required for the job:

- Strong technical skills in securing websites and online financial transactions, networking, IT security practices, applications and databases
- Problem solving and root cause identification skills.
- Strong analytic and decision making abilities.