Job Profile for System Security Management Officer

- Ensure that guidelines for security in projects are met
- Ensure network security risk, application security (e.g. pen testing), Data base & Asset risk mgt. protection & review
- All activities pertaining to information and cyber risk assessment and response strategy are properly implemented
- Ensure that security vulnerabilities as well as incidents are managed proactively to prevent or minimize disruptions to business activities in case of possible security breaches

Role Qualification:

Academic/Professional: B.Sc./MSc in Computer Science, programming, Information Security/Information Technology, Electrical/Electronic Engineering or Computer Engineering/Information Systems Management or related field

Work Experience: Experience in information security, business continuity and data privacy. Experience with security testing and tech. Recognized professional certifications such as CEH, CISA, CISM, CISSP, PMP will be an added advantage.

Skills and Competencies:

- A forensic approach to challenges
- Analytical Skills/ Problem solving
- Interpersonal Skills
- Verbal & Written communication skills, including presentation skills with an abiltiy to communicate with a range of technical and non-technical team members and other relevant individuals
- Time management and organisational skills to manage a variety of tasks, prioritise workload and meet deadlines while providing high quality and timely products
- Demonstrate the ability to learn and apply critical thinking to a variety of situations
- Strong background and technical knowledge and skills in information technology, information security and cyber security with a clear understanding of security controls design and implementation and information security trends
- Knowledge of and in-depth experience in more than one major IT discipline (e.g., distributed computing, networks, financial applications design and development, IT security and business recovery)
- Sound working knowledge of information security & risk assessment methodologies/frameworks/standards such as NIST, PCIDSS, IS27001
- Good knowledge of network, web related protocols/technologies and security tools
- Experience with the use of leading security tools to determine emerging threat patterns and vulnerabilities
- Good knowledge of network security, application and database security, identity and access management
- Experience with IT performance management, network administration and system security
- Good understanding of cyber security risks associated with various technologies and ways to manage them

Key Responsibilities:

- Ensure a proactive information security and cyber security risk assessment is carried out in line with the requirements of the business as well as the best practices.
- Ensure a robust risk response plan is established to address potential information / cyber threats across the 3 Lines of Defence.
- Define security architecture design requirements, controls and provide expert advice for all projects.
- Ensure implemented security architecture design, requirements and controls meet applicable policies and standards in all projects.

- Participate in projects committees, meeting and engagements.
- Ensure the appropriate scanning technologies are configured and maintained.
- Review and validate security tools implemented by the first line
- Run and analyse vulnerability and compliance scans to support vulnerability management
- Responsible for performing vulnerability assessment and penetration testing on a regular basis
- Report all vulnerabilities and their current status to the CISO, CSO and other relevant stakeholders or as directed by the CISO and CSO.
- Monitor the company's digital presence and ensure all digital presence requirements are maintained.
- Support the management of all digital and technical assets
- Define business requirements (e.g. regulatory...) for information security operations, define use case, configure, maintain, implement
- Ensure that a robust threat intelligence program is put in place
- Ensure security event and cyber threat monitoring, analysis and reporting including documentation and mitigation of discovered cyber risks
- Investigate security alerts and provide incident response
- Ensure that cyber incident response team and underlying processes are in place and security incidents are managed effectively
- Responsible for maintaining the Security Operation Centre (SOC)
- Perform monitoring of operational activities done (security monitoring)
- Follow up and ensure remediation of the alerts from security event monitoring (malware analysis, threat hunting, alerts from security systems…) and management of security devices (AV, proxy, email gateway, FW, network devices, etc.) by IT
- Evaluate & ensure remediation of security lapses in new technology or product before they are deployed
- Have a good knowledge of business risks associated with common security vulnerabilities and be able to effectively communicate same to application developers, Infrastructure & Network Team and/or senior managers effectively
- Comply with Group security requirements as communicated
- Collaborate with and support the Group Information Security Practice, Local CISO/CSO and other stakeholders as necessary to ensure that information security within AXA Mansard is relevant, cost-effective and is delivered in accordance with the Group Information Security Strategy
- Promote a culture of information security and raise awareness
- Stay current on IT security trends and news and proactively hunt for potential threat actors on the network

Interested Applicants should send their CVs **to jobtalentrecruit@gmail.com** stating the role applied for as subject of mail. e.g "System Security Management Officer"