

Job Profile for the Information Security Officer/ Cyber Security Analyst

To drive cultural and organizational change throughout the local entity and implement a sustainable information security practice. Also to contribute to the development of the security shared services and ensure implementation of the shared services within AXA Mansard

Role Qualification:

Academic/Professional: B.Sc/MSc in Computer Science, Information Security/Information Technology, Electrical/Electronic Engineering or Computer Engineering

Work experience: 1-3 years relevant work experience in a large scale IT environment

Certifications: Any of CISSP, CISA, CISM, CEH, OSCP, GWAPT

Key Responsibilities:

- Conduct application security/penetration tests of internal/external web, mobile and web service applications, leveraging both manual techniques and automated tools and report identified vulnerabilities
- Monitor the implementation of remediation action plans for vulnerability management; follow-up with relevant stakeholders responsible performing the actions
- Have a good knowledge of business risks associated with common security vulnerabilities and be able to effectively communicate same to application developers and/or senior managers effectively
- Possess the ability to work independently in an enterprise setting
- Ensure that application developers comply with Group high level security requirements for coding
- Collaborate with and support the Group Information Security Practice, Local CISO 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

Required Competencies

- Experience in conducting vulnerability assessments, code reviews and penetration tests against web/mobile application technologies, APIs, platforms to find flaws and exploits
- Good knowledge of network and web related protocols/technologies
- Experience with vulnerability assessment tools and penetration testing techniques
- Detailed technical knowledge in general information security
- Demonstrate the ability to learn and apply critical thinking to a variety of situations
- Good understanding of cyber security risks associated with various technologies and ways to manage them
- Ability to work as part of a team and build strong relationships with staff and other relevant individuals

Generic Skills

- Strong IT skills and knowledge including hardware, software and networks
- A forensic approach to challenges
- Analytical Skills/ Problem solving
- Interpersonal Skills
- Verbal & Written communication skills, including presentation skills with an ability 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

Interested Applicants should send their CVs to jobtalentrecruit@gmail.com stating the role applied for as subject of mail. e.g “Information Security Officer/ Cyber Security Analyst”