

Position: Unit Head IS/CISO
Division: Risk Management Division
Location: Head Office Karachi

Experience & Qualification:

Bachelors or Masters in the field of Computer Science or in same discipline. Additional, certifications (e.g. CISM, CISA, Ethical Hacking, etc.) in the same discipline would be preferred. 8 Years of experience in the same subject area.

Main Duties & Responsibilities:

- Develop, maintain and oversee Information Securities policies, processes and control framework to address all applicable IT security requirements.
- Ensure that information assets and technologies are adequately protected in line with regulatory requirements/guidelines as well as internal policies.
- Review IT security standards on a continuous basis with appropriate response planning.
- Develop and implement effective security monitoring of vulnerabilities, threats and events in network and host systems.
- Supervise the mechanism to detect, report, and mitigate incidents that may impair adequate data and infrastructure security.
- Conduct IT security risk assessments and ensure that the senior management is timely communicated.
- Develop SOP to handle security incidents and direct a full enquiry with recommended courses of action.
- Manage Threat Intelligence and SIEM platforms
- Anticipate new security threats and stay updated with growing challenges.
- Keep abreast with new laws/regulations and best practices related to IT security, business continuity/disaster recovery.
- Train & oversee personnel with significant IT security duties.
- Strengthen monitoring mechanism and controls especially from cyber threats
- Interact with vendors and to manage IT security projects
- Circulation of reports on Cyber activity taking place on Bank's network for senior management and other stakeholders.
- Vulnerability Assessment of OS, network, DBMS, applications, Software (SVA) and end users.
- Conduct/Participate in Internal/External penetration testing and security assessment exercises/security audits of Enterprise wide IT Infrastructure and Applications including Endpoints, Physical/Virtual Servers Infrastructure, Databases, Network Nodes, Security Appliances, Banking Systems, Storages, Web Applications and DWH/BI systems.
- Design, build, and review relevant training content to increase awareness of Information Security Policy, programs, and practices.
- Any other task assigned by the Line Manager/ Management is to be performed to the best of his/her capability.”