LOCATION Garowe

REPORTING TO

1. IMMEDIATE SUPERVISOR Information Technology Manager

2. TECHNICAL SUPERVISOR Risk Manager

POSITION One

DEADLINE 21-03-2019

REPORT STRUCTURE

1. Reports Information security related incidents and audits to Risk Manager.

2. Works with IT Department as software support assistant

GENERAL FUNCTION

The Information Security Officer (ISO) provides the vision and strategies necessary to ensure the confidentiality, integrity, and availability of Bank electronic information by communicating risk to senior administration, creating and maintaining enforceable policies and supporting processes, and ensuring compliance with regulatory requirements. To support these activities, the ISO coordinates activities with other departments, including the evaluation, procurement, and deployment of security-related products and develops and coordinates information security awareness and education programs. Additionally, the ISO ensures a Bank system-wide disaster recovery and incident response plans are in place.

ESSENTIAL DUTIES AND RESONSIBLITIES

- Enterprise Application Administration:
    1. Review and analyze existing application effectiveness and efficiency and develop strategies for improving these systems.
    2. Provide customer support and technical direction for problem resolution.
    3. Enforce and monitor security policies and procedures for software applications.
    4. Manage staff account on enterprise applications.
    5. Perform application tuning, configuration, monitoring, and administration.
    6. Plan and manage application software upgrades.
    7. Analyze custom administrative software requests and present solutions.
    8. Ensure that any new software integration into the organization systems meets functional requirements and system compliance.

9. Perform daily monitoring and capacity planning for enterprise information systems.
10. Build custom reports and dashboards to support management decision making.
11. Manages multiple linked databases to include security, data safety and integrity, disaster recovery, and development of bulk data import/export procedures.
12. Performs software installations and upgrades to operating systems and layered software applications.
13. Monitors and tunes systems to achieve optimum performance levels.
14. Develops and implements various training, job aids, and instruction for users on the use of operating systems, networking, applications, and databases.
15. Maintains currency of knowledge with respect to state-of-the-art technology, equipment, and/or systems.

· Information Security Functions:

1. May lead or guide the work of other staff engaged in similar functions.1. Creates information security strategies, both short-term and long-range, in support of the Bank's goals.
2. Directs an ongoing, proactive risk assessment program for all new and existing systems and remains familiar with the Bank's goals and business processes so effective controls can be put in place for those areas presenting the greatest information security risk.
3. Communicates risks and recommendations to mitigate risks to the senior administration by communicating in non-technical, cost/benefit terms and in a format relevant to senior administrators so decisions can be made to ensure the security of information systems and information entrusted to the Bank.
4. Oversees all ongoing activities related to the development, implementation, and maintenance of the Bank's information security policies and procedures by ensuring these policies and procedures encompass the overall security of electronic information at rest or in motion within the Amal Bank system and assisting departments in local process and procedure development, ensuring they are not in conflict with Bank policies.
5. Assists other departments to ensure regulatory compliance in areas such as the Payment Card Industry – Data Security Standards (PCI-DSS).
6. Chairs the Information Security Executive Committee (ISEC) and coordinates the activities of ISEC so that security decisions do not interrupt business processes while maintaining the confidentiality, integrity, and availability of Bank information.
7. Ensures vulnerabilities are managed by directing periodic vulnerability scans of servers connected to Amal Bank networks.
8. Develops information security awareness training and education programs, works with other Bank entities to present them to staff and participates in local, regional, and national awareness and education events, as appropriate.

9. Ensures sufficient resources are available and allocated to projects by balancing project funding requirements with the assigned budgets, coordinates and tracks project expenditures to ensure resources are used effectively and within budget, and provides periodic budget reports to his immediate supervisor.
10. Acts proactively to prevent potential disaster situations by ensuring that proper protections are in place, such as intrusion detection and prevention systems, firewalls, and effective physical safeguards, and provides for the availability of computer resources by ensuring a business continuity/disaster recovery plan is in place to offset the effects caused by intentional and unintentional acts.
11. Evaluates security incidents and determines what response, if any, is needed and coordinates Bank responses, including technical incident response teams, when sensitive information is breached.
12. Contributes to a work environment that encourages knowledge of, respect for, and development of skills to engage with those of other cultures or backgrounds.
13. Remains competent and current through self-directed professional reading, developing professional contacts with colleagues, attending professional development courses, attending training, conferences, and/or courses as directed by the supervisor, and obtaining certifications relevant to job duties.
14. Contributes to the overall success of the Bank by performing all other duties and responsibilities as assigned.

MINIMUM ACCEPTABLE QUALIFICATIONS

Education: Master Degree in IT security is preferred.

Experience: At least 3 years of varied information technology experience is required. Applicable experience includes, but is not limited to, computer and networking infrastructure, operating systems, application software development, project management, regulatory compliance, risk management, and providing training. one years of direct experience in information security-related duties is required. Experience in a Bank setting is preferred.

Skills: The ability to understand hardware and software systems is required. The ability to maintain confidentiality in regard to information processed, stored, or accessed by the systems is required. The ability to manage multiple concurrent projects and to reason analytically is required. The ability to work with and train people possessing differing levels of technical knowledge is required. Effective verbal and written communication skills and proficiency in writing technical specifications are required. The ability to develop knowledge of, respect for, and skills to engage with those of other cultures or backgrounds is required.

Other: Professional certification (CISSP, GIAC, CISA, CISM, etc.) is preferred.

Amal Bank is an equal opportunity employer and offers a competitive compensation package commensurate with qualifications and experience.

To apply for the position please click on apply now

http://portal.amalbankso.so:8080/job_application?new=1&job_title=information-security-officer