

Job Title : SO / AM, IT Security and Governance

OVERALL PURPOSE:

- ◆ This position is responsible for establishes, manages and administers Bank's security to ensure preventive and recovery strategies are in place, and minimize the risk of internal and external security threats. He/She is also responsible for Bank's secure posture following information security policy, standards and procedures to ensure that all information systems are functional and secure.

RESPONSIBILITIES:

Main Responsibilities

- ◆ To assist in developing and enhancing security policies, procedures, guidelines, and standards,
- ◆ To create and manage risk register and work with various teams on-going basis to guide the on mitigation.
- ◆ To perform risk assessment on all new technology related change request and projects.
- ◆ To lead system penetration test to ensure any gaps are addressed,
- ◆ To ensure that all new implementations of solutions comply with requirements of the security policy/compliance, standards, and regulatory NBC Technology Risk Management Guidelines and swift customer security controls framework, etc.),.
- ◆ To collaborate with related parties to design and implement security controls.
- ◆ To develop remediation and mitigation plans, and creating packages for the implementation of those plans.
- ◆ To integrate security architecture with projects and major changes.
- ◆ To participate in cross-functional efforts for managing organization-wide risks.
- ◆ To investigate suspected and actual security incidents in accordance with the security incident management standard, produce reports with recommendations and ensure any remedial action is taken,
- ◆ To work with internal stakeholders to develop relationships to help promote and improve information security and provide security advice on procurements, projects and new initiatives as required,
- ◆ To review and monitors compliance with information security policies and procedures, referring problems to the appropriate branch manager and department head,
- ◆ To prepares the disaster recovery plan (DR/BCP) and assist in coordinating contingency plan tests on a regular basis,
- ◆ To work with both internal and external Audit relates IT matters,
- ◆ To prepare monthly report submit to line manager.

Others:

- ◆ Respond to enquiries from staff and provide security advice as required,
- ◆ Work with technology related team/department to formulate IT operational procedures, and ensure IT operation functions meets business requirement,
- ◆ Prepare monthly security reports and user and role assessment review at periodical basis,
- ◆ Willing to learn new things and got global cyber certified,
- ◆ Other job assigned.

QUALIFICATIONS REQUIREMENTS:

- ◆ Bachelor degree or master graduated in of IT, Computer Science, Management of Information Systems or other related field
- ◆ At least 3 years working experience in IT Security and Governance or Other IT Security Related,
- ◆ A good working knowledge of information security including ISO/IEC 27001 Information Security Management Standard,
- ◆ CISSP, OSCP, CEH, CISA certify is a plus,
- ◆ Good working knowledge of information risk analysis/management,
- ◆ Ability to manage time and priorities appropriately,
- ◆ Positive attitude towards learning and development demonstrated by a record of continuing professional development,
- ◆ Good verbal and written communication skills and able to communicate effectively at all levels,
- ◆ Honesty, reliability, and a commitment to strict confidentiality.
- ◆ Good in analytical skills and interpersonal skills.

Contact Info:

Email: hr@vattanacbank.com

Phone Number: 023 963 999 / 070 723 747