SECURITY/RISK ASSESSMENT ANALYST

The Information Security Assessment Analyst position's core responsibilities are to conduct application and third party information security assessments. Additional responsibilities may include leading process improvement activities, participating in information security assessment special projects and other assessment related activities.

The Information Security Assessment Analyst position will be expected to:

Understand complex business and information technology management processes. Identify and evaluate technology risks internally and/or at third parties, internal controls which mitigate risks, and related opportunities for internal control improvements. Develop an understanding of the third parties' IT control environment and perform basic risk management approaches to evaluate their IT controls
Actively participate in decision making with third parties and internal SunTrust management for mitigating identified deficiencies and seek to understand the broader impact of the decisions made. Establish and nurture positive working relationships with third parties and service managers with the intention to exceed their expectations. Assess IT general controls and/or application layer security controls to ascertain whether they comply with SunTrust policies. Generate innovative ideas and challenge the status quo.

Responsible for developing, implementing, enforcement and validating of information security policies, standards, methods and procedures and monitors compliance across the enterprise. Builds and implements security awareness programs within the business unit. Performs procedures and assessments necessary to ensure the safety of information system assets and to protect systems from intentional or inadvertent access or destruction. Investigates, documents, and resolves information security incidents. Ensures users understand and adhere to necessary procedures to maintain security. Advises management of critical issues that may affect customers, suppliers or company.

Serves as a Senior level Information Security Officer and will be responsible for managing the relationship with assigned business units with regard to the Information Security Program. Oversees the risk assessment and information security awareness processes. Interface with end users as well as all levels of management, Senior Executives; and technical and business sources. Responsible for a deep understanding of business processes and technology used within the assigned areas to ensure that the business is in compliance with regulatory requirements and the SunTrust Information Security Policy and applicable procedures, processes and standards. Acts as primary Technology Risk and Compliance (TRaC) representative on higher risk projects to ensure that information security risks are managed and the TRaC risk assessment process is followed. Reviews work performed by less experienced TRaC Governance resources for high risk assessment activities. Serves as Program Owner and provides maintenance of program documentation procedures and processes to

ensure compliance with changes in business or regulatory drivers.

Ideal Candidate Will Have -

- 3+ years of risk management and/or internal controls
- Big 4, Consulting or IT internal audit experience
- CISA, CIA, CISSP certification
- Demonstrate professional skepticism to ensure evidence is sufficient when assessing the relevant controls
- Communicate and present concisely and effectively based on the appropriate level of management
- Manage competing deadlines and prioritize responsibilities to effectively meet business needs
- Develop and teach less experienced staff
- Work both independently and as part of a team at all levels and across departments
- Demonstrate an understanding of business processes, internal control risk management, IT controls, and how they interact together
- Demonstrate leadership and problem solving skills
- Possess advanced interview skills to tailor the types of questions based on responses provided by internal personnel or supplier contacts
- Open to travel 5-10%, if needed

Basic Qualifications -

Bachelor degree or an equivalent combination of education and work experience. 6 years information security experience or a combination of information technology work experience and information security experience. Demonstrate solid knowledge of information security risks and countermeasures and GLBA, PCI and other information security and control frameworks. Demonstrate effective verbal and written communication skills for the purpose of explaining technical information to clients, vendors, senior management and staff and ability to apply knowledge and deductive reasoning. Strong analytical, problem solving, organizational, documentation; time management skills. Strong attention to detail. Strong relationship and facilitation skills. Proficient with Microsoft Word, Excel, PowerPoint, and Access. Information Security certification such as CISSP.