Class Concept

This is administrative and supervisory work responsible for development and enforcement of an agency's security policy and strategy. Performs IT risk assessments, audits, and security incident investigations at the agency level. Administers security programs and procedures. Depending on the size of the organizational structure, this role may report to an IT Security & Compliance Manager II, a higher-level IT Director or Executive, or an Agency Enterprise Security and Risk Director. Position may serve as the Chief Security and Risk Manager in agencies with smaller IT units with limited scope and complexity and in such cases may report to a non-IT executive level position. Position supervises a team of IT Security & Compliance Specialists or may supervise other IT professionals if the role oversees all IT functions for an agency.

Recruitment Standards

Knowledge, Skills, and Abilities

- Working knowledge in the following information security areas: Security Governance and Management, Security Frameworks, Policies, and procedures, and Federal, State Privacy Laws and regulatory guidelines including HIPAA, Internal Revenue Tax Code, SSA, and/or NIST.
- Effective communication and interpersonal skills; the ability to work with internal and external audiences.
- Ability to lead effectively and interact with higher level management.
- Diverse skill base in both Information Systems and Information Security which address organizational structure and administration practices, system development and maintenance procedures, system software and hardware controls, security and access controls, computer operations, environmental protection and detection, and backup and recovery procedures.
- Ability to solve a wide range of technical problems, requiring ingenuity and innovation.
- Working knowledge of network, operating systems, databases, applications, and mobile security.
- Working knowledge of all phases of service development and deployment including architecture, design, development, testing, release, and operational maintenance.
- Ability to provide incident response and recovery activities as aligned with HIPAA, IRS, SSA, and the NIST Incident Response phased approach.
- Demonstrated organization, facilitation, communication, and presentation skills, incident management skills including analysis and response, conducting information security audits and reviews experience and experience with information security risk assessments and risk management.

Minimum Education and Experience

Bachelor's degree in computer science or a related IT field or closely related field from an appropriately accredited institution and two years of progressive experience in IT security or closely related area; or

Associate degree in computer science or a related IT field or closely related field from an appropriately accredited institution and three years of progressive experience in IT Security or closely related area; or an equivalent combination of education and experience.

Note: This is a generalized representation of positions in this class and is not intended to identify essential functions per ADA.