Class Concept

This level is distinguished form level I by the scope of the agency's design security systems and architectures that protect federally and state mandated information such as tax records, health information, research data, state security records or student educational records. They design security systems for organizations with complex network systems, major databases, emerging technologies, or systems with known vulnerabilities. Position may serve as the Chief Security and Risk Manager in agencies of midlevel IT units with moderate scope and complexity. Position supervises a team of IT Security & Compliance Specialists and/or manages IT Security & Compliance Manager I positions that oversee security for individual networks, systems, or databases.

Recruitment Standards

Knowledge, Skills, and Abilities

- Working knowledge of deploying, operating, and maintaining Enterprise Information Security programs and controls in the public service sector.
- Thorough 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.
- Thorough knowledge of application security controls and awareness of top security considerations for application development in the Software Development Lifecycle.
- Thorough knowledge of database security controls, including access control, auditing, and configuration best practices.
- inworking knowledge of risk management including vulnerability assessment, control assessment, likelihood determination and risk prioritization and demonstrated ability to conduct risk assessments, audits, and reviews.
- Demonstrated ability to problem solve and implement process improvement.
- Working knowledge of network architecture and concepts, application architecture, and interoperability of these architectures with one another.
- Thorough knowledge of computer and network forensics, system and network security, incident management, intrusion detection, vulnerability and patch management, log analysis, and related technologies.
- Ability to provide incident response and recovery activities as aligned with the HIPAA, IRS, SSA, and NIST Incident Response phased approach.
- Demonstrated ability to work well on collaborative, cross-functional teams.
- Solid interpersonal skills with ability to work effectively with people of all levels of information technology expertise with a wide range of constituencies and organizational relationships.
- Excellent communication skills; interpersonal, organizational and analytical skills, written and verbal communications and experience with management presentations.

Minimum Education and Experience

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

Associate degree in computer science or a related IT field or related degree from an appropriately accredited institution and four years of progressive experience in IT security or closely related area which includes two years supervisory experience; 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.