

2210 — Security (INFOSEC)

Involves ensuring the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools. Functions commonly performed by employees in this specialty may include: developing policies and procedures to ensure information systems reliability and accessibility and to prevent and defend against unauthorized access to systems, networks, and data; conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks and protection needs; promoting awareness of security issues among management and ensuring sound security principles are reflected in organizations' visions and goals; conducting systems security evaluations, audits, and reviews; developing systems contingency plans and disaster recovery procedures; developing and implementing programs to ensure that systems, network, and data users are aware of, understand, and adhere to systems security policies and procedures; participating in network and systems design to ensure implementation of appropriate systems security policies; facilitating the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes; assessing security events to determine impact and implementing corrective actions; and/or ensuring the rigorous application of information security/information assurance policies, principles, and practices in the delivery of all IT services.