

FUNCTIONAL AREA 8

Information Systems Security Administration (ISA)

Incumbents in this functional area ensure the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, testing, implementation, maintenance, and enhancements of information security systems and related programs, policies, procedures, and tools. They maintain the security of commercial-off-the-shelf (COTS) and State-developed applications installed on the State's information systems. The software and/or databases being secured may reside on mainframe, mid range, or PC servers or personal computers, laptops and/or mobile computing devices, be multi-user, multi-tasking and may consist of many interrelated programs spread across multiple platforms. Incumbents may, in addition to other duties, also oversee the authorization and monitoring of access to any part or the Department's facilities or infrastructure in accordance with established organization policy. Such requirements include the evaluation of information systems to identify risks, investigation of unauthorized access, and the performance of other administrative duties related to security management.

INFORMATION SYSTEMS SECURITY ADMINISTRATION	Assistant Information Technology Specialist	Information Technology Specialist I	Information Technology Specialist II	Information Technology Specialist III
Knowledge of:				
Client user and business needs		X	X	X
Contingency plan for backup and recovery functions		X	X	X
Security policy administration to effectively monitor security software		X	X	X
Information technology security certification and accreditation requirements and processes		X	X	X
IT systems security methods and procedures		X	X	X
Methods for evaluating, implementing, and disseminating IT security tools and procedures		X	X	X
Security technology, including technical documentation methods and procedures		X	X	X
Encryption principles and techniques for application, integration, and administration of the organizational security program		X	X	X
Methods, techniques, and tools used for risk assessment and mitigation of risk to IT projects			X	X
Network operations and protocols			X	X
Security strategies to maintain the integrity of data			X	X
Various database applications to determine			X	X

the level and type of security needed to protect the application				
Computer forensics principles			X	X
IT security practices and methods (current and trends) for strategic planning				X
Security policy administration to effectively monitor security software				X
Total infrastructure protection environment				X
Legislation or external regulations which affect security				X
Ability to:				
Participate in assessments of planned and installed information systems to identify vulnerabilities, risks and protection needs		X	X	X
Participate in systems security evaluations, audits, and reviews		X	X	X
Provide information systems security administration information and assistance to customers		X	X	X
Prepare and update information security manuals, instructions and operating procedures		X	X	X
Participate in defining IT security assignments		X	X	X
Assist users in defining their needs for new access and privileges		X	X	X
Ensure coordination and/or collaboration on security activities		X	X	X
Relate requirements to user privileges by gaining knowledge of their business needs		X	X	X
Participate in network and systems design to ensure implementation of appropriate systems security policies			X	X
Develop, implement, and coordinate activities designed to ensure, protect, and restore IT systems, services, and capabilities			X	X
Ensure proper protection of evidence used in investigating computer crimes			X	X
Develop systems security contingency plans and disaster recovery procedures			X	X
Evaluate established IT security methods and procedures and prepare recommendations for changes in methods and practices where appropriate			X	X
Identify and resolve potential security conflicts to minimize adverse impact to system custodians and stakeholders caused by a breach of security			X	X
Assess security events to determine impact, including implementing corrective actions and notifying all appropriate personnel			X	X
Facilitate the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes				X
Develop and implement programs to ensure				X

that systems, network, and data users are aware of, understand, and adhere to systems security policies and procedures				
Ensure sound security principles are reflected in organizations visions and goals				X
Advise other IT experts throughout the organization on a variety of situations and issues that involve applying or adapting new security theories, concepts, principles, standards, methods, or practices				X
Serve as senior expert and consultant to the executive management to advise on integrating security programs with other programs of equivalent scope and complexity				X
Develop new theories, concepts, standards and methodologies in security administration				X
Integrate information systems security with other security disciplines that certify systems or network accreditation				X
Provide technical direction/leadership of complex security program or project work				X

Information Technology Specialist I (Information Systems Security Administration)

Incumbents apply a basic understanding of information technology concepts, practices, methods and principles, with an emphasis in information systems/network security and information systems security certification. Working under direct technical supervision, incumbents perform a variety of analytical tasks related to ensuring the security of information technology systems for their organization. They assist in the technical aspects of system security to ensure, protect, and restore services and capabilities. Incumbents participate in conducting risk assessments and security-related training; documenting and escalating security violations; and reviewing automated security administration tools and network/application design to ensure security policies are followed.

Information Technology Specialist II (Information Systems Security Administration)

Incumbents demonstrate proficiency of business and technical IT competencies, with a specialization in security-related information technology concepts, practices, methods, and principles. Incumbents apply knowledge of the organization's technology and business infrastructure to effectively perform the full range of security administration responsibilities on systems that are at a minimum networked/multi-user/single platform. Work may include participation in the evaluation of information systems to develop risk assessment, systems security, or disaster recovery plans. As a lead technical security specialist incumbents develop and maintain detection systems, troubleshoot security vulnerabilities, and evaluate new detection technologies and recommend adoption. In the role of a security policy specialist incumbents provide guidance, assistance, and coordination to systems developers. They also analyze systems development plans to

ensure security requirements and specifications are adequately defined and in compliance with statewide standards. In both roles, technical decision making responsibility is taken for the analysis, evaluation, development, coordination, and dissemination of security tools and procedures to eliminate system vulnerabilities.

Information Technology Specialist III (Information Systems Security Administration)
RANGE A

At the Specialist III, Range A level incumbent's serve in a lead capacity and direct the work of assigned staff and/or serve as expert specialists who work independently and deal with complex and/or critical information systems/network security issues. Incumbents provide lead direction and training in the establishment and maintenance of a secure IT environment; during the planning stage incumbents perform a key role in strategy and design. Using their extensive knowledge of multiple or diverse IT environments, incumbents have responsibility to develop procedures and policies for evaluating, coordinating, and disseminating security tools. Expert level staff defines and implement strategies for security planning and testing to eliminate information system vulnerabilities. They also work with system developers to ensure security requirements are incorporated into the systems development life cycle process. Responsibilities include directing and applying control systems to prevent error, abuse, fraud, etc. In the event of a security breach incumbents facilitate the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes. They also investigate complex and highly sensitive violations referred by lower level staff, including obtaining factual information, and formulating responses regarding violation exposures.

Information Technology Specialist III (Information Systems Security Administration)
RANGE B

Range B level security administrator positions function at the principal level and have responsibility to make decisions or recommendations significantly changing, interpreting, or developing important information systems/network security policies or programs. Incumbents coordinate and build consensus across an organization for security planning and implementation. They direct security for extremely complex enterprise-wide and/or external to the state networked/multi-user/multiplatform information technology systems. These types of multi-user systems are typically found in either large department or data center environments. Incumbents lead in the analysis, evaluation, development, coordination, and dissemination of security tools and procedures to eliminate system vulnerabilities. Incumbents also develop procedures and policies for security-related strategic/tactical plans for information systems throughout the organizations. Principal level security specialists may also perform the following tasks on the extremely complex multi-user system described above:

- Analyze, design, develop, implement, test, and maintain a plan that includes the evolving business risk, encryption capability and information security control requirements department-wide and or state-wide.

- Ensure all security plans are consistent with budget requirements and other administrative actions for the organization.
- Monitor new technologies, trends and regulatory issues for impact on the security administration.

DRAFT