New York State Department of Civil Service
DIVISION OF CLASSIFICATION & COMPENSATION

Classification Standard

Occ. Code 0815670

Manager Information Technology Services 1 (Information Security), Grade 27 0815670
Manager Information Technology Services 2 (Information Security), Grade 29 0815770
Information Security Manager, M-8 0815850

Brief Description of Class Series

Positions in this title series manage information security systems and infrastructure to safeguard sensitive information assets and reduce cyber-related risk at the Office of Information Technology Services. Incumbents act as information security subject matter experts related to information systems analysis, design, development, maintenance, implementation, and quality assurance activities; monitor and coordinate responses to information security threats; and monitor, develop, implement, and enhance New York State information security policies and standards.

Distinguishing Characteristics

Managers Information Technology Services 1 and 2 (Information Security) perform similar duties. The levels are distinguished by the scope of the information security unit responsibilities, which is measured by the size of the agency or agencies served, variety of programs overseen, and supervisory responsibility.

Manager Information Technology Services 1 (Information Security): non-competitive; directs and manages the day-to-day operations of an information security unit to support the confidentiality, integrity, and availability of the State's information assets; supervise a team of Information Technology Specialist 4 (Information Security) and lower-level information security positions.

*Manager Information Technology Services 2 (Information Security)***:** non-competitive; directs and manages the day-to-day operations of a large information security unit or multiple units to support the confidentiality, integrity, and availability of the State's information assets; supervises a team of Manager Information Technology Services 1 (Information Security*)* and lower-level information security positions.

Information Security Manager: non-competitive; directs and oversees one or more bureaus within an Information Security Office; ensures information security

activities align with State policies and standards; supervises a team of Manager Information Technology Services 2 (Information Security) and lower-level information security positions.

Related Classes

Information Technology Specialists 2-4 (Information Security) oversee agency information security compliance programs; manage and resolve security threats to agency information systems; conduct first and second-level analysis, remediation, and escalation of cyber events; and conduct digital forensic and threat detection/prevention analysis.

Managers Information Technology Services 1 and 2 plan, direct and coordinate systems analysis, design, application program development, maintenance, implementation and quality assurance activities for one or more agencies or a major systems development group within an information technology organization. Incumbents direct the activities of lower-level Information Technology Specialists.

Chief Information Security Officers 1 and 2 represent their agency's interests with respect to the security of its information and information systems, and have a senior advisory role in decisions affecting information security and assurance. They implement, enhance, monitor and enforce agency and State information security policies and standards, and oversee alleged information security violations and follow agency and State procedures for referring the investigation to other investigatory entities, including law enforcement.

Illustrative Tasks

Manager Information Technology Services 1and 2 (Information Security)

Directs and manages implementation of information security and compliance programs.

- Provides direction and guidance to teams with responsibility for developing, deploying, and maintaining information security architecture.

- Directs the development, interpretation, review, and communication of information security policies, procedures, and standards.

- Coordinates the implementation of information security procedures, risk reviews, and remediation activity; monitors information security compliance; recommends improvements to monitor access to information assets and ensure security safeguards are maintained.

Manages and resolves security threats to agency information systems and information security incident response.

- Directs development and implementation of information security risk analysis and management processes; coordinates vulnerability scanning and analysis to help determine risk and remediation priorities; manages development and maintenance of enterprise risk registers, which includes reporting and tracking remediation efforts.

- Directs the characterization and analysis of network traffic to identify anomalies and potential threats to network resources; determines events that require investigation and response.

- Implements and improves information security incident response plans and reports.

- Develops and implements plans and procedures to ensure business critical services are recovered in disaster events.

- Directs investigation of alleged information security violations; coordinates collection, seizure, handling, and analysis of digital evidence; responds to requests for information from investigators.

- May testify in proceedings regarding analytical processes and findings.

Serves as an information security expert, and evaluates systems and contracts for alignment with State and agency information security policies and standards.

- Reviews contract, service level agreement, memorandum of understanding language, and other documents to verify needs, requirements, and alignment with State policies and standards.

- Provides information security expertise and recommendations to agency executives on a broad range of information security matters.

- Researches laws and regulations that could affect the security controls and classification of information assets.

- Monitors information security trends, tools, and techniques to maintain awareness and evaluate the applicability of the latest information security techniques and tools to agencies' security programs.

- Develops a multilayered and adaptive approach to counter information security threat environments; represents the agency at internal and external information security meetings.

Manages staff and resources dedicated to information security programs.

- Develops metrics to measure the efficiency and effectiveness of information security programs.

- Prepares information security staffing, development, and training budget plans to align with agency risk management and information security plans.

- Trains agency staff on information technology and information asset protection.

- Performs the full range of supervisory responsibility.

Information Security Manager

- Oversees and directs all activities for one or more bureaus within an Information Security Office, including supervision of a team of Manager Information Technology Services 2 (Information Security) and lower-level information security positions.

- Identifies and assists agencies in classifying and protecting information assets that support critical business functions, and managing related cybersecurity risks.

- Oversees implementation of information security policies and standards to ensure compliance and efficient delivery of services.

- Leads, develops, and directs problem solving initiatives, and anticipates information security needs, based on research of industry trends.

- Coordinates information security risk management initiatives across information technology and business teams.

- Reviews the framework for all information security initiatives including budgets, staff resources, hardware and software needs, and ensures that agencies' business needs are considered.

- Identifies, evaluates, reports, and advises executive management on cybersecurity risks, with consideration for compliance and regulatory requirements.

- Oversees cyber security threat and vulnerability analysis, and develops and updates information security strategic plans.

- Develops and guides implementation of safeguards to ensure system resiliency; coordinates the protection of critical infrastructure services; directs detection, containment, and cybersecurity incident response activities.

- Develops and manages information security awareness training programs.

Minimum Qualifications

Manager Information Technology Services 1 (Information Security)

Non-competitive: bachelor's degree with at least 15 credit hours in cyber security, information assurance or information technology and four years of information technology experience, including three years of information security or information assurance experience and two years at a supervisory level.

Manager Information Technology Services 2 (Information Security)

Non-competitive: bachelor's degree with at least 15 credit hours in cyber security, information assurance or information technology and five years of information technology experience, including four years of information security or information assurance experience and three years at a supervisory level or one year at a managerial level.

Information Security Manager

Non-competitive: bachelor's degree with at least 15 credit hours in cyber security, information assurance or information technology and six years of information technology experience, including five years of information security or information assurance experience and four years at a supervisory level or two years at a managerial level.

Note: bachelor's degree candidates without at least 15 course credits in cyber security, information assurance, or information technology require an additional year of general information technology experience to qualify. Appropriate information security or information assurance experience may substitute for the bachelor's degree on a year-for-year basis; an associate's degree requires an additional two years of general information technology experience. Experience solely in information security or information assurance may substitute for the general information technology experience.

Note: Classification Standards illustrate the nature, extent, and scope of duties and responsibilities of the classes they describe. Standards cannot and do not include all of the work that might be appropriately performed by a class. The minimum qualifications above are those which were required for appointment at the time the Classification Standard was written. Please contact the Division of Staffing Services for current information on minimum requirements for appointment or examination.

Date: 01/2021

AM