New York State Department of Civil Service
DIVISION OF CLASSIFICAION AND COMPENSATION

Classification Standard

Occ. Code 0836100

Chief Information Security Officer, M-2

Brief Description of Class

Chief Information Security Officers (CISOs) 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. They recommend and approve agency security policies, standards, processes, and education and awareness programs to verify that appropriate safeguards are implemented; and facilitate compliance with those policies, standards, and processes. They oversee alleged information security violations, incidents and events, and follow agency and State procedures for referring the investigation to other investigatory entities, including law enforcement.

Distinguishing Characteristics

Chief Information Security Officer: non-competitive; provides leadership and technical expertise to ensure the integrity, confidentiality, and availability of information assets under the general direction of the agency head, general counsel or executive designee. They oversee and coordinate information security and information assurance efforts across an agency; and exercise enterprise-wide authority for compliance with the agency’s information security and assurance policies.

Related Classes

Information Technology Specialists (Information Security) and Managers Information Technology Services (Information Security) function as information security administrators with responsibility to administer security tools, review security practices, identify and analyze security threats and solutions, and respond to security violations, incidents and events.

Illustrative Duties

Directs and manages an agency’s information security program.

- Directs the information security unit in developing, deploying, and maintaining agency information security architecture, policies, standards, and procedures in accordance with State information security policies and standards.

- Directs the development and implementation of the agency’s information security program and determines the level of security controls required to protect information technology and information assets.

- Monitors adopted and regulated industry compliance statutes and law standards to ensure organizational processes meet or exceed requirements and are audited within defined timeframes; recommends improvements to control access to agency information assets and ensures security safeguards are maintained.

- Coordinates agency technical efforts in response to information and system security compliance reviews or audits performed by external regulatory organizations or auditors.

- Directs the investigation of alleged information security violations, incidents or events, follows agency procedures for referring the investigation to other investigatory entities (e.g., law enforcement, and State and federal oversight agencies), and responds to requests for information from external investigators.

- Responds to inquiries for information to support agency processes related to litigation support, including electronic records management and electronic discovery preparedness (e.g., records integrity and preservation).

- Develops effective disaster recovery policies and standards; coordinates the development of implementation plans and procedures to ensure that business-critical services are recovered in the event of a disaster and provides direction and in-house consulting in these areas.

- Supervises, administers, or verifies training to agency employees, contractors, and third parties, as appropriate, on their responsibilities to protect agency IT and information assets.

Manages and resolves security threats to agency information systems.

- Develops information security risk analysis and risk management processes with business units, identifies acceptable levels of risk, and establishes roles and responsibilities with regard to information classification and protection.

- Develops, implements, and improves information security incident response plans and reports.

- Evaluates new security threats and counter measures that could affect agency information systems and recommends improvements to executive management to mitigate risks.

- Administers or verifies completion of regular internal intrusion testing, evaluates the results, and makes changes to agency information security procedures and training programs to improve compliance with State and agency information security policies.

Serves as information security expert and confirms systems and contract alignment with agency and State information security policies.

- Serves as agency information security expert and provides advice and recommendations to agency executives on information security matters.

- Reviews the security features of new computing systems, change controls to existing systems, and external network connections to ensure that the technology systems meet existing security policies and standards.

- Develops or reviews contract, service level agreement, memorandum of understanding language, and other documents to verify that they meet information security needs and requirements and align with agency and State information security policies.

- Maintains guidelines for the development of secure application code using industry best practices.

- As CISO for agencies that host other agency applications, provides information security consultation services to customer or partner agencies, and directs the development of test scenarios to secure agency applications and data.

Monitors information security industry trends, tools, and techniques.

- Represents the agency at internal and external information security meetings and conferences to maintain awareness and evaluates the applicability of the latest information security techniques and tools to the agency's security program.

- Collaborates with peers to develop a multilayered and adaptive approach to counter a dynamic information security threat environment.

- In consultation with agency counsel, researches relevant laws and regulations that could affect the security controls and classification of information assets and approves adjustments to meet legal and regulatory requirements.

Manages staff and resources dedicated to an agency’s information security program.

- Prepares an information security staffing, development, and training plan to align with the agency’s risk management and information security plans.

- Develops metrics to measure the efficiency and effectiveness of the program, facilitates appropriate resource allocation and increases the maturity of the security program.

- Supervises staff and assigns work, writes performance and probationary evaluations, conducts interviews, and hires staff.

In addition, when assigned to a centralized information security management role for multiple State agencies:

- Develops, implements, and monitors a strategic, comprehensive information security and risk management program to ensure the integrity, confidentiality, and availability of information owned, controlled or processed by the agency.

- Provides information security expertise to executive management (e.g., agency heads, commissioners or executive chamber staff) on a broad range of information security standards and best practices.

- Provides strategic and tactical security guidance for all IT projects to ensure alignment between security and enterprise architectures.

Supervision Exercised

Chief Information Security Officers may supervise lower-level information security staff assigned to an information security unit. In smaller information security units, the positions direct and coordinate staff from different business units but may not be responsible for the regular supervision of these individuals.

Minimum Qualifications

Chief Information Security Officer

Non-competitive: bachelor’s degree* and four years of information technology experience, including three years of information security or information assurance experience and two years at a supervisory level.

*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 information technology, information security, or information assurance 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: 1/2022

PH