IT SECURITY AND COMPLIANCE

General Summary

IT Security and Compliance Administrators plan, execute, and manage multi-faceted projects related to risk management, mitigation and response, compliance, control assurance, and user awareness. These individuals are focused on developing and driving security strategies, policies/standards, ensuring the effectiveness of solutions, and providing security-focused consultative and training services to the organization. Administrators are responsible for ensuring information security and compliance with relevant legislation, legal interpretation, compliance and regulatory standards; they also select and implement appropriate tools for necessary surveillance and monitoring of the organization's computing environment. Security and Compliance Administrators also execute appropriate post-incident response including issue identification, containment, eradication, restoration and recovery. The IT Security and Compliance function shall not contain any day-to-day network or system administration responsibilities not involving IT security.

IT Security and Compliance Administrator I

Jobcode: ICSC20
Pay Band: ID
FLSA Status: Non Exempt

Distinguishing Characteristics

Under direct supervision, perform all procedures necessary to ensure the safety of information systems and technology assets and to protect systems from intentional or inadvertent access or destruction.

Recommended Education and Experience for Full Performance

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and two (2) years of experience in IT security or compliance validation (e.g. HIPAA, PCI) or systems administration, network operations or end user support. Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling six (6) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience.

Minimum Qualifications

Associate's Degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and two (2) years of experience in IT security, compliance validation (e.g. HIPAA, PCI) or systems administration, network operations or end user support. Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling four (4) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience.

*Essential Duties and Responsibilities**

1. Conducts monitoring of data security and implements controls as directed.
2. Monitors firewall configuration.
3. Conducts data security remediation such as security patching.
4. Reviews data logs and activities and notifies more senior staff of "exceptions."
5. Develops and delivers security awareness training.
6. Provides input to the preparation of disaster recovery plans.
7. Provides input to the preparation of Incident Response (IR) documents and plans.
8. Prepares documentation for all actions taken.
9. Evaluates system user access records to ensure accounts are current or terminated in a timely manner.
10. Develops security solutions for low to medium complex assignments.

11. Works on multiple projects as a security team member. Participates with team(s) to gather a full understanding of project scope and business requirements.
12. May participate in security planning and analyst activities.
13. Works with clients to identify security requirements using methods that may include risk and impact assessments.
14. Follows up on deficiencies identified in monitoring reviews, self-assessments, automated assessments, and internal and external audits to ensure that appropriate remediation measures have been taken.
15. Captures, maintains, and monitors information security risk in one repository.
16. Checks existing accounts and data access permission requests against documented authorizations.
17. Assists in the data classification process.
18. Develops and generates reports.

IT Security and Compliance Administrator II

Jobcode: ICSC23
Pay Band: IE
FLSA Status: Exempt

Distinguishing Characteristics

Under general supervision, perform all procedures necessary to ensure the safety of information systems and technology assets and data and to protect systems from intentional or inadvertent access or destruction. Performs security audits and provides management with status reports. Develops plans and requirements for disaster and incident response. Ensures information security and compliance with relevant legislation, legal interpretation, compliance and regulatory standards.

Recommended Education and Experience for Full Performance

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and four (4) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling eight (8) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience.

Minimum Qualifications

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and two (2) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling six (6) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience.

*Essential Duties and Responsibilities**

1. Performs audits to ensure that users are adhering to the necessary procedures and processes to maintain IT security and compliance. Monitors compliance with security policies, standards, guidelines and procedures.
2. Coordinates and collaborates with compliance/regulatory auditors during formal audits.
3. Collaborates with third party security agencies or companies in performing security assessments.
4. Provides input into the development, review and implementation of enterprise-wide security policies, procedures, and standards to meet compliance responsibilities.
5. Participates with team(s) to gather a full understanding of project scope and business requirements.
6. Participates in designing secure infrastructure solutions and applications.
7. Works directly with the clients, third parties and other internal groups to facilitate information security risk analysis and risk management processes and to identify acceptable levels of residual risk.

8. Conducts impact analysis to ensure resources are adequately protected with proper security measures.
9. Analyzes security analysis reports for security vulnerabilities and recommends feasible and appropriate options.
10. Creates, disseminates and updates documentation of identified information security risks and controls. Follows up on deficiencies identified in monitoring reviews, self-assessments, automated assessments, and internal and external audits to ensure that appropriate remediation measures have been taken.
11. Checks existing accounts and data access permission requests against documented authorizations.
12. Assists in the data classification process.
13. Reports on significant trends and vulnerabilities.
14. Assists in preparing disaster recovery plans.
15. May assist security forensic investigators.
16. Reviews, documents, and discusses violations of computer security procedures with the Information Security Officer to report incidents.
17. Monitors reports of computer security threats to determine changes in security stance.
18. Assists in the development of plans to safeguard computer configurations against accidental or unauthorized modification, destruction, or disclosure.
19. Provides guidelines and expertise for creating security awareness training for users to ensure IT system security and compliance.
20. Develops and reports, as required, on any security deficiencies identified as Corrective Action Plans (CAPs) resulting from an audit, and maintain Plans of Actions and Milestones (POAMs).

IT Security and Compliance Administrator III

Jobcode: ICSC26
Pay Band: IF
FLSA Status: Exempt

Distinguishing Characteristics

Independently performs all procedures necessary to ensure the safety of information systems assets and data and to protect systems from intentional or inadvertent access or destruction. Conducts the most complex IT data and security audits, and leads or assists with forensic investigations. Serves as project lead and may mentor lower level Security and Compliance Administrators.

Recommended Education and Experience for Full Performance

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and six (6) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling ten (10) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience.

Minimum Qualifications

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and four (4) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling eight (8) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience.

*Essential Duties and Responsibilities**

1. Develops and implements strategies to align information security with business objectives and goals, protecting the integrity, confidentiality and availability of data, in collaboration with the Chief Information

Security Officer. Provides analysis, consultation and training reflective of significant knowledge of intrusion detection and internet architecture.
2. Contributes to designing and implementing the enterprise-wide organization continuity and disaster recovery management programs, including maturity models, methodologies, sourcing, strategies, plans, metrics and scorecards for all components of the program(s).
3. Develops and implements internal reviews and audits to ensure compliance with standards and processes (selecting sample, verifying documentation and other requirements).
4. Assists business partners with the determination of critical business processes and systems.
5. Leads and responds to security incidents and investigations and targets reviews of suspect areas.
6. Ensures recovery drills are performed. Analyzes recovery drills performance and recommends changes to plan, as needed.
7. Conducts the most complex IT data and security reviews and audits for regulatory and standards compliance. Participates in third party security investigations and compliance reviews as requested.
8. Develops, reviews and audits criteria for lower level security analysts to ensure that users adhere to the necessary procedures and processes to maintain IT security.
9. Identifies and resolves root causes of security-related problems and related issues.
10. Consults with clients on security violations.
11. Leads the development and documentation of information security standards, best practices and guidelines.
12. Acts as liaison between internal audit and IT to ensure commitments are met and controls are properly implemented.
13. Oversees security incident and response management.
14. Defines security configuration and operations standards for security systems and applications, including policy assessment and compliance tools, network security appliances, and host-based security systems.
15. Defines and validates baseline security configurations for operating systems, applications, networking and telecommunications equipment.
16. Interfaces with third-party vendors to evaluate new security products or as part of a security assessment process. Maintains contact with vendors regarding security system updates and technical support of security products.
17. Coordinates with vendors to ensure managed services are implemented and maintained appropriately.
18. Reviews and delivers information security performance summary with analytical evaluation to leadership teams, as needed. Identifies areas needing improvement and develops recommendations.
19. Leads and reviews application security risk assessments for new or updated internal or third party applications.
20. Evaluates and recommends tools and solutions that provide security functions.
21. May assist security forensic investigators.
22. Provides advice to management on "balance" between business needs and data security.
23. Mentors and trains team members and peers on security solutions and actively participates on system and application improvement project teams. Serves as a project lead on security-related matters.

IT Security and Compliance Supervisor

Jobcode: ICSS26
Pay Band: IF
FLSA Status: Exempt

Distinguishing Characteristics

Supervises a team of Security and Compliance Administrators who provide agency-wide information security programs, processes, compliance, evaluation, mitigation, and response. Ensures delivery of processes that reflect a deep understanding of information security regulations such as, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), ISO 27001 and 27018, Sarbanes-Oxley (SOX), Cloud Security Alliance (CSA), Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), Service Organization Control 2 (SOC2), Federal

Information Processing Standard (FIPS), and Family Educational Rights and Privacy Act (FERPA). Coordinates IT data and security audits with third parties, Security and Compliance Administrators and management and leads or assists with forensic investigations.

Recommended Education and Experience for Full Performance

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and six (6) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling ten (10) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience. At least two (2) years of which must be leading/supervising a security team.

Minimum Qualifications

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and four (4) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling eight (8) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience.

Essential Duties and Responsibilities*

1. Provides guidance and counsel to the agency CIO and executive management to define objectives for information security.
2. Leads the development and implementation of effective policies, processes and practices to secure protected and sensitive data; ensure information security and compliance with relevant legislation and legal interpretation.
3. Exercises full management responsibility for a technical group, including recruiting, hiring, training, developing, evaluating, and setting priorities within the scope of the agency's IT Security strategic plan.
4. Ensures work completion within schedule, budgetary, and design constraints; makes decisions about analysis, design, and testing; solves complex technical problems; provides alternative methods for achieving goals when necessary.
5. Works with business unit managers to ensure employees are aware of cybersecurity issues, are trained in good cybersecurity practices, and are practicing safe/secure data collection, data transfers and storage, and use of social media, mobile devices, and apps, among others. Develops enterprise education and communication plan.
6. Develops and maintains IT Audit and Forensics processes. Conducts risk assessments to properly analyze the risks to information assets.
7. Ensures organization continuity and disaster recovery plans are documented and maintained.
8. Provides leadership for all security incidents and acts as primary technical control point during significant information security incidents.
9. Oversees contractor/vendor work performance related to IT Security and Compliance efforts.
10. Coordinates the administration and logistical procedures for disaster recovery testing, and integration of all enterprise "critical" systems. Identifies and coordinates resolution of information security recovery issues.
11. Analyzes recovery drills performance and recommends changes to plan, as needed.
12. Ensures coordination of all IT internal and external assessment components.
13. Reviews and delivers information security performance summary with analytical evaluation to leadership teams, as needed. Identifies areas needing improvement and develops recommendations.
14. Recommends tools and solutions that provide security functions. Oversee key technologies such as ClearWell, RSA Archer.

15. Provides direct leadership to the information security team by setting, communicating and modeling high standards of performance, professionalism, and confidentiality; developing and maintaining a high level of work ethic and personal credibility with staff; and demonstrating consistent, sound judgment.

IT Security and Compliance Manager I
Jobcode: ICSX30
Pay Band: IG
FLSA Status: Exempt

Distinguishing Characteristics
Serve as Chief Information Security Officer for an agency. Responsible for the strategic leadership of the agency's information security programs, processes, compliance, evaluation, mitigation and response.

Essential Duties and Responsibilities*
1. Responsible for the strategic leadership of the agency's information systems and security programs.
2. Provides guidance and counsel to the agency CIO and executive management to define objectives for information security.
3. Establishes annual and long-range security and compliance goals, define security strategies, metrics, reporting mechanisms and program services; create maturity models and a roadmap for continual security program improvements.
4. Leads the development and implementation of effective policies and practices to secure protected and sensitive data; ensure information security and compliance with relevant legislation and legal interpretation.
5. Develops, maintains and oversees agency policies, processes and control techniques to address all applicable information security requirements and standards.
6. Provides leadership for all security incidents and acts as primary control point during significant information security incidents.
7. Exercises full management responsibility for a technical group, including recruiting, hiring, training, developing, evaluating, and setting priorities.
8. Ensures work completion within schedule, budgetary, and design constraints; makes decisions about analysis, design, and testing; solves complex technical problems; provides alternative methods for achieving goals when necessary.
9. Approves technical changes for presentation to the CIO or an agency Change Control Board, schedules projects, and manages timelines. Implements and monitors quality standards.
10. Manages vendor relations.
11. Demonstrates effective project management processes and outcomes in incident response and remediation.
12. Designs and implements the enterprise-wide organization continuity and disaster recovery management programs, including maturity models, methodologies, sourcing, strategies, plans, metrics and scorecards for all components of the program(s).
13. Develops risk management procedures, organization continuity scenarios, and contingencies and advises on organization continuity and disaster recovery plans.
14. Identifies and makes recommendations regarding critical points of failure. Recommends changes required to expand recovery plans. Reviews select changes to ensure they are appropriately assessed, tested, and incorporated into the larger enterprise plan.
15. Ensures organization continuity and disaster recovery plans are documented and maintained.
16. Contributes to senior management reports on the impact, cost, and expectations of the enterprise disaster recovery plan.
17. Coordinates, assesses and communicates requirements associated with impact, continuity, and recovery.
18. Works across IT domains to incorporate recommendations and enable timely, effective decisions regarding impact, continuity and recovery. Represents organization's security and IT risks among other organization or state risk management/security committees.

19. Coordinates the administration and logistical procedures for disaster recovery testing, and integration of all enterprise "critical" systems. Identifies and coordinates resolution of information security recovery issues.
20. Analyzes recovery drills performance and recommends changes to plan, as needed.
21. Ensures coordination of all IT internal and external assessment components.
22. Develops measures to evaluate the information security programs and modifies strategies as appropriate.
23. Reviews and delivers information security performance summary with analytical evaluation to leadership teams, as needed. Identifies areas needing improvement and develops recommendations.
24. Approves recommended tools and solutions that provide security functions.
25. Performs cost-benefit and risk analysis.

Recommended Education and Experience for Full Performance

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and eight (8) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling twelve (12) years may substitute for the required education and experience. At least two (2) years of which must be leading/supervising a security team. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience. At least four (4) years of which must be supervising an applications development team.

Minimum Qualifications

Bachelor's degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and six (6) years of experience in IT security and compliance. Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling ten (10) years may substitute for the required education and experience. At least two (2) years of which must be leading/supervising a security team. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience. At least two (2) years of which must be supervising an applications development team.

IT Security and Compliance Manager II

Jobcode: ICSX40
Pay Band: II
FLSA Status: Exempt

Distinguishing Characteristics

Serve as Chief Information Security Officer (CISO) at DoIT. Responsible for developing statewide IT security and compliance functions in the following areas: strategic planning and evaluation, policy, compliance, audit, education, risk management and incident response, and assessment of emerging technologies and vulnerabilities. Deploys strategies aimed at protecting and securing the state's data, systems, and infrastructure.

Recommended Education and Experience for Full Performance

Bachelor's Degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and twelve (12) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling sixteen (16) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience. At least six (6) years of supervising a security/compliance team(s).

Minimum Qualifications

Bachelor's Degree in Computer Science, Management Information Systems (MIS), Information Technology, Engineering or similar technical degree and ten (10) years of experience in IT security or compliance validation (e.g. HIPAA, PCI). Any combination of education from an accredited college or university in a related field and/or direct experience in this occupation totaling fourteen (14) years may substitute for the required education and experience. A certificate in IT security/forensics (e.g. CISSP, CEH, CCFP, CCSP, HCISPP, SSCP) or regulated compliance (e.g. PCIP, ASV, ISA, QSA) can be used to substitute one year of experience. At least four (4) years of supervising a security/compliance team.

Essential Duties and Responsibilities*

1. Responsible for the strategic leadership of the state's information security programs.
2. Provides guidance and counsel to the state CIO and executive management to define objectives for information security.
3. Works with agency CISOs or CIOs to oversee the formation and operations of an integrated statewide information security organization that is organized toward a common goal and standards in information security.
4. Leads information security planning processes to establish an inclusive and comprehensive information security program for the entire state in support of all businesses and services.
5. Establishes annual and long-range security and compliance standards and goals, define security strategies, metrics, reporting mechanisms and program services; create maturity models and a roadmap for continual program improvements.
6. Leads the development and implementation of effective and policies and practices to secure protected and sensitive data; ensures information security and compliance with relevant legislation and legal interpretation.
7. Provides leadership philosophy for the Information Security Office to create a strong bridge between organizations; brings groups together to share information and resources to create better decisions, policies and practices for the state.
8. Develops, maintains and oversees policies, processes and control techniques to address all applicable information security requirements.
9. Provides leadership for all security incidents and acts as primary control point during significant information security incidents.
10. Manages statewide information security governance processes; chairs or leads security-related advisory committees.
11. Provides leadership in the communication of state security standards for information technology across all state agencies.

Bargaining Unit: **Not represented.**

Statutory Requirements:

Conditions of Employment:

Working Conditions: Working Conditions for individual positions in this classification will vary based on each *agency's utilization*, *essential functions* and the *recruitment needs* at the time a vacancy is posted. All requirements are subject to possible modification to reasonably accommodate individuals with disabilities.

Established: 6/16/2016 **Revised: 08/25/2018 (Supervisor added)**

**Essential Duties and Responsibilities are intended to be cumulative for each progressively higher level of work. The omission of specific statements does not preclude management from assigning other duties which are reasonably within the scope of duties. Classification description subject to change. Please refer to SPO website (www.spo.state.nm.us) to ensure this represents the most current copy of the position.*

*** Means two (2) or any combination of full-time equivalent (FTE) status that equals at least two (2) regular or term status employees in non-temporary positions.*