South Carolina – Division of State Human Resources

InfoSec / Privacy Workforce Position Descriptions (PDs)

Contents

About this Document

The Division of Information Security (DIS), Enterprise Privacy Office (EPO), and Human Resources Division (HRD) have identified 12 unique positions (both new and existing) that can perform the roles and responsibilities necessary to support information security and privacy for the State. These positions are divided into the following groups:

- Core positions: Positions that are dedicated full-time to information security and/or privacy roles
- Hybrid positions: Positions that have both information security or privacy and non-information security or privacy roles and responsibilities

Position Descriptions were created to capture the roles and responsibilities of these information security and privacy positions and to aid in the hiring, performance management, and retention of personnel, where appropriate. The Position Descriptions include position requirements; knowledge, skills, and abilities (KSAs); reporting structure; and job purpose and functions.

Information Privacy Analyst I

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - Zero to three years of experience in the area of information privacy administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to understand information privacy laws, policies, procedures, and technology.
   - Basic knowledge of information privacy risks in systems, networks, and data.
   - Basic knowledge of data classification levels within the State of South Carolina's data classification schema and their applications.
   - Basic understanding of the information privacy incident response as it relates to privacy incidents.
   - Basic understanding of the data lifecycle (e.g., identification, use, access, transmission, storage, and destruction of data).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Privacy Analyst I position[1] will be under the supervision of the Information Privacy Analyst II/III or Information Privacy Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Privacy Analyst I is primarily responsible for assisting senior analysts (Information Privacy Analysts II and III) in enforcing, evaluating and monitoring compliance requirements related to the Privacy program of the organization. The Information Privacy Analyst I will participate in investigations of privacy complaints and incidents, collection of data, and report of findings to management[2].

6. **Job Functions:**
   - Performs research and supports evaluation of the organization's Privacy program and associated policies, standards, procedures, and controls.
   - Supports the development of Privacy compliance documentation to guide employees in confirming that privacy is incorporated into the organization's processes, initiatives, and development of information systems.
   - Assists senior analysts in classifying information assets across the organization based on the data classification schema.

---

[1] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level privacy position in the organization, it is recommended that reporting duties be coordinated with agency leadership and that the employee have at least two years of experience .

[2] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

- Monitors the status and effectiveness of privacy controls across departments and provides reporting and escalation, when needed.
- Assists in the investigation and documentation of privacy complaints and reports results to management.
- Assists senior analysts in performing reviews of information systems and/or processes to identify privacy-related vulnerabilities.
- Participates in the response plan for violations of the organization's Privacy program and associated policies, and provides communication to internal departments, including remediation steps.
- Assists in deployment of Privacy training awareness and communication programs to educate and update employees on privacy requirements.

Information Privacy Analyst II

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - Three to five years of experience in the area of information privacy administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information privacy laws, policies, procedures, and technology.
   - Knowledge of the State of South Carolina's data classification schema and its application.
   - Experience with the data lifecycle (e.g., identification, use, access, transmission, storage, and destruction of data).
   - Understanding of the incident response process as it relates to privacy incidents.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures, and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), American Institute of Certified Public Accountants (AICPA).
   - Preferred, but not required, certification may include: Certified Information Privacy Professional/U.S. Government (CIPP/G) or Certified Information Privacy Professional/U.S. Privacy-Sector (CIPP/US).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Privacy Analyst II position[3] will be under the supervision of the Information Privacy Analyst III or Information Privacy Manager but may occasionally lead small projects independently.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Privacy Analyst II is primarily responsible for implementing the organization's Privacy program and associated policies. They will monitor the effectiveness of privacy controls and conduct investigations into privacy complaints and incidents.

6. **Job Functions:**
   - Contributes to the implementation of the Privacy program and associated policies, standards, procedures, and controls within the organization.

[3] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level privacy position in the organization, it is recommended that reporting duties be coordinated with agency leadership and that the employee have at least two years of experience .

- Works with senior analysts (Information Privacy Analyst III) to define and incorporate privacy controls into the organization's processes, initiatives, and development of information systems.
- Identifies information assets and classifies them based on their level of sensitivity, value, and criticality to the organization, in line with the data classification schema.
- Works with senior analysts to provide mitigation for privacy risks.
- Investigates privacy complaints and adopts the appropriate steps to respond to, and address, the complaints.
- Works with Privacy Manager to Identify and investigate privacy incidents that violate the organization's Privacy program.
- Supports management[4] role as a liaison for any complaints and/or investigations related to privacy.
- Supports the development of Privacy training and communication programs to educate and update employees on privacy requirements.

[4] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Privacy Analyst III

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - More than five years of experience in the area of information privacy administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information privacy laws, policies, procedures and technology.
   - Knowledge of the State of South Carolina's data classification schema and its application.
   - Experience with the data lifecycle (e.g., identification, use, access, transmission, storage and destruction of data).
   - Understanding of the incident response process as it relates to privacy incidents.
   - Knowledge of applicable privacy trends and best practices.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), American Institute of Certified Public Accountants (AICPA).
   - Preferred, but not required certification may include: Certified Information Privacy Professional/U.S. Government (CIPP/G) or Certified Information Privacy Professional/U.S. Privacy-Sector (CIPP/US).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Privacy Analyst III position[5] will work with minimal supervision, reporting to the Information Privacy Manager or Agency Privacy Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Privacy Analyst III is primarily responsible for collaborating with cross-functional teams to develop, implement, and promote the organization's Privacy program and associated policies. They will monitor all privacy-related policies, standards, procedures and controls within the organization to identify vulnerabilities and risks.

6. **Job Functions:**
   - Collaborates with management[6] to develop and implement the privacy program and associated policies, standards, procedures, and controls within the organization.

[5] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level privacy position in the organization, it is recommended that reporting duties be coordinated with agency leadership and that the employee have at least two years of experience.

[6] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

- Provides mentorship and guidance to Privacy staff; provides relevant technical training and guidance to staff and other departments.
- Provides subject matter expertise to confirm privacy is incorporated into the organization's processes, initiatives, and development of information systems.
- Enforces the data classification schema to classify information assets based on the data's level of sensitivity, value, and criticality to the organization.
- Collaborates with management to review controls to help maintain the privacy of the organization's data.
- Performs review of information systems and/or processes to identify privacy-related vulnerabilities.
- Works with management to provide mitigation for privacy risks.
- Leads investigations of privacy complaints and reports findings to management.
- Develops a response plan for violations of the organization's Privacy program and associated policies.
- May serve as a liaison to regulatory and accrediting bodies for matters relating to privacy.
- Performs research and advises management on applicable privacy trends and best practices.

Information Privacy Manager I

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - Four to six years of experience in the area of information privacy administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information privacy laws, policies, procedures, and technology.
   - Knowledge of the State of South Carolina's data classification schema and its application.
   - Experience with the appropriate handling of data throughout the lifecycle (e.g., identification, use, access, transmission, storage, and destruction of data).
   - Ability to synthesize information and communicate privacy concepts to technical and non-technical audiences
   - Ability to apply information privacy principles to business processes.
   - Knowledge of applicable privacy trends and best practices.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., Agency privacy policies and procedures; Fair Information Practice Principles, National Institute of Standards and Technology (NIST) and U.S. Office of Management and Budget privacy memoranda).
   - Preferred, but not required certification may include: Certified Information Privacy Professional/U.S. Government (CIPP/G), Certified Information Privacy Professional/U.S. Private-Sector (CIPP/US), or Certified Information Privacy Manager (CIPM).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Privacy Manager I position[7] will be under the supervision of the Information Privacy Manager II/III or Agency Privacy Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Privacy Manager I is primarily responsible for supporting the development and implementation of the organization's Privacy program and associated policies. They will monitor compliance activities to provide mitigation for privacy risks.

[7] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level privacy position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. Job Functions:

- Supports senior managers (Information Privacy Manager II and III) in developing and implementing the Privacy program and associated policies, standards, procedures and controls within the organization.
- Provides mentorship, guidance, and relevant privacy training to other Privacy staff and other staff members of the organization.
- Maintains awareness of changes in laws, regulations, or organization policy to recommend needed revisions to the Privacy program and to advise management[8] regarding applicable privacy trends and best practices.
- Collaborates with other departments (e.g., legal, compliance, HR) to monitor compliance with privacy requirements to confirm these requirements are appropriately implemented and enforced.
- Works across the organization's business units and departments to implement the data classification schema for classifying data based on the data's level of sensitivity, value, and criticality to the organization.
- Manages and performs privacy risk assessments and privacy compliance monitoring activities, and analyzes results to recommend mitigation for privacy risks associated with non-compliance.
- Provides guidance on controls to help secure and maintain the organization's data.
- Works with appropriate staff to execute against the organization's response plan for privacy incidents.
- Confirms the organization maintains appropriate privacy and confidentiality consent, authorization forms, information notices, and materials reflecting the organization's current Privacy program.
- May serve as a liaison to regulatory and accrediting bodies for matters relating to privacy.

[8] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Privacy Manager II

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - Three to five years of management experience.
   - Seven to ten years of experience in the area of information privacy administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information privacy laws, policies, procedures, and technology.
   - Knowledge of the State of South Carolina's data classification schema and its application.
   - Experience the management of data throughout the lifecycle (e.g., identification, use, access, transmission, storage and destruction of data).
   - Experience in performing privacy risk assessments and audits.
   - Experience in conducting privacy impact assessments.
   - Experience in incident response as it relates to privacy incidents.
   - Strong situational analysis and decision-making abilities.
   - Ability to apply information privacy principles to business practices.
   - Knowledge of applicable privacy trends and best practices.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., Agency privacy policies and procedures; Fair Information Practice Principles, National Institute of Standards and Technology (NIST), and U.S. Office of Management and Budget privacy memoranda).
   - Preferred, but not required certification may include: Certified Information Privacy Professional/U.S. Government (CIPP/G), Certified Information Privacy Professional/U.S. Private-Sector (CIPP/US), or Certified Information Privacy Manager (CIPM).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Privacy Manager II position[9] will be under the supervision of the Information Privacy Manager III or Agency Privacy Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

[9] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level privacy position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

5. **Job Purpose:**
   - The Information Privacy Manager II is primarily responsible for developing and implementing the organization's Privacy program. They will also provide subject matter expertise on the review and revision processes of the organization's existing Privacy program. They will work to raise privacy awareness across the organization.

6. **Job Functions:**
   - Works with organization's management[10] to implement and enforce a Privacy program and associated policies, standards, procedures and controls within the organization.
   - Provides mentorship, guidance, and relevant privacy training to other privacy staff and other staff members of the organization.
   - Maintains awareness of changes in laws, regulations, or organization policy to recommend needed revisions to the privacy program and to advise management of applicable privacy trends and best practices.
   - Collaborates with other departments (e.g., legal, compliance, HR) to monitor the organization's compliance with privacy requirements to confirm these requirements are appropriately implemented and enforced.
   - Leverages the data classification schema to classify the organization's data to protect the data's confidentiality, integrity, and availability.
   - Provides guidance to management for mitigation of privacy risks identified in risk assessments and compliance monitoring activities.
   - Establishes and administers processes and procedures for receiving, documenting, tracking, and investigating complaints concerning the organization's privacy program.
   - Works with appropriate staff to execute against the organization's response plan for privacy incidents.
   - Raises privacy awareness across the organization by providing education, training, and regular communications on privacy requirements.
   - May serve as a liaison to regulatory and accrediting bodies for matters relating to privacy.
   - Performs research and advises management on applicable privacy trends and best practices.

[10] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Privacy Manager III

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - More than five years of privacy management experience.
   - More than ten years of experience in the area of information privacy administration.
   - Educational background or work experience in the legal field is desirable.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information privacy laws, policies, procedures, and technology.
   - Knowledge of the State of South Carolina's data classification schema and its application.
   - Experience the management of data throughout the lifecycle (e.g., identification, use, access, transmission, storage and destruction of data).
   - Experience in performing privacy risk assessments, privacy impact assessments, and audits.
   - Experience in incident response as it relates to privacy incidents.
   - Knowledge of user access management requirements and controls.
   - Ability to apply information privacy principles to business practices.
   - Strong situational analysis and decision-making abilities.
   - Ability to effectively communicate complex and sensitive topics.
   - Expert knowledge of applicable privacy trends and best practices.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., Agency privacy policies and procedures; Fair Information Practice Principles; National Institute of Standards and Technology (NIST), and U. S. Office of Management and Budget privacy memoranda).
   - Preferred, but not required certification may include: Certified Information Privacy Professional/U.S. Government (CIPP/G), Certified Information Privacy Professional/U.S. Private-Sector (CIPP/US), or Certified Information Privacy Manager (CIPM).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Privacy Manager III position[11] will be under the supervision of the Agency Privacy Officer, if applicable.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

[11] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level privacy position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

5. **Job Purpose:**
    - The Information Privacy Manager III is primarily responsible for developing and overseeing the implementation of a Privacy program that outlines the organization's privacy vision, mission, and goals. They will develop and enforce information privacy policies, standards, procedures and controls to confirm compliance with applicable laws and regulations**.**

6. **Job Functions:**
    - Collaborates with management[12] to develop a Privacy program that outlines the organization's privacy vision, mission and goals.
    - Provides mentorship, guidance, and relevant privacy training to other privacy staff and other staff members of the organization.
    - Reviews and revises the privacy program on a periodic basis in light of changes in laws, regulations, or company policy.
    - Reports on a periodic basis the status of the Privacy program to organization's stakeholders and/or management.
    - Provides subject matter expertise of applicable state privacy policies, standards, procedures, and controls to confirm they are appropriately embedded in the organization's privacy practices.
    - Leverages the data classification schema to establish a procedure to classify the organization's data to protect its confidentiality, integrity, and availability.
    - Establishes controls to help maintain the privacy of the organization's data.
    - Leads privacy impact assessments to identify privacy risks and potential impacts associated with processes, data, and systems that are privacy-sensitive.
    - Work with the organization's business units and departments to develop a response plan for privacy incidents.
    - May serve as a liaison to regulatory and accrediting bodies for matters relating to privacy.
    - Serves as the overall liaison for any complaints and/or investigations related to privacy.

[12] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Agency Privacy Officer (APO)

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - More than five years of privacy management experience.
   - More than ten years of experience in the area of information privacy administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information privacy laws, policies, procedures, and technology.
   - Knowledge of the State of South Carolina's data classification schema and its application.
   - Experience with the management of data throughout the lifecycle (e.g., identification, use, access, transmission, storage and destruction of data).
   - Experience in performing privacy risk assessments, privacy impact assessments, and audits.
   - Experience in incident response as it relates to privacy incidents.
   - Knowledge of user access management requirements and controls.
   - Expert knowledge of applicable privacy trends and best practices.
   - Strong situational analysis and decision making abilities.
   - Ability to apply information privacy principles to business processes.
   - Ability to effectively communicate complex and sensitive topics.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., Agency privacy policies and procedures; Fair Information Practice Principles; National Institute of Standards and Technology (NIST), and U.S. Office of Management and Budget privacy memoranda).
   - Ability to obtain the following certifications: Certified Information Privacy Professional/U.S. Government (CIPP/G), Certified Information Privacy Professional/U.S. Private-Sector (CIPP/US), or Certified Information Privacy Manager (CIPM).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Agency Privacy Officer (APO) position[13] will report to the respective Agency Director and/or Chief Operating Officer (COO).

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The APO is primarily responsible for developing and overseeing the implementation of a Privacy program that outlines the organization's privacy vision, mission, and goals. They

[13] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level privacy position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

will develop and enforce information privacy policies, standards, procedures and controls to confirm compliance with applicable laws and regulations.

6. Job Functions:

- Leads the development and maintenance of the agency's information privacy program and associated strategies with consideration for the business processes and overall goals of the organization.
- Provides mentorship, guidance, and relevant privacy training to other privacy staff and other staff members of the organization.
- Reviews and revises the privacy program on a periodic basis in light of changes in laws, regulations, or company policy.
- Updates Agency Directors and/or COOs on agency-related information privacy status (risks, issues, mitigation plans).
- Reports on a periodic basis the status of the Privacy program to organization's stakeholders and/or management.
- Provides subject matter expertise of applicable state privacy policies, standards, procedures, and controls to confirm they are appropriately embedded in the organization's privacy practices.
- Leverages the data classification schema to establish a procedure to classify the organization's data to protect its confidentiality, integrity, and availability.
- Establishes controls to help maintain the privacy of the organization's data.
- Leads privacy impact assessments to identify privacy risks and potential impacts associated with processes, data, and systems that are privacy-sensitive.
- Works with the organization's business units and departments to develop a response plan for privacy incidents.
- May serve as a liaison to regulatory and accrediting bodies for matters relating to privacy.
- Serves as the overall liaison for any complaints and/or investigations related to privacy.

Information Security Analyst I

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - Zero to three years of experience in areas of information security administration, network administration and/or information technology administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to understand and apply information technology and security concepts.
   - Basic knowledge of potential vulnerabilities and deviations from standard information security practices.
   - Basic knowledge of operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), cloud computing, networks, hardware and software platforms, and protocols as they relate to information security.
   - Basic knowledge of the principles, methods, and tools used for evaluating risks.
   - Basic knowledge of data collection, transmission and storage methods.
   - Basic knowledge of procedures, tools and applications used to preserve data confidentiality, integrity and availability.

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Analyst I position[14] will be under direct supervision of the Information Security Analyst II/III or Information Security Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Analyst I is primarily responsible for operations of information security measures, processes and controls to protect the organization's information systems, networks and data. They will also support senior analysts (Information Security Analysts II and III) to evaluate and identify information security risks and threats and escalate information security issues to management[15], as needed.

6. **Job Functions:**
   - Applies available resources to support the enforcement of security processes in compliance with applicable information security policies, standards, procedures and controls.

[14] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

[15] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

- Monitors the organization’s systems and networks and supports investigation of information security incidents.
- Implements information security systems, such as firewalls and data encryption, and other applications to protect organization information.
- Provides timely reports to management, as required, to address or mitigate threats.
- Assists in implementing and testing disaster recovery plans.
- Supports information security risk assessments, IT audits and/or vulnerability assessments.
- Reviews firewall and router rules and access control lists.
- Works with senior analysts to conduct information security investigations following a potential compromise of organization systems, network or data.
- Supports local operation and maintenance of information security tools and processes.
- Supports tests and surveys of the organization’s information security controls to assist management in identifying and addressing information security risks and threats.
- Assists senior analysts to prepare information security reports, detailing the progress of specified activities, such as audits, vulnerability tests and incident management.
- Supports tests and surveys of the organization’s facilities to minimize environmental risks.

Information Security Analyst II

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - Three to five years of experience in areas of information security administration, network administration and/or information technology administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Understanding of information technology and security concepts.
   - Experience in the installation, setup and operation of IT infrastructure (e.g., routers, switches, firewalls, data encryption and intrusion protection devices).
   - Knowledge of operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), cloud computing, networks, hardware and software platforms, and protocols as they relate to information security.
   - Experience in performing vulnerability assessments, including scanning, analysis of results, and manual validation.
   - Experience in information security incident response and risk management.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required certifications may include: Certified Information Systems Security Professional (CISSP), or Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including employee independence and discretion.**
   - The Information Security Analyst II position[16] will be under the supervision and guidance of the Information Security Analyst III or Information Security Manager, but may occasionally lead small projects independently.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Analyst II is primarily responsible for planning and implementing information security measures to protect the organization's information systems, networks and data, including evaluation of system and infrastructure security controls against requirements to identify and recommend improvement opportunities.

[16] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. **Job Functions:**
    - Determines resources available to support enforcement of security processes in conformance with applicable information security policies, standards, procedures and controls.
    - Monitors potential information security threats to the organization's systems, networks and data.
    - Identifies information security opportunities and recommends process or technology enhancements.
    - Coordinates across the organization disaster recovery and business continuity activities.
    - Assists information security engineers to plan and perform information security risk and vulnerability reviews, including penetration tests and security design reviews, to identify vulnerabilities in the organization's systems.
    - Assesses the impact of external actions on the organization's information systems and networks, and determines if an information security incident has occurred.
    - Conducts information security investigations following a potential compromise of information systems, networks or data.
    - Prepares reports that document the extent of damage (cost, reputation, etc.) to the organization by an information security incident.
    - Plans and performs maintenance of information security solutions and tools.
    - Provides training to organization employees on information security procedures.

Information Security Analyst III

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - More than five years of experience in areas of information security administration, network administration and/or information technology administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information technology and security concepts.
   - Experience in the installation, setup and operation of IT infrastructure (e.g., routers, switches, firewalls, data encryption and intrusion protection devices).
   - Knowledge of operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), cloud computing, networks, hardware and software platforms, and protocols as they relate to information security.
   - Experience performing vulnerability scanning execution, assessment, and analysis.
   - Experience managing and responding to information security risks, threats and incidents.
   - Expert knowledge of applicable information security trends and best practices.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required certifications may include: Certified Information Systems Security Professional (CISSP), or Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including employee independence and discretion.**
   - The Information Security Analyst III position[17] will work with minimal supervision, reporting to the Information Security Manager. The Information Security Analyst III will lead and/or participate in cross-functional groups.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Analyst III is primarily responsible for assessing and evaluating the organization's information security solutions and processes, as well as providing technical advisory to influence the design and implementation of security information technology systems and networks. The Information Security Analyst III will guide junior analysts (Information Analysts I and II) to identify and address risks, and lead the response to information security issues.

[17] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. **Job Functions:**
    - Collaborates with management[18] to adapt or enhance existing resources to maintain and deploy information security processes within the organization in compliance with information security policies, standards, procedures and controls.
    - Provides mentorship and guidance to junior staff; provides relevant technical training and guidance to junior analysts and other departments.
    - Leads junior analysts in core information security functions (for example, installation, configuration and maintenance of information security equipment including firewalls, intrusion protection systems, and routers).
    - Collaborates with management to design and implement long-term information security strategies.
    - Leads post-incident forensic investigations.
    - Analyses and reports results of vulnerability and penetration tests.
    - Reviews information security incidents within the organization and discusses procedures with appropriate staff to make certain incidents are not repeated.
    - Develops, tests and guides implementation of disaster recovery plans in case of an information security incident.
    - Develops standards and other related guidance for threat management.
    - Monitors use and regulates access to safeguard organization information.
    - Advises management on data deletion and restoration incorporating external knowledge of data backup and restoration tools.

[18] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Security Architect I

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - Zero to three years of experience with enterprise information security architecture and information security system design.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to understand and apply concepts of information security principles.
   - Basic understanding of information security technologies, such as identity and access management, encryption, and multi-factor authentication, among others.
   - Basic understanding of dependencies and distinctions between business information systems and technology architecture layers.
   - Basic knowledge of information security design elements of operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), cloud systems and network platforms.
   - Experience in performing and analyzing results of network/infrastructure and applications vulnerability assessments and penetration tests.
   - Experience in responding to information security threats and incidents.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required certifications may include: Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Architect I position[19] will be under the supervision and guidance of the Information Security Architect II/III or Information Security Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Architect I is primarily responsible for supporting the design and implementation of the organization's information security architecture, in alignment with applicable information security policies, standards, procedures and controls.

[19] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. Job Functions:

- Maintains information security policies, standards, procedures and controls to protect information systems architecture, that may include data center, server, network, storage, applications, and related access controls.
- Assists in the design and development of technical security requirements for network infrastructure and applications.
- Collaborates with senior architects (Information Security Architect II and III) to integrate security controls into a cohesive architecture that sufficiently mitigates risk to the organization.
- Assists senior architects and management[20] in the implementation of information security program tools and solutions.
- Participates in information security projects to implement architecture and design recommendations to achieve effective and efficient solutions.
- Works closely with information technology and other business functions to confirm that security requirements are addressed in all phases of an information security project lifecycle.
- Assists in information technology audits by developing, executing and analyzing results from test scripts and other tools.
- Supports information security vulnerability assessments, including penetration tests and security design reviews, and the analysis of results.
- Researches new tools and techniques to enhance information security practices.

[20] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Security Architect II

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - Three to five years of experience with enterprise information security architecture and information security system design.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to understand and apply concepts of information security principles.
   - Understanding of information security technologies, such as identity and access management, encryption, and multi-factor authentication, among others.
   - Technical proficiency in broader areas of information technology, including operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), servers, cloud computing, networks, desktops and mobile devices.
   - Experience in managing and responding to information security risks, threats and incidents.
   - Experience in performing, analyzing and reporting results of network/infrastructure and applications vulnerability assessments and penetration tests.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required certifications may include: Certified Information Systems Security Professional (CISSP), or Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Architect II position[21] will be under the supervision of the Information Security Architect III or Information Security Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Architect II is primarily responsible for defining, enhancing, testing and implementing the organization's information security architecture, while ensuring consistent administration of information security policies, standards, procedures and controls to effectively improve security posture.

[21] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. **Job Functions:**
    - Designs, implements and tests information security controls to protect the organization's information security architecture, including data center, server, networks, storage, applications and related access controls.
    - Recommends and develops information security measures to protect the organization's information against unauthorized data modification or loss.
    - Partners with management[22] to confirm that security is integrated into the information systems and applications used by the organization.
    - Conducts technology and vendor assessments to validate that information security technology portfolios are kept up to date and meet contractual requirements.
    - Specifies intrusion detection and prevention methodologies and enhancements to information security systems; directs equipment and software installation and calibration.
    - Manages infrastructure vulnerability and compliance monitoring and reporting, including coordination of related governance and remediation activities across the organization.
    - Monitors information technology audits to identify risks and potential improvement opportunities.
    - Develops key indicators of malicious activities and confirms that mitigation and detection measures are designed and built into applications.
    - Collaborates with appropriate staff on the review of existing technology infrastructure and provides recommendations on information security implications.

[22] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Security Architect III

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - More than five years of experience with enterprise information security architecture and information security system design.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to understand and apply concepts of information security principles.
   - Advanced knowledge of information security technologies, such as identity and access management, encryption, and multi-factor authentication, among others.
   - Technical proficiency in areas of information technology, including operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), cloud computing, servers, networks, desktops and mobile devices.
   - Experience in managing and responding to information security risks, threats and incidents.
   - Experience in performing, analyzing and presenting results of vulnerability assessments and penetration tests.
   - Ability to develop executive reports based on findings for presentation to leadership
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required certifications may include: Certified Information Systems Security Professional (CISSP), or Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Architect III position[23] will be under the supervision of the Information Security Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Architect III is primarily responsible for leading the development of organization-wide information security architectures and design. They will also lead research, development and recommendation of technical and architectural security practices for current and future information security initiatives within the organization from definition phase through implementation and monitoring.

[23] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. **Job Functions:**
    - Collaborates with management[24], security teams and other stakeholders to determine information security needs and requirements for wide area networks (WANs), local area networks (LANs), virtual private networks (VPNs), firewalls, routers, and related security and network devices.
    - Provides mentorship and guidance to junior staff; provides relevant technical training and guidance to junior architects and other departments.
    - Influences the overall information security strategy for new and existing technology solutions, while considering potential risks in the organization's current technology deployments.
    - Reviews the organization's information security architecture and platforms to identify integration issues and opportunities to enhance information security practices.
    - Monitors and provides input at key checkpoints throughout the program or project lifecycle.
    - Leads remediation activities or projects within the organization and collaborates with impacted business functions in remediation.
    - Leads results analysis of information technology audits and vulnerability reviews, including penetration tests and security design reviews of network infrastructure and applications.
    - Develops and maintains infrastructure security metrics for framework maturity, security posture governance, and reporting.
    - Performs research on information security trends and advices management on information security best practices.

[24] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Security Engineer I

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four plus years of relevant work experience.
   - Zero to three years of experience in areas of information security engineering, network administration and/or information security administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to understand and apply concepts of information security principles.
   - Technical knowledge of information security engineering, computer and network security, authentication and security protocols, and applied cryptography.
   - Knowledge of networking protocols and understanding of information security related technologies, including encryption, firewalls, antivirus software, intrusion prevention systems and access lists.
   - Experience in information security incident monitoring and analysis.
   - Knowledge of programming code, scripting and concepts.
   - Experience in performing and managing vulnerability assessments and penetration tests on network infrastructure and applications.
   - Experience in responding to information security risks, threats and incidents.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).
   - Preferred, but not required certifications may include: Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Engineer I position[25] will be under the supervision of the Information Security Engineer II/III or the Information Security Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Engineer I is primarily responsible for the coordination and implementation of information security measures to safeguard the organization's information against accidental or unauthorized modification, destruction or disclosure.

[25] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. Job Functions:

- Works with system architects and other information technology functions to translate information security policies, standards, procedures and controls into engineering and system implementation recommendations.
- Assists senior engineers (Information Security Engineers II and III) to assess the organization's information security infrastructure and design to validate system and network security.
- Monitors information security tools and technologies deployed in the current environment to confirm they are in line with architectural requirements.
- Participates in cross-functional meetings with appropriate staff to develop system design recommendations for all required engineering disciplines, such as hardware, software, platform, maintainability and reliability.
- Performs information security research and analysis for assigned systems and network infrastructure.
- Supports planning of configuration changes for major information security infrastructure platforms.
- Conducts information security impact analyses of controls on proposed system changes.
- Monitors system threats and vulnerabilities, and assesses impact on the organization caused by information security incidents.
- Supports information security risk and vulnerability reviews, including penetration tests and security design reviews on network infrastructure and applications.
- Assists in the definition of alerts and logging security requirements, and conducts reviews of alerts and logs from firewall, intrusion prevention systems, data storage tools, antivirus and other security threat data sources.
- Assists in the design implementation of information security incident response plans.

Information Security Engineer II

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - Three to five years of experience in areas of information security engineering, network administration, and/or information security administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of networking protocols and understanding of information security related technologies including encryption, firewalls, antivirus software, intrusion prevention systems and access lists.
   - Experience in programming code, scripting and concepts.
   - Experience in performing and managing vulnerability assessments and penetration tests on network infrastructure and applications.
   - Extensive experience in analyzing network attacks and definition of risk mitigation strategies.
   - Experience in managing information security risks, threats and developing an incident response plan.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).
   - Preferred, but not required certifications may include: Certified Information Systems Security Professional (CISSP), and/or Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Engineer II position[26] will be under the supervision of the Information Security Engineer III or Information Security Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Engineer II is primarily responsible for the security and integrity of systems, networks and data aligned with organization requirements. They will work with the appropriate staff across the organization to evaluate proposed technologies and ascertain that information security requirements are satisfied for all projects.

[26] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. Job Functions:

- Confers with information technology and other security teams to identify and plan for the security of information systems, networks and data within the organization; assesses, analyzes and documents information security requirements.
- Generates information security system engineering plans, designs, and technical reports.
- Partners with system owners to provide information security systems engineering guidance to programs on how to design and implement secure systems.
- Monitors and assesses risk factors such as operational criticality of systems, sensitivity or value of information, and associated security environment.
- Monitors all layers of the system, network and application infrastructure to confirm they integrate in a secure fashion.
- Performs information security risk and vulnerability reviews, including penetration tests and security design reviews on network infrastructure and applications.
- Conducts periodic assessments of technical security controls to determine design and operating effectiveness.
- Recommends enhancements to existing approaches and techniques to achieve continuous improvement in systems development processes.
- Assists in the development and implementation of information security incident response plans.
- Provides mentorship and guidance to junior staff (Information Security Engineer I).

Information Security Engineer III

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - More than five years of experience in areas of information security engineering, network administration and/or information security administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Advanced experience with system testing methodologies (penetration testing, configuration analysis) and experience with a variety of security testing and penetration testing tools.
   - Expertise in networking protocols and information security related technologies including encryption, firewalls, antivirus software, intrusion prevention systems and access lists.
   - Experience in programming code, scripting and concepts.
   - Experience in performing and managing vulnerability assessments and penetration tests on network infrastructure and applications.
   - Experience in analyzing network attacks and definition of risk mitigation strategies.
   - Experience in managing information security risks, threats and developing an incident response plan.
   - Expert knowledge of applicable information security trends and best practices.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).
   - Preferred, but not required certifications may include: Certified Information Systems Security Professional (CISSP), and/or Global Information Assurance Certification (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Engineer III position[27] will be under the supervision of the Information Security Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security Engineer III is primarily responsible for providing information security engineering expertise and guidance on the design and development of enterprise and system architectures aligned with applicable policies, standards, procedures and controls.

[27] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. Job Functions:

- Partners with appropriate staff to identify dependencies of information security control elements with other functions and systems within the organization and recommends protection strategy.
- Provides mentorship and guidance to junior staff; provides relevant technical training and guidance to staff and other departments.
- Analyzes systems for information security control implementation, and provides recommendations for optimization.
- Tests information security architecture and design solutions.
- Works with system owners to identify risk tradeoffs between organization mission and information security, and recommends improvements and operational solutions.
- Leads the development and implementation of threat monitoring and analysis technology infrastructure, including network planning, physical and virtual server design, and alerting capabilities.
- Serves as a subject matter expert for designated information security controls.
- Provides expert oversight in the development, testing, and operation of information security tools.
- Manages information security risk and vulnerability reviews, including penetration tests and security design reviews on network infrastructure and applications.
- Leads the implementation of information security incident response plans.
- Provides mentorship and guidance to junior staff; provides relevant technical training and guidance to staff and other departments.

Information Security Manager I

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, management information systems, or another related field, or high school diploma with four years of relevant work experience in project management or information risk management.
   - Four to six years of experience in areas of information security, information technology, information risk management, compliance, or a related field.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to apply information security principles to business solutions.
   - Ability to act as liaison and effectively communicate information security topics (e.g., data constraints, information needs) to both technical and non-technical audiences at all levels of the organization.
   - Knowledge of developing and managing an information security program, including its policies, standards, procedures, technologies, and controls.
   - Preferred, but not required knowledge of operating systems, cloud computing, network platforms, and hardware and software platforms as they relate to information security, or experience managing staff with those responsibilities.
   - Experience in identifying and managing information security risks, threats and incidents, and performing vulnerability assessments at an enterprise level, or managing staff performing these activities.
   - Strong situational analysis and decision making abilities.
   - Knowledge in identifying and managing information security risks, threats, and incidents at an enterprise level.
   - Experience planning and deploying both business and IT related initiatives.
   - Knowledge of or ability to learn applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP)).
   - Preferred, but not required certifications may include: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), GIAC Security Leadership Certification (GSLC), or other Global Information Assurance Certifications (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Manager I position[28] may be under the supervision of the Information Security Manager II/III or Chief Information Security Officer.

[28] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - May be expected to be on call 24/7.

5. **Job Purpose:**
   - The Information Security Manager I is primarily responsible for developing and implementing an organization-wide information security program and ongoing activities to preserve the availability, integrity and confidentiality of the organization's information resources in compliance with applicable information security policies, standards, procedures and controls.

6. **Job Functions:**
   - Assists in the establishment and maintenance of the agency's information security program and associated strategies to support the business processes and overall goals of the organization.
   - Establishes and maintains internal and external communication channels to support information security across the organization.
   - Collaborates with all levels of the organization to properly align information security considerations with business objectives and the resulting risk to the organizational operations.
   - Captures, tracks, and assesses metrics to measure the effectiveness of the agency's information security program and its threat and vulnerability management capabilities.
   - Demonstrates deep knowledge of the data shared across the organization and the relationships between those data and the agency's various business units.
   - Provides mentorship, guidance, and relevant information security training to agency staff.
   - Establishes goals and objectives for information security personnel.
   - Enforces security requirements during the design, development, testing, and delivery of information systems to confirm that organization assets are appropriately secure at all times against risks and threats.
   - Oversees and conducts risk management activities (e.g., risk assessment, gap analysis, business impact analysis) to identify current and future threats and to help the organization reach an acceptable level of risk.
   - Manages vulnerability assessments and oversees preparation and presentation of assessment results.
   - Supports the design, implementation, and maintenance of the incident response process and investigation of information security incidents.
   - Performs research on information security trends and advises management[29] on information security best practices.

[29] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Security Manager II

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, management information systems, or another related field or high school diploma with four years of relevant work in in project management or information risk management.
   - Seven to ten years of information technology administration, project management or related experience, inclusive of three to five years of experience information security, information technology, information risk management, compliance or a related field
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to apply information security principles to business solutions.
   - Ability to act as liaison and effectively communicate information security topics (e.g., data constraints, information needs) to both technical and non-technical audiences at all levels of the organization.
   - Strong situational analysis and decision making abilities.
   - Experience in identifying and addressing information security and compliance requirements in business functions and providing people, processes, and technologies that meet those requirements.
   - Knowledge of developing and managing an information security program, including its policies, standards, procedures, technologies, and controls.
   - Experience planning and deploying both business and IT related initiatives.
   - Experience in developing an analytical representation or illustration of an organization's business processes using a variety of tools and techniques to identify and help defend against risks and threats to an organization.
   - Preferred, but not required knowledge of various operating systems, cloud computing, network platform, and hardware and software platforms as they relate to information security, or experience managing staff with those responsibilities.
   - Experience in identifying and managing information security risks, vulnerabilities, threats and incidents at an enterprise level.
   - Knowledge of or ability to learn applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required certifications may include: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), GIAC Security Leadership Certification (GSLC), or other Global Information Assurance Certifications (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Manager II position[30] may be under the supervision of the Information Security Manager III or Chief Information Security Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - May be expected to be on call 24/7.

5. **Job Purpose:**
   - The Information Security Manager II is primarily responsible for the creation, implementation and oversight of the information security program including policies, strategies and safeguards to mitigate information security risks within the organization.

6. **Job Functions:**
   - Establishes and manages the agency's information security program and associated strategies with consideration for the business processes and overall goals of the organization.
   - Collaborates with agency executive management[31] to define acceptable levels of risk and to establish risk mitigation and management plans at an enterprise level.
   - Provides oversight for the development and implementation of information security processes, procedures and appropriate controls across business units taking into account the people (e.g., customers, suppliers, employees), resources and technologies involved in the processes.
   - Formulates the tactical and strategic information security goals and associated key performance indicators to measure the effectiveness of the agency's information security program and its threat and vulnerability management capabilities
   - Provides mentorship, guidance, and relevant information security training to agency staff.
   - Manages incident response and investigation activities for information security incidents.
   - Manages vulnerability assessments and oversees preparation and presentation of assessment results.
   - Works closely with HR and management to deploy information security awareness training to improve information security compliance.
   - Performs research on information security trends and advises management on information security best practices.

[30] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

[31] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Security Manager III

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, management information systems, or another related field, or high school diploma with four years of relevant work in project management or information risk management.
   - More than ten years of experience in areas of information technology administration, project management, or a related field, with a minimum of five years of experience in the areas of information security, information risk management, compliance, or a related field.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to apply information security principles to business solutions.
   - Strong situational analysis and decision making abilities.
   - Ability to act as a liaison and effectively communicate information security topics (e.g., data constraints, information needs) to both technical and non-technical audiences at all levels of the organization.
   - Experience in identifying and addressing information security and compliance requirements in business functions and providing people, processes, technologies that meet those requirements.
   - Experience in developing an analytical representation or illustration of an organization's business processes using a variety of tools and techniques to identify and help defend against risks and threats to an organization.
   - Knowledge of developing and managing an information security program, including its policies, standards, procedures, technologies, and controls.
   - Experience planning and deploying both business and IT related initiatives.
   - Preferred, but not required knowledge of various operating systems, cloud computing, network platform, and hardware and software platforms as they relate to information security, or experience managing staff with those responsibilities.
   - Experience in identifying and managing information security risks, vulnerabilities, threats and incidents at an enterprise level.
   - Knowledge of or ability to learn applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP)).
   - Preferred, but not required certifications may include: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), GIAC Security Leadership Certification (GSLC), or other Global Information Assurance Certifications (GIAC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security Manager III position[32] may be under supervision of the Chief Information Security Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - May be expected to be on call 24/7.

5. **Job Purpose:**
   - The Information Security Manager III is primarily responsible for developing and working with organization management[33] to develop and implement a strategic information security plan. They will enforce information security policies, standards, procedures and controls across the organization.

6. **Job Functions:**
   - Leads the development and maintenance of the agency's information security program and associated strategies with consideration for the business processes and overall goals of the organization.
   - Partners with agency executive management[32] to define acceptable levels of risk and to establish risk mitigation and management plans, processes, and policies at an enterprise level.
   - Oversees the formulation of tactical and strategic information security goals and associated key performance indicators to measure the effectiveness of the agency's information security program and its threat and vulnerability management capabilities
   - Provides mentorship, guidance, and relevant information security training to agency staff.
   - Provides subject matter expertise regarding information security initiatives.
   - Facilitates collaboration between business functions (e.g., information technology, privacy, information security) to validate compliance with information security policies, standards, procedures, and controls and better understand risks within business processes and initiatives.
   - Oversees the development and performance of vulnerability and risk assessments for business process, network and applications.
   - Leads the development and implementation of information security processes, procedures and appropriate controls across business units taking into account the people (e.g., customers, suppliers, employees), resources and technologies involved in the processes.
   - Leads the development of impact assessment tools, procedures, and program guidelines to measure risk and determine the level of recovery services required in the event of an information security incident.
   - Initiates, facilitates, and promotes communications and training activities to reinforce information security awareness throughout the organization.

[32] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

[33] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

- Performs research on information security trends and advises management on information security best practices.

Chief Information Security Office (CISO)

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, management information systems, or another related field, or high school diploma with four years of relevant work in project management or information risk management.
   - More than ten years of experience in areas of information technology administration, project management, or a related field, with a minimum of five years of experience in the areas of information security, information risk management, compliance, or a related field.
   - Eligibility to obtain and retain a Secret or higher security clearance from appropriate federal authorities.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Ability to apply information security principles to business solutions.
   - Strong situational analysis and decision making abilities.
   - Ability to act as a liaison and effectively communicate information security topics (e.g., data constraints, information needs) to both technical and non-technical audiences at all levels of the organization.
   - Experience in identifying and addressing information security and compliance requirements in business functions and providing people, processes and technologies that meet those requirements.
   - Experience in developing an analytical representation or illustration of an organization's business processes using a variety of tools and techniques to identify and help defend against risks and threats to an organization.
   - Knowledge of developing and managing an information security program, including its policies, standards, procedures, technologies, and controls.
   - Experience planning and deploying both business and IT related initiatives.
   - Knowledge of various operating systems, cloud computing, network platform, and hardware and software platforms as they relate to information security, or experience managing staff with those responsibilities.
   - Experience in identifying and managing information security risks, vulnerabilities, threats and incidents at an enterprise level.
   - Knowledge of or ability to learn applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP)).
   - Professional certification related to information security or privacy (e.g., Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), GIAC Security Leadership Certification (GSLC), Global Information Assurance Certifications (GIAC), or another related certification).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The CISO position[34] will report to the respective Agency Director and/or Chief Operating Officer (COO).

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - May be expected to be on call 24/7.

5. **Job Purpose:**
   - The CISO is primarily responsible for developing and working with organization management[35] to develop and implement a strategic information security plan. They will enforce information security policies, standards, procedures and controls across the organization.

6. **Job Functions:**
   - Leads the development and maintenance of the agency's information security program and associated strategies with consideration for the business processes and overall goals of the organization.
   - Partners with organization management[2] to define acceptable levels of risk and to establish risk mitigation and management plans, processes, and policies at an enterprise level.
   - Oversees the formulation of tactical and strategic information security goals and associated key performance indicators to measure the effectiveness of the agency's information security program and its threat and vulnerability management capabilities
   - Provides mentorship, guidance, and relevant information security training to agency staff
   - Oversees and liaises with organization management to ensure that agencies are aware of any new and/or modified information security requirements.
   - Update Agency Directors and/or COOs on agency-related information security status (risks, issues, mitigation plans).
   - Provides subject matter expertise regarding information security initiatives.
   - Facilitates collaboration between business functions (e.g., information technology, privacy, information security) to validate compliance with information security policies, standards, procedures, and controls and better understand risks within business processes and initiatives.
   - Oversees the development and performance of vulnerability and risk assessments for business process, network and applications.
   - Leads the development and implementation of information security processes, procedures and appropriate controls across business units taking into account the people (e.g., customers, suppliers, employees), resources and technologies involved in the processes.

[34] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

[35] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

- Leads the development of impact assessment tools, procedures, and program guidelines to measure risk and determine the level of recovery services required in the event of an information security incident.
- Initiates, facilitates, and promotes communications and training activities to reinforce information security awareness throughout the organization.
- Performs research on information security trends and advises organization management on information security best practices.

Information Security and Privacy Auditor I

1. **Minimum requirements for the position:**
   - Bachelor degree in a technical or privacy-related field, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - Zero to three years of experience in information security, information technology or privacy audit.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Basic knowledge of auditing standards, information security and privacy compliance frameworks and principles.
   - Basic knowledge of potential vulnerabilities and deviations from standard information security and privacy practices.
   - Basic knowledge of the principles, methods, and tools used for evaluating information security and privacy risks.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures, and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), American Institute of Certified Public Accountants (AICPA).
   - Preferred, but not required, certifications may include: Certified Information Systems Auditor (CISA), or Certified Internal Auditor (CIA).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security and Privacy Auditor I position[36] will be under the supervision of the Information Security and Privacy Auditor II/III, Information Security Manager, or Information Privacy Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security and Privacy Auditor I is primarily responsible for assisting senior auditors (Information Security and Privacy Auditor II and III) in performing information security and privacy audits to help ensure regulatory compliance. This individual will focus on documenting and reporting results of audits to management[37].

[36] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

[37] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

6. **Job Functions:**
    - Participates in the planning and development of information security and privacy audits.
    - Monitors the organization's compliance with established information security policies, standards, procedures and controls, by scheduling and assisting senior auditors to perform periodic compliance audits.
    - Assists senior auditors in maintaining and updating existing information security and privacy audit programs.
    - Leverages past audit results to identify and remediate discrepancies in current audits.
    - Identifies current information security and privacy controls and evaluates their operating effectiveness.
    - Supports audits of the organization's information security and privacy policies, standards, procedures, and controls to determine potential risks.
    - Documents information security and privacy audit results and findings and prepares them for internal review.
    - Assists senior auditors in developing remediation recommendations to address control deficiencies and to mitigate information security and privacy risks.

Information Security and Privacy Auditor II

1. **Minimum requirements for the position:**
   - Bachelor degree in a technical or privacy-related field, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - Three to five years of experience in information security, information technology or privacy audit.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Understanding of information security and privacy frameworks and principles.
   - Experience in evaluating system controls associated with business applications.
   - Experience executing audits within complex technical environments that includes various operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), network platforms and cloud computing.
   - Knowledge of the principles, methods, and tools used for evaluating risks.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), American Institute of Certified Public Accountants (AICPA, Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required, certifications may include: Certified Information Systems Auditor (CISA) or Certified Internal Auditor (CIA).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security and Privacy Auditor II position[38] will be under the supervision of the Information Security and Privacy Auditor III, Information Security Manager or Information Privacy Manager.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security and Privacy Auditor II is primarily responsible for conducting compliance reviews and audits on information security and privacy controls to identify compliance gaps and risks and to provide recommendations for remediation. The auditor will work with senior auditors (Information Security and Privacy Auditor III) and

[38] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

management[39] to maintain or enhance existing information security and privacy audit programs and processes.

6. Job Functions:

- Performs information security and privacy program compliance audits.
- Works with senior auditors and management to develop the scope, objectives, and auditing methodology for information security and privacy audits.
- Works with management to maintain and enhance existing information security and privacy audit programs to concur with regulatory changes.
- Identifies control deviations within the organization's technical infrastructure systems and key information security development initiatives.
- Works with junior auditors (Information Security and Privacy Auditor I) to document information security and privacy audit results and findings for internal review.
- Evaluates audit findings to confirm information security and privacy controls are implemented as designed and that they remain operating effectively.
- Develops recommendations to remediate control deficiencies and to mitigate information security and privacy risks.
- Performs follow-up review on audit procedure issues noted in past audits to confirm they are not repeated in future audits.

[39] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Information Security and Privacy Auditor III

1. **Minimum requirements for the position:**
   - Bachelor degree in a technical or privacy-related field, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - More than five years of experience in information security, information technology or privacy audit.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of information security and privacy policies and procedures development and implementation.
   - Knowledge of information security and privacy business and IT / application controls.
   - Experience developing information security and privacy audit programs.
   - Experience in executing IT audits within a complex technical environments that includes various operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), network platforms and cloud computing.
   - Knowledge of applicable trends and best practices.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), American Institute of Certified Public Accountants (AICPA, Federal Risk and Authorization Management Program (FedRAMP).
   - Preferred, but not required, certifications may include: Certified Information Systems Auditor (CISA) or Certified Internal Auditor (CIA).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Security and Privacy Auditor III position[40] will be under the supervision of the Information Security Manager, Information Privacy Manager or Chief Information Security Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - The Information Security and Privacy Auditor III is primarily responsible for planning and overseeing information security and privacy program audits within the organization. This individual will lead junior auditors (Information Security and Privacy Auditor I and II) in planning and conducting information security and privacy audits. This individual will also

[40] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

be responsible for providing guidance on the development of recommendations and remediation plans for control deficiencies and information security and privacy risks.

6. Job Functions:

- Works with management[41] to develop an information security and privacy audit program for the organization.
- Provides mentorship and guidance to junior staff; provides relevant technical training and guidance to junior auditors and other departments.
- Establishes a framework, approach, and process to audit information security controls and privacy programs against the information security and privacy regulations and program objectives.
- Oversees periodic information security and privacy program audits to determine degree of compliance with applicable policies, standards, procedures and controls.
- Provides briefings to management on audit status and results and advises if immediate action is required; leads the presentation of formal reports to stakeholders and management.
- Identifies audit issues and control weaknesses and advises on corrective actions for the audit procedure.
- Collaborates with appropriate staff and coordinates across the organization to address issues identified during audits.
- Develops recommendations to remediate control deficiencies and to mitigate information security and privacy risks.
- Performs research on information security and privacy audit trends and advises management on information security and privacy best practices.

[41] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Governance, Risk, and Compliance (GRC) Manager I

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - One to three years of GRC management experience.
   - Four to six years of experience in areas of audit, risk management, governance, information security and/or compliance.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Knowledge of governance, risk and compliance (GRC) program management.
   - Knowledge of GRC platforms.
   - Understanding of risk assessment process, monitoring, reporting etc.
   - Knowledge of evolving GRC environment and how changes in requirements and market trends may affect GRC processes and technology.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).
   - Preferred, but not required certifications may include: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), or Certified in Risk and Information Systems Control (CRISC).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The GRC Manager I position[42] will be under the supervision of the GRC Manager II/III, Chief Information Security Officer, Chief Information Technology Officer, Chief Risk Officer or Chief Compliance Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - NA

5. **Job Purpose:**
   - The GRC Manager I is primarily responsible for implementing and maintaining the organization's GRC program. They will work with management[43] to implement processes to measure and monitor identified risks, and provide mitigation.

6. **Job Functions:**
   - Supports the development and review of the organization's GRC strategy that aligns the business, information technology and governance model.

[42] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level GRC position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

[43] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

- Provides mentorship, guidance, and relevant technical training to other information security staff and other departments.
- Supports the maintenance of the information security framework by updating controls in conjunction with regulatory requirements.
- Works with information security management to monitor the effectiveness of the organization's GRC processes.
- Supports the organization's transition to a GRC platform for tracking risks due to non-compliance, information security and privacy control adoption and monitoring for implementation of security controls.
- Collaborates with management to leverage existing technology investments to support the GRC program
- Implements processes, standards and baseline thresholds for measurement, monitoring, reporting, mitigation and remediation of identified risks.
- Provides support to help maintain collaboration among departments across the organization.
- Supports training deployment to raise GRC program awareness across the organization.
- Performs research in GRC technology, processes updates, and best practices, and advises management on adoption to improve GRC capabilities.
- Assists in the development of reports and dashboards to present the level of controls compliance and the current IT risk posture.

Governance, Risk, and Compliance (GRC) Manager II

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - Three to five years of GRC management experience.
   - Seven to ten years of experience in areas of audit, risk management, governance, information security and/or compliance.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Experience in governance, risk and compliance (GRC) program management.
   - Experience using GRC platforms.
   - Knowledge of risk assessment processes, principles and reporting structure.
   - Experience in understanding of remediation procedures to mitigate risks.
   - Knowledge of evolving GRC environment and how changes in requirements and market trends may affect GRC processes and technology.
   - Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).
   - Preferred, but not required certifications may include: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), or Certified in Governance of Enterprise Information Technology (CGEIT).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The GRC Manager II position[44] will be under the supervision of the GRC Manager III, Chief Information Security Officer, Chief Information Technology Officer, Chief Risk Officer or Chief Compliance Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - NA

5. **Job Purpose:**
   - The GRC Manager II is primarily responsible for working with management[45] to establish the overall GRC strategy of the organization. They will manage the organization's governance requirements, develop risk measurement processes and standards, and monitor the organization's compliance with applicable policies, standards, procedures and controls.

[44] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level GRC position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

[45] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

6. Job Functions:

- Works with management to develop and implement a GRC strategy that aligns the business, information technology and governance domains.
- Provides mentorship, guidance, and relevant technical training to other information security staff and other departments.
- Assesses the maturity of existing discrete compliance and risk management programs to support scope definition of the GRC program.
- Assists in the vendor selection process and development of the organization's GRC platform.
- Work with information security staff to establish processes, standards and baseline thresholds for measurement, monitoring, reporting, mitigation and remediation of identified risks.
- Monitors and suggests improvements to the GRC program.
- Understands the organization's response plan for risks and threats, and supports the remediation and response process by reporting necessary information and materials to the organization's management.
- Collaborates across the organization to facilitate proactive alignment between internal and external security requirements and processes and technology to administer GRC.
- Performs research in GRC technology, processes updates, and best practices, and advises management on adoption to improve GRC capabilities.
- Develops reports and dashboards to present the level of controls compliance and the current IT risk posture.

Governance, Risk, and Compliance (GRC) Manager III

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - More than five years of GRC management experience.
   - More than ten years of experience in areas of audit, risk management, governance, information security and/or compliance.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?**
   - Experience in governance, risk and compliance (GRC) program development and management.
   - Experience managing and using GRC Platforms.
   - Knowledge of compliance principles, reporting structure and processes.
   - Experience in developing remediation procedures to mitigate risks.
   - Knowledge of evolving GRC environment and how changes in requirements and market trends may affect GRC processes and technology.
   - In-depth knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).
   - Preferred, but not required certifications may include: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), or Certified in the Governance of Enterprise Information Technology (CGEIT).

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The GRC Manager III position[46] will be under the supervision of the Chief Information Security Officer, Chief Information Technology Officer, Chief Risk Officer or Chief Compliance Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - NA

5. **Job Purpose:**
   - The GRC Manager III works with business units and other applicable departments (e.g., information security, IT, legal, audit) to establish an internal framework to satisfy governance requirements, tracking and reporting how the organization complies with established governance requirements. They will lead efforts to develop and implement a GRC strategy and platform for tracking risks, controls, risk assessments, issues and their remediation.

[46] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level GRC position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

6. Job Functions:

- Facilitates collaboration across the organization and with management[47] to develop a GRC strategy that aligns the business, information technology and governance domains.
- Works with management to develop and manage the organization's GRC program based on regulatory requirements and organization needs.
- Provides mentorship, guidance, and relevant technical training to other information security staff and other departments.
- Serves as a subject matter expert of the GRC Program, as applicable to the organization.
- Leads the organization's efforts to adopt an enterprise GRC platform by overseeing the vendor selection processes and managing the development and implementation of the platform.
- Understands the organization's response plan for risks and threats, and supports the remediation and response process by providing supporting materials.
- Recommends standard processes for collaboration between legal and compliance functions to effectively assess and plan for changing legal and regulatory mandates.
- Supports the periodic assessment of the organization's risk and compliance profile and recommends necessary adjustments to comply with changes in the legal and regulatory landscape.
- Performs research in GRC technology, processes updates, and best practices, and advises management on adoption to improve GRC capabilities.
- Defines reports and dashboards to present the level of controls compliance and the current IT risk posture.

[47] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Program Manager - Security

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - One to three years of compliance *and/or information security management experience.*
   - Four to six years of experience in areas of information technology administration, network administration, *and/or information security administration.*
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?** [48]
   - Experience in compliance program management.
   - Knowledge of compliance laws and regulations on a state and federal level.
   - Knowledge of information technology and *information security* compliance requirements.
   - *Knowledge of information security policies and procedures, such as disaster recovery, risk assessments, vulnerability assessments and incident response.*
   - *Knowledge of the principles, methods and tools used for evaluating risks.*
   - *Experience in managing intrusion detection systems and enterprise anti-virus software.*
   - *In-depth knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).*
   - *Preferred, but not required certifications may include: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), or Global Information Assurance Certification (GIAC).*

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - *The Program Manager (Compliance / Security) position*[49] *will be under the supervision of the Information Technology Director, Chief Information Security Officer or Chief Compliance Officer.*

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - N/A

5. **Job Purpose:**
   - *The Program Manager (Compliance / Security) is primarily responsible for managing the organization's security program to include planning, designing, implementing, supporting and monitoring information security systems, plans, policies and procedures. They will work with appropriate staff to identify compliance risks, vulnerabilities and provide*

[48] Information security required knowledge, skills and abilities are highlighted in *blue* and italicized.

[49] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information technology, information security and/or compliance position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

mitigations plans to address them, including coordination of responses to internal and external security threats to information technology, systems and security.

6. Job Functions[50]:

- Assists management[51] to identify potential areas of compliance vulnerability and risk, develops and implements corrective action plans, and provides guidance on resolution of such risks; reviews and revises organization's policies and procedures for the general operation of the compliance program and related activities as necessary to prevent illegal, unethical, or improper conduct.
- Receives and investigates complaints, directs mitigation efforts, trains staff and monitors compliance with applicable requirements.
- *Develops, directs and manages preparation, coordination and sustainability of organization's disaster recovery and business continuity plans for information technology, including plan establishment and testing to confirm full recovery within appropriate timeframes.*
- *Monitors changes in federal or state legislation and regulations, contracts and accreditation standards affecting information security obligations, requirements, standards and best practices.*
- *Supports the maintenance of the organization's information security program to enforce compliance with applicable policies, standards, procedures and controls.*
- *Understand the metrics set forth by the State; works with stakeholders to gather and respond to data calls and measure the effectiveness of the organization's information security program controls.*
- *Works with information technology business unit to understand information security applications, systems and tools, including virus protection, user authentication and intrusion prevention detection.*
- *Understands information security incident response plans and works with stakeholders comply with those plans and address any information security incidents.*
- *Coordinates vulnerability assessments on existing and planned systems and develops action plans to mitigate security gaps.*
- *Coordinates the delivery of information security training to the organization, and assists in the promotion of information security across the organization so employees are complaint on information security requirements.*
- *Assists the organization's employees to maintain awareness of, understand and interpret information security requirements.*

[50] Information security responsibilities are highlighted in *blue* and italicized.

[51] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Program Manager - Privacy

1. **Minimum requirements for the position:**
   - Bachelor degree, associate degree with two years of relevant work experience, or high school diploma with four years of relevant work experience.
   - One to three years of compliance and/or privacy management experience.
   - Four to six years of experience in information privacy administration.
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?** [52]
   - Experience in compliance program management.
   - Knowledge of compliance laws and regulations on a state and federal level.
   - Experience providing mitigation for compliance risks, vulnerabilities and complaints.
   - *Knowledge of information privacy compliance requirements.*
   - *Experience with the data lifecycle (e.g., identification, use, access, transmission, storage and destruction of data).*
   - *Experience in privacy impact assessments and incident response as it relates to privacy incidents.*
   - *Knowledge of applicable internal and/or external regulatory policies, standards, procedures, technology and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), American Institute of Certified Public Accountants (AICPA).*
   - *Preferred, but not required, certifications may include: Certified Information Privacy Professional/U.S. Government (CIPP/G), Certified Information Privacy Professional/U.S. Private-Sector (CIPP/US) or Certified Information Privacy Manager (CIPM).*

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - *The Program Manager (Compliance / Privacy) position*[53] *will be under the supervision of the Agency Information Privacy Manager, or Agency Privacy Officer.*

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, or overnight travel).**
   - N/A

5. **Job Purpose:**
   - *The Program Manager (Compliance / Privacy) is primarily responsible for managing the organization's privacy program to include planning, designing, implementing, supporting, and monitoring privacy policies, standards, procedures and controls. This individual will work with appropriate staff to identify compliance risks and vulnerabilities and provide*

[52] Privacy required knowledge, skills, and abilities are highlighted in *blue* and italicized.

[53] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information technology, privacy and/or compliance position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

mitigation plans to address these issues, including coordination of responses to internal and external threats to privacy.

6. **Job Functions[54]:**
   - Assists management[55] in identifying potential areas of compliance vulnerability and risk, develops and implements corrective action plans, and provides guidance on resolution of such risks; reviews and revises the organization's policies and procedures for the general operation of the compliance program and related activities, as necessary, to prevent illegal, unethical, or improper conduct.
   - Receives and investigates complaints, directs mitigation efforts, trains staff, and monitors compliance with applicable requirements.
   - Monitors changes in federal or state legislation and regulations, contracts, and accreditation standards affecting privacy obligations, requirements, standards, and best practices.
   - Works with appropriate stakeholders in developing and implementing an effective compliance training program for the organization's staff, monitors compliance with legal requirements, policies, and procedures, and responds to alleged violations of law, policies, and procedures.
   - *Supports the maintenance of the organization's privacy program, including privacy policy, to ensure compliance with applicable policies, standards, procedures, and controls.*
   - *Provides privacy subject-matter expertise on an array of topics, initiatives, and projects advising on federal and state privacy laws, including incident notification laws.*
   - *Coordinates delivery of privacy training to the organization and assists in the promotion of privacy awareness across the organization to ensure employee compliance with privacy requirements.*
   - *Serves as the organization's liaison for any complaints and/or investigations related to privacy.*
   - *Understands privacy impact assessment guidance in order to accurately and consistently identify and address privacy issues within the organization.*
   - *Assists the organization's employees in maintaining an awareness and understanding of privacy requirements as they pertain to the employees' role in the organization.*

[54] Privacy responsibilities are highlighted in *blue* and italicized.

[55] The definition of management may vary by organization and may include line or middle management, department heads, and/or agency leadership.

Information Technology Director

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - More than seven years of information technology management experience.
   - More than ten years of experience in areas of information technology administration, network administration, *and/or information security administration.*
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?** [56]
   - Knowledge of information technology concepts and principles.
   - Experience in information technology project management.
   - Experience in designing, developing and implementing information technology solutions.
   - *Experience in and knowledge of operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), hardware and software platforms, and protocols as they relate to information technology.*
   - *Knowledge of information security program development and maintenance, including information security concepts, principles, policies and procedures.*
   - *Experience in managing and responding to information security risks, threats and incidents.*
   - *Knowledge of how information security risks fit within the organization's risk management framework and business, and IT processes.*
   - *Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Federal Risk and Authorization Management Program (FedRAMP).*

3. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Information Technology Director position[57] will be under the supervision of the Agency Executive Director or Chief Information Officer.

4. **Indicate additional comments regarding this position (e.g., work environment, physical requirements, overnight travel).**
   - May be expected to be on call 24/7.

5. **Job Purpose:**
   - The Information Technology Director is primarily responsible for planning, directing and administering the functions of the offices of information technology *and information security, including* operations, planning and application development. They will provide

[56] Information security required knowledge, skills and abilities are highlighted in *blue* and italicized.

[57] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information technology, information security and/or compliance position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

support and information to leadership to facilitate organization-wide implementation of information technology *and security policies and procedures.*

6. Job Functions[58]:

- Manages information technology department to include: staffing, leave approval, EPMS reviews, work/project assignments, and training.
- Responds to user requests, issues timely diagnoses and fixes problems with technological infrastructure.
- Provides reports on client management data.
- Provides technical expertise and assistance to projects, programs and staff via input, involvement and training. Maintains familiarity with industry trends and technological improvements.
- Develops and manages the information technology budget, vendors, and policies and procedures.
- Meets with organization's management[59], users, vendors, and supervisory personnel to discuss and resolve operational problems, plans and administrative issues.
- *Leads the development and maintenance of the information security program, including policies, standards, procedures, and controls across the organization.*
- *Works with appropriate staff to validate systems, applications and operations in compliance with policies, standards, procedures, and controls.*
- *Integrates information security related policies and procedures into the accepted information technology management framework.*
- *Implements security controls based on the classification of data and applicable compliance requirements to provide appropriate access controls to information and systems across the organization.*
- *Provides coordination across the organization to assess, monitor and appropriately manage information security risks and threats.*
- *Works with the Division of Information Security and the Enterprise Privacy Office to appropriately manage and respond to incidents.*

[58] Information security responsibilities are highlighted in *blue* and italicized.

[59] The definition of management may vary by organization, and may include line or middle management, department heads and/or agency leadership.

Network Administrator

1. **Minimum requirements for the position:**
   - Bachelor degree in information technology, computer science, related technical field, or high school diploma with four years of relevant work experience.
   - One to three years of information technology management experience.
   - Four to six years of experience in areas of network administration, information technology administration *and/or information security administration.*
   - Work and/or consulting experience in federal, state, city or local government is desirable.

2. **What knowledge, skills, and abilities are needed by an employee upon entry to this job including any special certifications or license?** [60]
   - Knowledge of *network security principles,* network capacity planning, and general network management best practices.
   - Experience in and knowledge of networks, data centers, storage and servers as they relate to information technology and network administration.
   - Experience with enterprise-level LAN, WAN, and WLAN engineering, design and implementation.
   - *Knowledge of industry standards for secure configuration of network and infrastructure devices.*
   - *Knowledge of information security concepts and principles.*
   - *Knowledge of information security technology development and maintenance.*
   - *Experience managing vulnerability on networks and applications.*
   - *Experience in managing and responding to information security risks, threats and incidents.*
   - *Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls (e.g., National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT)).*

1. **Describe the guidelines and supervision an employee receives to do this job, including the employee's independence and discretion.**
   - The Network Administrator position[61] will be under the supervision of the Information Technology Director.

2. **Indicate additional comments regarding this position (e.g. work environment, physical requirements, overnight travel).**
   - N/A

3. **Job Purpose:**
   - The Network Administrator is primarily responsible for planning and coordinating the design, installation and connectivity of computer and network systems, to confirm stable operations of the organization's information technology assets. They will also troubleshoot network performance issues, and analyze network traffic and provide

[60] Information security required knowledge, skills and abilities are highlighted in *blue* and italicized.

[61] Span of control and reporting structure may vary by organization; in the event that this position is the most senior-level information technology and/or information security position in the organization, it is recommended that reporting duties be coordinated with agency leadership.

capacity planning solutions. *Additionally, they will support the implementation and maintenance of information security policies, standards, procedures and controls to protect the organization's information systems.*

6. **Job Functions[62]:**
   - Develops and enforces compliance with information technology policies and procedures consistent with state and federal requirements and industry best practices.
   - Leads, manages and supervises the organization, operation and development of the information technology department.
   - Makes sure that technical staff provides support and maintenance of information technology assets across the organization.
   - Leads information technology projects, to make sure goals and deadlines are met.
   - Holds staff accountable for goals and objectives as well as day to day activities.
   - Assists department management in making short and long term decisions regarding information technology procurement, adoption and deployment. Manages vendor relationships to make certain that the department receives the best value possible for its purchases and investments.
   - *Supports implementation and maintenance of information security policies, standards, procedures and controls to protect information systems that may include networks, servers, data centers, storage, applications, and related controls as they pertain to LAN, WAN and WLAN engineering, design and implementation.*
   - *Identifies and supports the implementation of network security technologies and solutions in compliance with applicable policies, standards, procedures and controls.*
   - *Monitors network threats and vulnerabilities in case of a security incident to assess their impact on the organization's network and applications.*
   - *Monitors server and network operations for security and takes steps to confirm network availability, reliability and security. Serves as point of contact for the organization and coordinates activities to meet security requirements.*
   - *Provides recommendations on countermeasures and mitigation procedures for a potential network attacks.*
   - *Assists organization personnel to maintain awareness of, understand and interpret information security and privacy requirements as it pertains to technical security requirements.*

[62] Information security responsibilities are highlighted in *blue* and italicized.