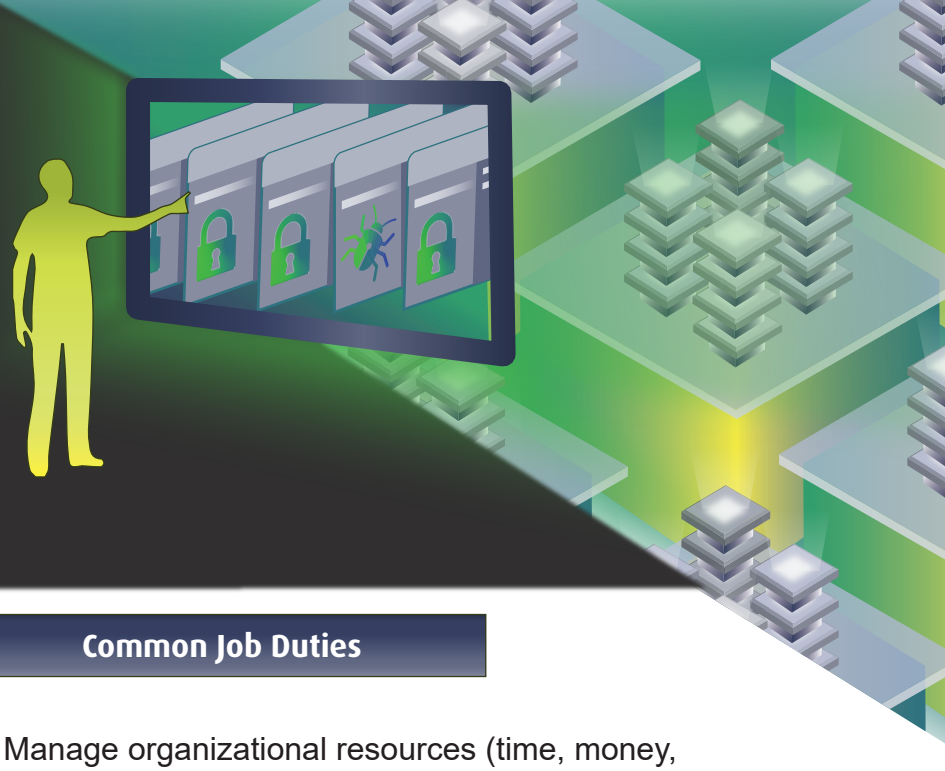
# Master Information Systems Security Officer



## Median Salary

**$87,000 - $110,000**

## Job Growth

**+20%**

## Soft Skills

**Strong Leadership**

**Good Communication**

**Efficient Multitasker**

**Creative Problem Solver**

**Comfortable Delegating**

## Common Job Duties

- Manage organizational resources (time, money, personnel, etc.) to support security goals and policies
- Create and execute strategies to improve the reliability and security of IT projects
- Define, implement and maintain corporate security policies and procedures
- Spearhead vulnerability audits, forensic investigations, and mitigation procedures
- Respond immediately to security-related incidents and provide a thorough post-event analysis
- Manage a diverse team of security administrators, analysts and IT professionals
- Institute organization-wide training in security awareness, protocols and procedures

## Mile2 Cybersecurity Certification's Suggested Course Progression

| C)SP | C)ISSO | C)ISSM | IS20 |
|---|---|---|---|
| Security Principles | Information Systems Security Officer | Information Systems Security Manager | IS20 Controls |

The person who carries the Certified Master Information Systems Security Officer Certification should be able to acquire necessary resources, advise senior leadership, collaborate with stakeholders, evaluate effectiveness, identify cybersecurity problems, manage threats, oversee information security awareness programs, participate in risk assessments, support compliance activities, and define or implement policies and procedures to ensure protection of critical infrastructure.


*Earn all four certifications listed above to earn your Certified Master Information Security Systems Officer Badge

10213 Wilsky Blvd, Tampa, FL 33625 Phone: +1-813-920-6799 Toll Free: +1 800-816-4532

# Master Information Systems Security Officer

**ABILITIES**

- Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
- Integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources
- Identify critical infrastructure systems that were designed without system security consider ations.

**KNOWLEDGE**

- Computer networking concepts and protocols, and network security methodologies.
- Risk management processes (e.g., methods for assessing and mitigating risk).
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Cybersecurity and privacy principles.
- Cyber threats and vulnerabilities.
- Specific operational impacts of cybersecurity lapses.
- Applicable business processes and operations of customer organizations.
- Encryption algorithms
- Data backup and recovery.
- Business continuity and disaster recovery continuity of operations plans.
- Host/network access control mechanisms.
- Cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- Vulnerability information dissemination sources.
- incident response and handling methodologies.
- industry-standard and organizationally accepted analysis principles and methods.
- intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- Risk Management Framework (RMF) requirements.
- Measures or indicators of system performance and availability.
- Current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.
- Network traffic analysis methods.
- New and emerging information technology (IT) and cybersecurity technologies.
- How traffic flows across the network.
- System and application security threats and vulnerabilities.
- Resource management principles and techniques.
- Server administration and systems engineering theories, concepts, and methods.
- Server and client operating systems.
- System software and organizational design standards, policies, and authorized approaches relating to system design.
- System life cycle management principles, including software security and usability.
- Technology integration processes.
- Organization’s enterprise information technology (IT) goals and objectives.
- What constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.
- Information security program management and project management principles and techniques.
- Supply Chain Risk Management Practices (NIST SP 800-161)
- Organization's risk tolerance and/or risk management approach.
- Enterprise incident response program, roles, and responsibilities.
- Current and emerging threats/threat vectors.
- Critical information technology (IT) procurement requirements.
- System administration, network, and operating system hardening techniques.
- Applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
- Information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
- Critical infrastructure systems with information communication technology that were designed without system security considerations.
- Network security architecture concepts including topology, protocols, components, and principles.
- Network systems management principles, models, methods, and tools.
- Security architecture concepts and enterprise architecture reference models.
- Personally Identifiable Information (PII) data security standards.
- Payment Card Industry (PCI) data security standards.
- Personal Health Information (PHI) data security standards.
- Laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Organization's information classification program and procedures for information compromise.
- Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Penetration testing principles, tools, and techniques.
- Controls related to the use, processing, storage, and transmission of data.
- Application Security Risks

**SKILLS**

- Creating policies that reflect system security objectives.
- Determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes.
- Evaluating the trustworthiness of the supplier and/or product.

**TASKS**

- Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
- Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.
- Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
- Advise senior management (e.g., CIO) on cost/benefit analysis of i nformation security programs, policies, processes, systems, and elements.
- Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.
- Collect and maintain data needed to meet system cybersecurity reporting.
- Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
- Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
- Ensure that security improvement actions are evaluated, validated, and implemented as required.
- Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.
- Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).
- Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.

If a person holds the Master Information Systems Security Officer from Mile2, we certify that they have passed the four certification exams in the role-based progression and thereby has adequate KSA's listed above to complete the applicable tasks required for the job role of Information Systems Security Officer.

# Master Information Systems Security Officer

- Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.
- Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.
- Evaluate cost/benefit, economic, and risk analysis in decision-making process.
- Identify alternative information security strategies to address organizational security objective.
- Identify information technology (IT) security program implications of new technologies or technology upgrades.
- Interface with external organizations to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.
- Interpret and/or approve security requirements relative to the capabilities of new information technologies.
- Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.
- Lead and align information technology (IT) security priorities with the security strategy.
- Lead and oversee information security budget, staffing, and contracting.
- Manage the monitoring of information security data sources to maintain organizational situational awareness.
- Manage the publishing of Computer Network Defense guidance for the enterprise constituency.
- Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.
- Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended l evel of protection.
- Oversee the information security training and awareness program.
- Participate in an information security risk assessment during the Security Assessment and Authorization process.
- Participate in the development or modification of the computer environment cybersecurity program plans and requirements.
- Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.
- Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.
- Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.
- Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.
- Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.
- Recognize a possible security violation and take appropriate action to report the incident, as required.
- Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.
- Recommend policy and coordinate review and approval.
- Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
- Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
- Use federal and organization-specific published documents to manage operations of their computing environment system(s).
- Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
- Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
- Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
- Evaluate the effectiveness of procurement function in addressing i information security requirements and supply chain risks through procurement activities and recommend improvements.
- Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.
- Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
- Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.
- Support necessary compliance activities .
- Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.
- Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
- Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.
- Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.
- Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.

If a person holds the Master Information Systems Security Officer from Mile2, we certify that they have passed the four certification exams in the role-based progression and thereby has adequate KSA's listed above to complete the applicable tasks required for the job role of Information Systems Security Officer.