Information Systems Security Management Professional (ISSMP)

Duration: 5 Days

Course Description:

The Information Systems Security Management Professional (ISSMP) is security leader who specializes in establishing, presenting and governing information security programs and demonstrates management and leadership skills. ISSMPs direct the alignment of security programs with the organization's mission, goals and strategies in order to meet enterprise financial and operational requirements in support of its desired risk position.

Target Audience:

The ISSMP is ideal for those working in roles such as:

- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer
- Senior Security Executive

Prerequisites:

- Candidates must be a CISSP in good standing and have two years' cumulative, full-time experience in one or more of the five domains of the current ISSMP outline.
- Candidates must have a minimum of seven years' cumulative, full-time experience in two or more of the domains of the current ISSMP outline.
- Earning a post-secondary degree (bachelor's or master's) in computer science, information technology (IT) or related fields or an additional credential from the ISC2 approved list may satisfy one year of the required experience.
- Part-time work and internships may also count towards the experience requirement.

Course Outlines:

Domain 1: Leadership and Operational Management

- Establish security's role in organizational culture, vision, and mission
- Align security program with organizational governance
- Define and implement information security strategies
- Define and maintain security policy framework
- Manage security requirements in contracts and agreements
- Manage security awareness and training programs
- Define, measure and report security metrics
- Prepare, obtain, and manage security budget
- Manage security programs
- Apply product development and project management principles

Domain 2: Systems Lifecycle Management

- Manage integration of security throughout system life cycle
- Integrate organization initiatives and emerging technologies throughout the security architecture
- Define and manage comprehensive vulnerability management programs (e.g., vulnerabilities, scanning, penetration testing, threat analysis)
- Manage security aspects of change control

Domain 3: Risk Management

- Develop and manage a risk management program
- Manage security risks within the supply chain (e.g., supplier, vendor, third-party risk, contracts)
- Conduct risk assessments
- Manage risk controls

Domain 4: Security Operations

- Establish and maintain security operations center
- Establish and maintain threat intelligence program
- Establish and maintain incident management program

Domain 5: Contingency Management

- Facilitate development of contingency plans
- Develop recovery strategies
- Maintain contingency plan, resiliency plan (e.g., Continuity of Operations Plan (COOP)), business continuity plan (BCP) and disaster recovery plan (DRP)
- Manage disaster response and recovery process

Domain 6: Law, Ethics and Security Compliance Management

- Identify the impact of laws and regulations that relate to information security
- Understand, adhere to, and promote professional ethics
- Validate compliance in accordance with applicable laws, regulations, and industry standards
- Coordinate with auditors and regulators in support of internal and external audit processes
- Document and manage compliance exceptions