# Information Systems Security Management Professional (ISSMP)

## 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 to meet enterprise financial and operational requirements in support of its desired risk position.

## Course Duration:

5 days

## Required Experience:

Candidates must have a CISSP in good standing and have 2-years' cumulative, full-time experience in 1 or more of the six domains of the current ISSMP Exam Outline.
Or candidates must have a minimum of 7 -years' cumulative, full-time experience in 2 or more of the six domains of the current ISSMP Exam Outline. Earning a post-secondary degree (bachelor's or master's) in computer science, 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 be considered.

## Course Outline:

**Domain 1: Leadership and Organizational Management**

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

**Domain 2: Systems Lifecycle Management**

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

**Domain 3: Risk Management**

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

**Domain 4: Security Operations**

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

**Domain 5: Contingency Management**

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

**Domain 6: Law, Ethics, and Security Compliance Management**

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

## Who Should Attend

- Chief Information Officer (CIO)
- Chief Information
- Security Officer (CISO)
- Chief Technology Officer (CTO)
- Senior Security Executive