ISSMP®

Information Systems Security Management Professional

ISC2™ Certification

Certification **Exam Outline**

Effective Date: August 1, 2025

ISC2™

About ISSMP

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.

The broad spectrum of topics included in the ISSMP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security management. Successful candidates are competent in the following six domains:

- Leadership and Organizational Management
- Systems Lifecycle Management
- Risk Management
- Security Operations
- Contingency Management
- Law, Ethics and Security Compliance Management

Experience Requirements

Candidates must be a CISSP in good standing and have two years cumulative, full-time experience in one or more of the six domains of the current ISSMP outline.

Or

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 (bachelors or masters) 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.

Accreditation

ISSMP is in compliance with the stringent requirements of the ANSI National Accreditation Board (ANAB) ISO/IEC Standard 17024.

Job Task Analysis (JTA)

ISC2 has an obligation to its membership to maintain the relevancy of the ISSMP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the ISSMP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

ISSMP Examination Information

Length of exam	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

ISSMP Examination Weights

Domains	Weight
1. Leadership and Organizational Management	21%
2. Systems Lifecycle Management	15%
3. Risk Management	20%
4. Security Operations	18%
5. Contingency Management	12%
6. Law, Ethics, and Security Compliance Management	14%
Total:	**100%**

Domain 1:
Leadership and Operational Management

1.1 Establish security’s role in organizational culture, vision, and mission

- Defining information security program vision and mission
- Aligning security with organizational goals, objectives, and values
- Defining security’s relationship with the overall organization processes
- Defining the relationship between organizational culture and security

1.2 Align security program with organizational governance

- Identifying and navigating organizational governance structure
- Verifying and validating roles of key stakeholders
- Validating sources and boundaries of authorization
- Advocating and obtaining organizational support for security initiatives

1.3 Define and implement information security strategies

- Identifying security requirements from organizational initiatives
- Evaluating capacity and capability to implement security strategies
- Prescribing security architecture design
- Managing implementation of security strategies
- Reviewing and maintaining security strategies

1.4 Define and maintain security policy framework

- Determining applicable external standards, laws, and regulations
- Determining data classification and protection requirements
- Establishing internal policies
- Advocating and obtaining organizational support for policies
- Developing procedures, standards, guidelines, and baselines
- Ensuring periodic review of security policy framework

Domain 1:
Leadership and Operational Management

1.5 Manage security requirements in contracts and agreements

- Evaluating service management agreements (e.g., risk, financial)
- Governing managed services (e.g., infrastructure, cloud services)
- Managing security impact of organizational change (e.g., mergers and acquisitions, outsourcing, capability development)
- Ensuring that applicable regulatory compliance statements and requirements are included in contractual and service management agreements
- Monitoring and enforcing compliance with contractual and service management agreements

1.6 Manage security awareness and training programs

- Promoting security programs to key stakeholders
- Identifying needs and implementing training programs by target segment
- Monitoring, evaluating, and reporting on effectiveness of security awareness and training programs

1.7 Define, measure and report security metrics

- Identifying Key Performance Indicators (KPI) and Key Risk Indicators (KRI)
- Associating metrics to the risk posture of the organization
- Using metrics to drive improvements to the security program and operations

1.8 Prepare, obtain, and manage security budget

- Preparing and securing annual budget
- Adjusting or requesting budget based on evolving risks and threat landscape
- Managing and reporting financial responsibilities

Domain 1:
Leadership and Operational Management

1.9 Manage security programs

- Defining roles and responsibilities
- Determining and managing team accountability
- Building cross-functional relationships
- Resolving conflicts between security and other stakeholders
- Identifying communication bottlenecks and barriers
- Integrating security controls into organization processes

1.10 Apply product development and project management principles

- Incorporating security throughout the lifecycle
- Identifying and applying applicable methodology (e.g., agile, waterfall, lean, rapid application development)
- Analyzing project scope, timelines, quality, and budget

Domain 2: Systems Lifecycle Management

2.1 Manage integration of security throughout system life cycle

- » Integration of information security decision points and requirements throughout the system life cycle
- » Implementation of security controls throughout the system life cycle
- » Overseeing security configuration management (CM) processes

2.2 Integrate organization initiatives and emerging technologies throughout the security architecture

- » Implementing security principles
- » Addressing impact of organization initiatives on security posture

2.3 Define and manage comprehensive vulnerability management programs (e.g., vulnerabilities, scanning, penetration testing, threat analysis)

- » Identification, classification, and prioritization of assets, systems, and services based on criticality and impact to the organization
- » Prioritization of threats and vulnerabilities based on risk
- » Management of security testing
- » Management of mitigation and/or remediation of vulnerabilities
- » Monitoring and reporting of vulnerabilities

2.4 Manage security aspects of change control

- » Integration of security requirements with change control process
- » Conducting a security impact analysis
- » Identification and coordination with the stakeholders
- » Management of documentation and tracking
- » Ensuring policy compliance (e.g., continuous monitoring)

Domain 3: Risk Management

3.1 Develop and manage a risk management program

- » Identifying risk management program objectives
- » Defining risk management objectives with risk owners and other stakeholders
- » Determining scope of organizational risk program
- » Identifying organizational risk tolerance/appetite
- » Obtaining and verifying organizational asset inventory
- » Analyzing organizational risks
- » Determine countermeasures, compensating and mitigating controls
- » Identifying risk treatment options
- » Conducting Cost-benefit analysis (CBA) of risk treatment options
- » Recommending risk treatment options to stakeholders
- » Documenting and managing agreed risks and issues treatments
- » Testing, monitoring, and reporting on risks and issues

3.2 Manage security risks within the supply chain (e.g., supplier, vendor, third-party risk, contracts)

- » Identifying supply chain security risk objectives
- » Integrating supply chain security risks into organizational risk management
- » Verifying and validating security risk control within the supply chain
- » Monitoring and reviewing the supply chain security risks

Domain 3:
Risk Management

3.3 Conduct risk assessments

- Identifying risk factors
- Determining the risk assessment approach (e.g., qualitative, quantitative)
- Performing the risk analysis

3.4 Manage risk controls

- Identifying controls
- Determining control effectiveness
- Evaluating control coverage
- Monitoring/reporting risk control effectiveness and coverage

Domain 4: Security Operations

4.1 Establish and maintain security operations center

» Development of security operations center (SOC) documentation

4.2 Establish and maintain threat intelligence program

» Aggregating threat data from multiple threat intelligence sources
» Conducting baseline analysis of network traffic, data, and user behavior
» Detecting and analyzing anomalous behavior patterns for potential concerns
» Conducting threat modeling
» Identifying and categorizing attacks
» Correlating related security events and threat data
» Defining actionable alerts

4.3 Establish and maintain incident management program

» Development of program documentation
» Establishing incident response (IR) case management processes
» Establishing incident response (IR) team
» Applying incident management methodologies
» Establishing and maintaining incident handling processes
» Establishing and maintaining investigation processes
» Quantifying and reporting incident impacts and investigations to stakeholders
» Conducting root cause analysis

Domain 5: Contingency Management

5.1 Facilitate development of contingency plans

- Identifying and analyzing factors related to resiliency planning (e.g., Continuity of Operations Plan (COOP), external factors, laws, regulations, business impact analysis (BIA))
- Identifying and analyzing factors related to the business continuity plan (BCP) (e.g., time, resources, verification, business impact analysis (BIA))
- Identifying and analyzing factors related to the disaster recovery plan (DRP) (e.g., time, resources, verification)
- Coordinating contingency management plans with key stakeholders
- Defining internal and external crisis communications plan
- Defining and communicating contingency roles and responsibilities
- Identifying and analyzing contingency impact on organization processes and priorities
- Managing third-party contingency dependencies (e.g., cloud providers, utilities)
- Preparing security management succession plan

5.2 Develop recovery strategies

- Identifying and analyzing alternatives
- Recommending and coordinating recovery strategies
- Assigning recovery roles and responsibilities

Domain 5:
Contingency Management

5.3 Maintain contingency plan, resiliency plan (e.g., Continuity of Operations Plan (COOP)), business continuity plan (BCP) and disaster recovery plan (DRP)

- » Planning testing, evaluation, and modification
- » Determining survivability and resiliency capabilities
- » Managing plan update process

5.4 Manage disaster response and recovery process

- » Declaring and communicating disaster
- » Implementing plan
- » Restoring normal operations
- » Gathering lessons learned
- » Updating plan based on lessons learned

Domain 6:
Law, Ethics and Security Compliance Management

6.1 Identify the impact of laws and regulations that relate to information security

- Identifying legal jurisdictions that the organization and users operate within (e.g., trans-border data flow)
- Identifying applicable security and privacy laws/regulations/standards
- Identifying intellectual property laws
- Identifying and advising on risks of non-compliance and non-conformity

6.2 Understand, adhere to, and promote professional ethics

- ISC2 Code of Ethics
- Organizational code of ethics

6.3 Validate compliance in accordance with applicable laws, regulations, and industry standards

- Informing and advising senior management
- Evaluating and selecting compliance framework(s)
- Implementing the compliance framework(s)
- Defining and monitoring compliance metrics

Domain 6:
Law, Ethics and Security Compliance Management

6.4 Coordinate with auditors and regulators in support of internal and external audit processes

» Planning

» Scheduling

» Coordinating audit activities

» Evaluating and validating findings

» Formulating response

» Monitoring and validating implemented mitigation and remediation actions

6.5 Document and manage compliance exceptions

» Identifying and documenting controls and workarounds

» Reporting and obtaining authorized approval of risk waiver

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at **www.ISC2.org/certifications/references**.

Examination Policies and Procedures

ISC2 recommends that ISSMP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at **www.ISC2.org/Register-for-Exam**.

Legal Info

For any questions related to **ISC2's policies**, please contact the ISC2
Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas Tel: +1.866.331.ISC2 (4722), press 1
Email: membersupport@isc2.org

Asia-Pacific Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa Tel: +44 (0)203-960-7800
Email: info-emea@isc2.org