CISSP®

ISSMP®

Certified Information Systems Security Professional

Management

Certification **Exam Outline**

Effective Date: May 2018

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

About CISSP-ISSMP

The Information Systems Security Management Professional (ISSMP) is a CISSP 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 6 domains:

- Leadership and Business Management
- Systems Lifecycle Management
- Risk Management
- Threat Intelligence and Incident Management
- Contingency Management
- Law, Ethics, and Security Compliance Management

Experience Requirements

Candidates must be a CISSP in good standing and have 2 years cumulative paid full-time work experience in 1 or more of the 6 domains of the CISSP-ISSMP CBK.

Accreditation

ISSMP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² 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.

CISSP-ISSMP Examination Information

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

CISSP-ISSMP Examination Weights

Domains	Weight
1. Leadership and Business Management	22%
2. Systems Lifecycle Management	19%
3. Risk Management	18%
4. Threat Intelligence and Incident Management	17%
5. Contingency Management	10%
6. Law, Ethics, and Security Compliance Management	14%
Total:	**100%**

Domain 1: Leadership and Business Management

1.1 Establish Security's Role in Organizational Culture, Vision, and Mission

- Define information security program vision and mission
- Align security with organizational goals, objectives, and values
- Explain business processes and their relationships
- Describe the relationship between organizational culture and security

1.2 Align Security Program with Organizational Governance

- Identify and navigate organizational governance structure
- Recognize roles of key stakeholders
- Recognize sources and boundaries of authorization
- Negotiate organizational support for security initiatives

1.3 Define and Implement Information Security Strategies

- Identify security requirements from business initiatives
- Evaluate capacity and capability to implement security strategies
- Manage implementation of security strategies
- Review and maintain security strategies
- Describe security engineering theories, concepts, and methods

1.4 Define and Maintain Security Policy Framework

- Determine applicable external standards
- Manage data classification
- Establish internal policies
- Obtain organizational support for policies
- Develop procedures, standards, guidelines, and baselines
- Ensure periodic review of security policy framework

1.5 Manage Security Requirements in Contracts and Agreements

- Evaluate service management agreements (e.g., risk, financial)
- Govern managed services (e.g., infrastructure, cloud services)
- Manage impact of organizational change (e.g., mergers and acquisitions, outsourcing)
- Monitor and enforce compliance with contractual agreements

1.6 Oversee Security Awareness and Training Programs

» Promote security programs to key stakeholders
» Identify training needs by target segment
» Monitor and report on effectiveness of security awareness and training programs

1.7 Define, Measure, and Report Security Metrics

» Identify Key Performance Indicators (KPI)
» Relate KPIs to the risk position of the organization
» Use metrics to drive security program development and operations

1.8 Prepare, Obtain, and Administer Security Budget

» Manage and report financial responsibilities
» Prepare and secure annual budget
» Adjust budget based on evolving risks

1.9 Manage Security Programs

» Build cross-functional relationships
» Identify communication bottlenecks and barriers
» Define roles and responsibilities
» Resolve conflicts between security and other stakeholders
» Determine and manage team accountability

1.10 Apply Product Development and Project Management Principles

» Describe project lifecycle
» Identify and apply appropriate project management methodology
» Analyze time, scope, and cost relationship

Domain 2: Systems Lifecycle Management

2.1 Manage Integration of Security into System Development Lifecycle (SDLC)

- Integrate information security gates (decision points) and milestones into lifecycle
- Implement security controls into system lifecycle
- Oversee configuration management processes

2.2 Integrate New Business Initiatives and Emerging Technologies into the Security Architecture

- Participate in development of business case for new initiatives to integrate security
- Address impact of new business initiatives on security

2.3 Define and Oversee Comprehensive Vulnerability Management Programs (e.g., vulnerability scanning, penetration testing, threat analysis)

- Classify assets, systems, and services based on criticality to business
- Prioritize threats and vulnerabilities
- Oversee security testing
- Mitigate or remediate vulnerabilities based on risk

2.4 Manage Security Aspects of Change Control

- Integrate security requirements with change control process
- Identify stakeholders
- Oversee documentation and tracking
- Ensure policy compliance

Domain 3: Risk Management

3.1 Develop and Manage a Risk Management Program

- Communicate risk management objectives with risk owners and other stakeholders
- Understand principles for defining risk tolerance
- Determine scope of organizational risk program
- Obtain and verify organizational asset inventory
- Analyze organizational risk management requirements
- Determine the impact and likelihood of threats and vulnerabilities
- Determine countermeasures, compensating and mitigating controls
- Recommend risk treatment options and when to apply them

3.2 Conduct Risk Assessments (RA)

- Identify risk factors
- Manage supplier, vendor, and third-party risk
- Understand supply chain security management
- Conduct Business Impact Analysis (BIA)
- Manage risk exceptions
- Monitor and report on risk
- Perform cost–benefit analysis

Domain 4:
Threat Intelligence and Incident Management

4.1 Establish and Maintain Threat Intelligence Program

- Synthesize relevant data from multiple threat intelligence sources
- Conduct baseline analysis
- Review anomalous behavior patterns for potential concerns
- Conduct threat modeling
- Identify ongoing attacks
- Correlate related attacks
- Create actionable alerting to appropriate resources

4.2 Establish and Maintain Incident Handling and Investigation Program

- Develop program documentation
- Establish incident response case management process
- Establish Incident Response Team (IRT)
- Understand and apply incident management methodologies
- Establish and maintain incident handling process
- Establish and maintain investigation process
- Quantify and report financial and operational impact of incidents and investigations to stakeholders
- Conduct Root Cause Analysis (RCA)

Domain 5: Contingency Management

5.1 Oversee Development of Contingency Plans (CP)

- Analyze challenges related to the Business Continuity (BC) process (e.g., time, resources, verification)
- Analyze challenges related to the Disaster Recovery (DR) process (e.g., time, resources, verification)
- Analyze challenges related to the Continuity of Operations Plan (COOP)
- Coordinate with key stakeholders
- Define internal and external incident communications plans
- Define incident roles and responsibilities
- Determine organizational drivers and policies
- Reference Business Impact Analysis (BIA)
- Manage third-party dependencies
- Prepare security management succession plan

5.2 Guide Development of Recovery Strategies

- Identify and analyze alternatives
- Recommend and coordinate recovery strategies
- Assign recovery roles and responsibilities

5.3 Maintain Business Continuity Plan (BCP), Continuity of Operations Plan (COOP), and Disaster Recovery Plan (DRP)

- Plan testing, evaluation, and modification
- Determine survivability and resiliency capabilities
- Manage plan update process

5.4 Manage Recovery Process

- Declare disaster
- Implement plan
- Restore normal operations
- Gather lessons learned
- Update plan based on lessons learned

Domain 6:

Law, Ethics, and Security Compliance Management

6.1 Understand the Impact of Laws that Relate to Information Security

- Understand global privacy laws
- Understand legal jurisdictions the organization operates within (e.g., trans-border data flow)
- Understand export laws
- Understand intellectual property laws
- Understand industry regulations affecting the organization
- Advise on potential liabilities

6.2 Understand Management Issues as Related to the (ISC)^2 Code of Ethics

6.3 Validate Compliance in Accordance with Applicable Laws, Regulations, and Industry Best Practices

- Obtain leadership buy-in
- Select compliance framework(s)
- Implement validation procedures outlined in framework(s)
- Define and utilize security compliance metrics to report control effectiveness and potential areas of improvement

6.4 Coordinate with Auditors, and Assist with the Internal and External Audit Process

- Prepare
- Schedule
- Perform audit
- Evaluate findings
- Formulate response
- Validate implemented mitigation and remediation actions

6.5 Document and Manage Compliance Exceptions

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

(ISC)² 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 (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org