CISSP®

ISSMP®

Certified Information Systems Security Professional

Management

Certification **Exam Outline**

Effective Date: April 2013

(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. Successful candidates are competent in the following 5 domains:

- Security Leadership and Management
- Security Lifecycle Management
- Security Compliance Management
- Contingency Management
- Law, Ethics and Incident 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 5 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. Security Leadership and Management	38%
2. Security Lifecycle Management	21%
3. Security Compliance Management	14%
4. Contingency Management	12%
5. Law, Ethics and Incident Management	15%
Total:	**100%**

Domain 1: Security Leadership and Management

1.1 Understand Security's Role in the Organization's Culture, Vision and Mission

- Define information security program vision and mission
- Align security with organization's goals and objectives
- Understand business processes and their relationships
- Describe the relationship between organization culture and security

1.2 Align Security Program with Organizational Governance

- Understand the organizational governance structure
- Understand the roles of key stakeholders
- Recognize sources and boundaries of authorization
- Define the security governance structure

1.3 Define and Implement Information Security Strategies

- Identify security requirements from business initiative
- Evaluate the capacity and capability to implement security strategies
- Manage implementation of security strategies
- Review and maintain security strategies

1.4 Manage Data Classification

- Sensitivity
- Criticality

1.5 Define and Maintain Security Policy Framework

- Determine applicable external standards
- Establish internal policies
- Garner/build organizational support for policies
- Direct development of and approve procedures, standards, guidelines and baselines
- Ensure periodic review of security policy framework

1.6 Manage Security Requirements in Contracts and Agreements

- Evaluation of service management agreements (e.g., risk, financial)
- Governance of managed services (e.g., "infrastructure, software, platform" as a service)
- Understand impact of organizational change (e.g., mergers and acquisitions, outsourcing, divestitures)
- Monitor and enforce compliance with contractual agreements

1.7 Develop and Maintain a Risk Management Program

- Understand enterprise risk management objectives
- Evaluate risk assessment results
- Communicate security business risk to management
- Determine and manage the appropriate countermeasures and make recommendations
- Obtain management acceptance and support of residual risk

1.8 Manage Security Aspects of Change Control

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

1.9 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

1.10 Define, Measure, and Report Security Metrics

- Identify KPIs
- Relate KPIs to the risk position of the organization
- Use metrics to drive security program development

1.11 Prepare, Obtain, and Administer Security Budget

- Manage and report financial responsibilities
- Prepare and secure annual budget
- Understand economic environment

1.12 Manage the Security Organization (e.g., define roles and responsibilities, determine FTEs, performance evaluation)

1.13 Understand Project Management Principles (e.g., time, scope, and cost relationship, work breakdown structure)

Domain 2: Security Lifecycle Management

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

- Identify lifecycle processes within the organization
- Integrate information security gates (decision points) and milestones into lifecycle
- Monitor compliance with the lifecycle
- Oversee the configuration management process

2.2 Integrate New Business Initiatives into the Security Architecture

- Participate in development of business case for new initiatives to integrate security
- Address impact of new business initiatives on security (e.g., cloud, big data)

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
- Remediate vulnerabilities based on risk

Domain 3: Security Compliance Management

3.1 Validate Compliance with Organizational Security Policies and Procedures

- Define a compliance framework
- Implement validation procedures outlined in framework
- Utilize and report on security compliance metrics

3.2 Manage and Document Exceptions to the Compliance Framework

3.3 Coordinate with Auditors and Assist with the Internal and External Audit Process

- Preparation
- Scheduling (e.g., availability, mitigation timeline)
- Evaluation (e.g., validate findings, assess impact, provide comments, and resolution)
- Formulate response

Domain 4: Contingency Management

4.1 Oversee Development of Contingency Plans

- Address challenges related to the business continuity process (e.g., time, resources, verification)
- Address challenges related to the disaster recovery process (time, resources, verification)
- Coordinate with key stakeholders
- Understand organizational drivers and policies
- Oversee Business Impact Analysis (BIA) process

4.2 Guide Development of Recovery Strategies

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

4.3 Manage Maintenance of the BCP and DRP plans (e.g., lessons learned, architecture changes)

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

Domain 5: Law, Ethics and Incident Management

5.1 Understand the Impact of Laws that Relate to Information Security

- Understand global privacy laws (e.g. customer, employee)
- Understand legal footprint of the organization (e.g., trans border data flow)
- Understand export laws
- Understand intellectual property laws (e.g., trademark, copyright, patent, licensing)
- Manage liability (e.g., downstream and upstream/direct and indirect)

5.2 Develop and Manage the Incident Handling and Investigation Processes

- Establish and maintain incident handling process
- Establish and maintain investigation process
- Quantify and report the financial impact of incidents and investigations to senior management

5.3 Understand Management Issues as They Relate to the (ISC)² Code of Ethics

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: +1.727.785.0189
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