CISSP®

ISSMP®

Certified Information Systems Security Professional

Management

Certification **Exam Outline**

Effective Date: November 15, 2022

(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. CISSP-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 CISSP-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 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 two years cumulative paid work experience in one or more of the six domains of the CISSP-ISSMP CBK. You can learn more about CISSP-ISSMP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CISSP-Concentrations#steps-to-certification.

Accreditation

CISSP-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 CISSP-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 CISSP-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 items	125
Item 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	20%
2. Systems Lifecycle Management	18%
3. Risk Management	19%
4. Threat Intelligence and Incident Management	17%
5. Contingency Management	15%
6. Law, Ethics and Security Compliance Management	11%
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
- » Define security's relationship to the overall business processes
- » Define the relationship between organizational culture and security

1.2 Align security program with organizational governance

- » Identify and navigate organizational governance structure
- » Validate roles of key stakeholders
- » Validate sources and boundaries of authorization
- » Advocate and obtain 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
- » Prescribe security architecture and engineering theories, concepts and methods

1.4 Define and maintain security policy framework Determine applicable external standards

- » Determine applicable external standards
- » Determine data classification and protection requirements
- » Establish internal policies
- » Advocate and 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)
- Ensure that appropriate regulatory compliance statements and requirements are included in contractual agreements
- Monitor and enforce compliance with contractual agreements

1.6 Manage security awareness and training programs

- Promote security programs to key stakeholders
- Identify needs and implement training programs 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)
- Associate Key Performance Indicators (KPI) to the risk posture of the organization
- Use metrics to drive security program development and operations

1.8 Prepare, obtain and administer security budget

- Prepare and secure annual budget
- Adjust budget based on evolving risks and threat landscape
- Manage and report financial responsibilities

1.9 Manage security programs

- Define roles and responsibilities
- Determine and manage team accountability
- Build cross-functional relationships
- Resolve conflicts between security and other stakeholders
- Identify communication bottlenecks and barriers
- Integrate security controls into human resources processes

1.10 Apply product development and project management principles

- Incorporate security into project lifecycle
- Identify and apply appropriate project management methodology
- Analyze project time, scope and cost relationship

Domain 2: Systems Lifecycle Management

2.1 Manage integration of security into Systems Development Life Cycle (SDLC)

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

2.2 Integrate new business initiatives and emerging technologies into the security architecture

- Integrate security into new business initiatives and emerging technologies
- Address impact of new business initiatives on security posture

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

- Identify, classify and prioritize assets, systems and services based on criticality to business
- Prioritize threats and vulnerabilities
- Manage security testing
- Manage mitigation and/or remediation of vulnerabilities based on risk

2.4 Manage security aspects of change control

- Integrate security requirements with change control process
- Identify and coordinate with the stakeholders
- Manage documentation and tracking
- Ensure policy compliance (e.g., continuous monitoring)

Domain 3: Risk Management

3.1 Develop and manage a risk management program

- Identify risk management program objectives
- Communicate and agree on risk management objectives with risk owners and other stakeholders
- Determine scope of organizational risk program
- Identify organizational security risk tolerance/appetite
- Obtain and verify organizational asset inventory
- Analyze organizational risks
- Determine countermeasures, compensating and mitigating controls
- Perform cost-benefit analysis (CBA) of risk treatment options

3.2 Conduct risk assessments

- Identify risk factors

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

- Identify supply chain security risk requirements
- Integrate supply chain security risks into organizational risk management
- Validate security risk control within the supply chain
- Monitor and review the supply chain security risks

Domain 4:
Threat Intelligence and Incident Management

4.1 Establish and maintain threat intelligence program

- Aggregate threat data from multiple threat intelligence sources
- Conduct baseline analysis of network traffic, data and user behavior
- Detect and analyze anomalous behavior patterns for potential concerns
- Conduct threat modeling
- Identify and categorize an attack
- Correlate related security event and threat data
- 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
- 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 Facilitate development of contingency plans

» Identify and analyze factors related to the Continuity of Operations Plan (COOP)
» Identify and analyze factors related to the business continuity plan (BCP) (e.g., time, resources, verification)
» Identify and analyze factors related to the disaster recovery plan (DRP) (e.g., time, resources, verification)
» Coordinate contingency management plans with key stakeholders
» Define internal and external crisis communications plans
» Define and communicate contingency roles and responsibilities
» Identify and analyze contingency impact on business processes and priorities
» Manage third-party contingency dependencies
» Prepare security management succession plan

5.2 Develop recovery strategies

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

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

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

5.4 Manage disaster response and 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 Identify the impact of laws and regulations that relate to information security

- Identify applicable privacy laws
- Identify legal jurisdictions the organization and users operate within (e.g., trans-border data flow)
- Identify export laws
- Identify intellectual property (IP) laws
- Identify applicable industry regulations
- Identify and advise on non-compliance risks

6.2 Adhere to the (ISC)^2 Code of Ethics as related to management issues

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

- Inform and advise senior management
- Evaluate and select compliance framework(s)
- Implement the compliance framework(s)
- Define and monitor compliance metrics

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

- Plan
- Schedule
- Coordinate audit activities
- Evaluate and validate findings
- Formulate response
- Validate implemented mitigation and remediation actions

6.5 Document and manage compliance exceptions

- Identify and document compensating controls and workarounds
- Report and obtain 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

(ISC)² recommends that CISSP-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/Exams/Before-Your-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 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