CISSP®

ISSEP®

Certified Information Systems Security Professional Engineering

Certification Exam Outline

Effective Date: March 2018

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

About CISSP-ISSEP

The Information Systems Security Engineering Professional (ISSEP) is a CISSP who specializes in the practical application of systems engineering principles and processes to develop secure systems. An ISSEP analyzes organizational needs, defines security requirements, designs security architectures, develops secure designs, implements system security, and supports system security assessment and authorization for government and industry.

The broad spectrum of topics included in the ISSEP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of security engineering. Successful candidates are competent in the following 5 domains:

- Security Engineering Principles
- Risk Management
- Security Planning, Design, and Implementation
- Secure Operations, Maintenance, and Disposal
- Systems Engineering Technical 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-ISSEP CBK.

Accreditation

ISSEP 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 ISSEP. 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 ISSEP. 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-ISSEP Examination Information

Length of exam	3 hours
Number of questions	150
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

CISSP-ISSEP Examination Weights

Domains	Weight
1. Security Engineering Principles	22%
2. Risk Management	24%
3. Security Planning, Design, and Implementation	22%
4. Secure Operations, Maintenance, and Disposal	21%
5. Systems Engineering Technical Management	11%
Total:	**100%**

Domain 1: Security Engineering Principles

1.1 General Security Principles

- Identify organizational security authority
- Identify elements of a system security policy
- Understand trust concepts and hierarchies
- Determine boundaries governed by security policies
- Specify complete mediation
- Determine least common mechanism
- Understand open design concepts
- Analyze psychological acceptability/usability
- Understand the importance of consistent measurement

1.2 Security Risk Management Principles

- Align security risk management with enterprise risk management
- Integrate risk management throughout the lifecycle

1.3 System Resilience Principles

- Apply resilience methods to address threats
- Understand concepts of layered security
- Specify fail-safe defaults
- Avoid single points of failure

1.4 Vulnerability Management Principles

- Incorporate least privilege concepts
- Understand economy of mechanism
- Understand separation of privilege/duties concepts
- Understand security best practices applicable to the context

Domain 2: Risk Management

2.1 Risk Management Process

- Establish risk context
- Identify system security risks
- Perform risk analysis
- Perform risk evaluation
- Recommend risk treatment options

2.2 Operational Risk Management

- Confirm operational risk appetite
- Identify remediation needs and other system changes
- Propose remediation for unaccepted security risks
- Assess proposed remediation or change activities
- Participate in implementation of the remediation or change
- Perform verification and validation activities relative to the requirements impacted
- Update risk assessment documentation to account for the impact of the remediation or change

Domain 3: Security Planning, Design, and Implementation

3.1 Stakeholder Requirements Definition

- Define security roles and responsibilities
- Understand stakeholders' mission/business and operational environment
- Identify security-relevant constraints and assumptions
- Identify and assess threats to assets
- Determine protection needs
- Document stakeholder requirements
- Analyze stakeholder requirements

3.2 Requirements Analysis

- Develop system security context
- Identify security functions within the security concept of operations
- Develop system security requirements baseline
- Analyze and define security constraints
- Analyze system security requirements for completeness, adequacy, conflicts, and inconsistencies

3.3 System Security Architecture and Design

- Perform functional analysis and allocation
- Maintain mutual traceability between specified design and system requirements
- Define system security design components
- Perform trade-off studies for system components
- Assess information protection effectiveness

3.4 Implementation, Integration, and Deployment of Systems or System Modifications

- Perform system security implementation and integration
- Perform system security deployment activities

3.5 Verification and Validation of Systems or System Modifications

- Perform system security verification
- Perform system security validation

Domain 4:
Secure Operations, Maintenance, and Disposal

4.1 Secure Operations

- Document and maintain secure operations strategy
- Maintain and monitor continuous monitoring processes
- Support the incident response process

4.2 Secure Maintenance

- Develop and direct secure maintenance strategy
- Participate in system remediation and change management processes
- Perform scheduled security reviews

4.3 Secure Disposal

- Develop and direct secure disposal strategy
- Verify proper security protections are in place during the decommissioning and disposal processes
- Document all actions and results of the disposal process

Domain 5: Systems Engineering Technical Management

5.1 Acquisition Process

- » Prepare security requirements for acquisitions
- » Participate in vendor selection
- » Participate in supply chain risk management
- » Participate in contractual documentation development to verify security inclusion
- » Perform acquisition acceptance verification and validation

5.2 System Development Methodologies

- » Integrate security tasks and activities into system development methodologies
- » Verify security requirements are met throughout the process

5.3 Technical Management Processes

- » Identify opportunities for automation of security processes
- » Perform project planning processes
- » Perform project assessment and control processes
- » Perform decision management processes
- » Perform risk management processes
- » Perform configuration management processes
- » Perform information management processes
- » Perform measurement processes
- » Perform quality assurance processes

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 ISSEP 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