CISSP®

Certified Information Systems Security Professional

ISSEP® Engineering

Certification **Exam Outline**

Effective Date: November 13, 2020

(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 five domains:

- Systems Security Engineering Foundations
- Risk Management
- Security Planning and Design
- Systems Implementation, Verification and Validation
- Secure Operations, Change Management and Disposal

Experience Requirements

Candidates must be a CISSP in good standing and have two years cumulative paid work experience in one or more of the five domains of the CISSP-ISSEP CBK. You can learn more about CISSP-ISSEP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CISSP-ISSEP/experience-requirements.

Accreditation

CISSP-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 items	125
Item 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. Systems Security Engineering Foundations	25%
2. Risk Management	14%
3. Security Planning and Design	30%
4. Systems Implementation, Verification and Validation	14%
5. Secure Operations, Change Management and Disposal	17%
Total:	**100%**

Domain 1: Systems Security Engineering Foundations

1.1 Apply systems security engineering fundamentals

- Understand systems security engineering trust concepts and hierarchies
- Identify the relationships between systems and security engineering processes
- Apply structural security design principles

1.2 Execute systems security engineering processes

- Identify organizational security authority
- Identify system security policy elements
- Integrate design concepts (e.g., open, proprietary, modular)

1.3 Integrate with applicable system development methodology

- Integrate security tasks and activities
- Verify security requirements throughout the process
- Integrate software assurance methods

1.4 Perform technical management

- 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 (QA) processes
- Identify opportunities for security process automation

1.5 Participate in the acquisition process

- Prepare security requirements for acquisitions
- Participate in selection process
- Participate in Supply Chain Risk Management (SCRM)
- Participate in the development and review of contractual documentation

1.6 Design Trusted Systems and Networks (TSN)

Domain 2: Risk Management

2.1 Apply security risk management principles

» Align security risk management with Enterprise Risk Management (ERM)

» Integrate risk management throughout the lifecycle

2.2 Address risk to system

» Establish risk context

» Identify system security risks

» Perform risk analysis

» Perform risk evaluation

» Recommend risk treatment options

» Document risk findings and decisions

2.3 Manage risk to operations

» Determine stakeholder risk tolerance

» Identify remediation needs and other system changes

» Determine risk treatment options

» Assess proposed risk treatment options

» Recommend risk treatment options

Domain 3: Security Planning and Design

3.1 Analyze organizational and operational environment

- Capture stakeholder requirements
- Identify relevant constraints and assumptions
- Assess and document threats
- Determine system protection needs
- Develop Security Test Plans (STP)

3.2 Apply system security principles

- Incorporate resiliency methods to address threats
- Apply defense-in-depth concepts
- Identify fail-safe defaults
- Reduce Single Points of Failure (SPOF)
- Incorporate least privilege concept
- Understand economy of mechanism
- Understand Separation of Duties (SoD) concept

3.3 Develop system requirements

- Develop system security context
- Identify functions within the system and security Concept of Operations (CONOPS)
- Document system security requirements baseline
- Analyze system security requirements

3.4 Create system security architecture and design

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

Domain 4: Systems Implementation, Verification and Validation

4.1 Implement, integrate and deploy security solutions

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

4.2 Verify and validate security solutions

- Perform system security verification
- Perform security validation to demonstrate security controls meet stakeholder security requirements

Domain 5: Secure Operations, Change Management and Disposal

5.1 Develop secure operations strategy

- Specify requirements for personnel conducting operations
- Contribute to the continuous communication with stakeholders for security relevant aspects of the system

5.2 Participate in secure operations

- Develop continuous monitoring solutions and processes
- Support the Incident Response (IR) process
- Develop secure maintenance strategy

5.3 Participate in change management

- Participate in change reviews
- Determine change impact
- Perform verification and validation of changes
- Update risk assessment documentation

5.4 Participate in the disposal process

- Identify disposal security requirements
- Develop secure disposal strategy
- Develop decommissioning and disposal procedures
- Audit results of the decommissioning and disposal process

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 Americas
Tel: +1-866-331-ISC2(4722)
Email: membersupport@isc2.org

(ISC)² Asia Pacific
Tel: +852-2850-6951
Email: membersupportapac@isc2.org

(ISC)² EMEA
Tel: +44-203-960-7800
Email: membersupportemea@isc2.org