CISSP®

ISSEP®

Certified Information Systems Security Professional

Engineering

Certification **Exam Outline**

Effective Date: March 2012

(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 information security. Successful candidates are competent in the following 4 domains:

- Systems Security Engineering (SSE)
- Certification and Accreditation (C&A)/Risk Management Framework (RMF)
- Technical Management
- U.S. Government Information Assurance Related Policies and Issuances

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 4 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. Systems Security Engineering (SSE)	50%
2. Certification and Accreditation (C&A)/Risk Management Framework (RMF)	15%
3. Technical Management	15%
4. U.S. Government Information Assurance Related Policies and Issuances	20%
Total:	**100%**

Domain 1: Systems Security Engineering (SSE)

1.1 Understand relationship between security engineering and systems engineering

- Understand security and systems engineering methodologies (e.g., Institute of Electrical and Electronics Engineers (IEEE) 1220, INCOSE Systems Engineering Handbook)
- Understand process models (e.g., lifecycle models, Systems Security Engineering Capability Maturity Model (SSE-CMM), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 21827, ISO/IEC 15288)

1.2 Discover information protection needs

- Understand the customer's mission or business
- Understand the customer's operational environment (e.g., physical and human)
- Identify data types and determine additional legal / regulatory requirements
- Determine relationship / importance of information to mission
- Identify security services / objectives (e.g., Confidentiality, Integrity, Availability (CIA) triad)
- Identify classes of threats
- Determine impacts to the mission or business
- Identify security roles and responsibilities
- Identify constraints and assumptions
- Document the information protection needs
- Assess information protection effectiveness (e.g., gap analysis)

1.3 Define System Security Requirements

- Develop system security context (e.g., support system, application)
- Develop security concept of operations (CONOPS) as part of the overall system CONOPS
- Develop system security requirements baseline
- Review design constraints
- Assess information protection effectiveness
- Design System Security Architecture
- Perform functional analysis and allocation
- Assess information protection effectiveness

1.4 Develop Detailed Security Design

- Define system security design components
- Perform trade-off studies
- Assess information protection effectiveness
- Design System Security Architecture
- Perform functional analysis and allocation
- Assess information protection effectiveness

1.5 Implement System Security

- Support security implementation, integration, and test
- Support test and evaluation process
- Assess information protection effectiveness

Domain 2: Certification and Accreditation (C&A)/ Risk Management Framework (RMF)

2.1 Understand the U.S. Government C&A/RMF process to be applied (e.g., National Information Assurance Certification and Accreditation Process (NIACAP), DoD Information Assurance Certification and Accreditation Process (DIACAP), National Institute of Standards and Technology Special Publication (NIST SP) 800-37 rev 1)

- Understand the purpose of C&A/RMF
- Identify and understand criteria used to determine applicability of U.S. Government C&A/RMF processes

2.2 Understand the roles and responsibilities of stakeholders identified within the C&A/RMF process

2.3 Integrate the C&A/RMF process with systems security engineering

- Understand the attributes and significance of well-defined, integrated processes (e.g., administrative security policies/procedures and their relationship to C&A/RMF)
- Understand documentation requirements
- Understand the purpose of specific documentation (e.g., change management plan, systems engineering management plan)
- Understand the importance of security guidance and standards
- Understand the relationship of an organization's business goals from a systems security engineering perspective
- Understand continuous improvement process
- Identify and correlate C&A/RMF phases and tasks with systems engineering phases and tasks
- Participate in development and execution of the Plan of Action and Milestones (POAM)
- Support C&A/RMF activities as appropriate based on C&A/RMF tailoring (e.g., register system with the appropriate information assurance program, communicate results of risk analysis to certifier and accreditor, prepare and present C&A/RMF documentation to accreditor, submit reports to centralized database)

Domain 3: Technical Management

3.1 Understand and support the acquisition process

3.2 Initiate the technical effort

- Understand the importance of project charters
- Document risks, assumptions, and constraints
- Understand the purpose of stakeholder analysis
- Determine scope of technical effort

3.3 Plan the technical effort

- Use system development methodologies / models
- Identify project team members and their roles
- Develop work breakdown structure and project schedule
- Identify deliverables
- Identify risks and risk management strategies
- Define performance metrics
- Allocate resources and estimate project costs
- Align technical effort with organizational processes (e.g., change management, configuration management)
- Prepare technical management plan (e.g., System Engineering Management Plan (SEMP), Test and Evaluation Master Plan (TEMP))
- Review project plan
- Obtain customer concurrence

3.4 Implement and manage the technical effort

- Execute project plans
- Comply with organizational processes (e.g., change control, quality assurance)
- Monitor and control project resources, project parameters, and performance metrics (e.g., Earned Value Management (EVM), Technical Performance Measures (TPM))
- Report project status

3.5 Close the technical effort

- Obtain final acceptance of technical project
- Support the project closure processes
- Collect and record lessons learned
- Release project resources
- Archive historical data
- Dispose of sensitive data

Domain 4: U.S. Government Information Assurance Related Policies and Issuances

4.1 Understand national laws and policies

4.2 Understand civil agency policies and guidelines

4.3 Understand DoD policies and guidelines

4.4 Understand applicable international standards

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: +1.727.785.0189
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