

ISSEP - Information Systems Security Engineering Professional

SecureNinja's CISSP-ISSEP training and certification boot camp in Washington, DC and San Diego, CA is a specialty of the CISSP in which you will learn the competence of the four domains of the Information Systems Security Engineering Professional (ISSEP) Concentration, with in-depth study of information security topics related specifically to engineering.

Topics Covered

- Be able to demonstrate his or her knowledge of the standards and regulations pertaining to systems security engineering, certification and accreditation, information assurance, and technical management.
- Be able to demonstrate his or her knowledge of the four domains of the CISSP-ISSEP CBK through various scenarios and models
- Create a study plan to successfully pass the CISSP-ISSEP Examination

The five domains of the CBK covered by CISSP-ISSEP certification are:

- **Domain 1: Systems Security Engineering Foundations**

Focuses on understanding and applying security engineering principles, methodologies, and processes. It covers security design considerations, system security architecture, and security engineering frameworks to ensure robust and resilient information systems.

- **Domain 2: Risk Management**

Involves identifying, assessing, and mitigating risks throughout the system lifecycle. It includes risk analysis methodologies, threat modeling, security assessments, and ensuring compliance with security policies and regulations to protect systems from potential vulnerabilities and threats.

- **Domain 3: Security Planning and Design**

Covers the development of security architectures and plans that align with organizational objectives and regulatory requirements. It includes designing secure systems, implementing security controls, and integrating security into system development lifecycles to enhance overall system security posture.

- **Domain 4: Systems Implementation, Verification, and Validation**

Ensures that security measures are properly implemented and function as intended throughout a system's lifecycle. It includes security testing, verification, validation, and evaluation of security controls to confirm compliance with security

requirements and effectiveness in mitigating risks.

- **Domain 5: Secure Operations, Change Management, and Disposal**

Addresses maintaining security during system operations, securely managing changes, and ensuring the proper decommissioning of systems. It includes incident response, continuous monitoring, security auditing, and securely disposing of retired systems to prevent unauthorized access or data breaches.

Who Would Benefit

CISSPs looking to become an Information Systems Security Engineering Professional

Prerequisites

CISSP certification

Required Exams

CISSP-ISSEP Exam

- Format: 125 multiple-choice questions.
- Duration: 3 hours.
- Passing Score: 700 out of 1000 points.

Courseware

SecureNinja Courseware

Course Length

- 5 Days
- 40 hours

Follow On Courses

CISSP-ISSAP, CISSP-ISSMP