Hewlett Packard Enterprise

CISSP—ISSEP: Information Systems Security Engineering Professional H0DU9S

This Official (ISC)² course provides a comprehensive review of information security concepts and industry best practices, covering the four domains of the ISSEP CBK: Systems Security Engineering, Certification and Accreditation (C&A)/Risk Management Framework (RMF), technical management, U.S. government information assurance related policies and issuances.

HPE course number	H0DU9S
Course length	4 days
Delivery mode	ILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

Why HPE Education Services?

- IDC MarketScape leader 4 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and (ISC)²
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, January 2016

Audience

This course is intended for CISSPs who have at least 2 years of recent full-time professional work experience in engineering and are pursuing ISSEP training and certification to demonstrate mastery in security engineering to advance within their current information security careers. The training seminar is ideal for those working in positions such as, but not limited to:

- Senior systems engineer
- Information assurance systems engineer
- Information assurance officer
- Information assurance analyst
- Senior security analyst

Course description

In this course, you will find that several types of activities are used to reinforce topics and increase knowledge retention. These activities include open-ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

Course objectives

With a primary focus on the U.S. government policy and regulations, this course examines the process that is applied throughout the life cycle of the systems that comprise the ISSE model and ensures that security is included in these systems. After completing this course, participants will be able to:

- Describe concepts related to how certification and accreditation and risk management framework processes are applied and integrated/implemented with systems security engineering
- Explain the details of technical management, including how to design, implement, and execute technical aspects related to systems security engineering
- Describe how U.S. government information assurance laws, regulations, policies, and standards apply to information systems security

- Apply knowledge of systems security engineering to protect organizational information through a process, which includes identifying needs, designing the architecture, developing systems security requirements, and implementing those requirement

Benefits to you

This course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the ISSEP exam and features:

- Official (ISC)² courseware
- Taught by an authorized (ISC)² instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Detailed course outline

Domain 1: Systems Security Engineering (SSE)	• Understand relationship between security engineering and systems engineering • Discover information protection needs • Define System Security Requirements • Design System Security Architecture • Develop Detailed Security Design • Implement System Security
Domain 2: Certification and Accreditation (C&A)/Risk Management Framework (RMF)	• Understand the U.S. Government C&A/RMF process to be applied (e.g., National information Assurance Certification and Accreditation Process [DIACPA], National Institute of Standards and Technology) • Special Publication (NIST SP) 800-37 rev. 1) • Understand the roles and responsibilities of stakeholders identified within the C&A/RMF process • Integrate the C&A/RMF process with systems security engineering
Domain 3: Technical management	• Understand and support the acquisition process • Initiate the technical effort • Plan the technical effort • Implement and manage the technical effort • Close the technical effort
Domain 4: U.S. government information assurance related policies and issuances	• Understand national laws and policies • Understand civil agency policies and guidelines • Understand DoD policies and guidelines • Understand applicable international standards

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04755712, September 2016, Rev. 3

Hewlett Packard
Enterprise