Hewlett Packard Enterprise

CISSP—ISSAP: Information Systems Security Architecture Professional H0DU8S

This Official (ISC)² course provides a comprehensive review of information security concepts and industry best practices, covering the six domains of the ISSAP CBK: Access control systems and methodology, communications and network security, cryptography, security architecture analysis, technology related Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), physical security considerations.

HPE course number	H0DU8S
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 architecture and are pursuing ISSAP training and certification to demonstrate mastery in security architecture to advance within their current information security careers. The training seminar is ideal for those working in positions such as, but not limited to:

- System architect
- Chief technology officer
- System and network designer
- Business analyst
- Chief security officer

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

- Define an architecture that will ensure adequate security and reliability for the organization information systems design
- Identify and deploy physical access controls that will enable the complete information system security model to prevent, detect, and react to suspicious activity
- Describe how cryptography is used to protect an organization's data and communications from security threats
- Explain how to select, implement, and monitor communications products according to company standards and policies

- Develop a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for an organization through an understanding of identifying adverse events that could potentially threaten an organization's ability to thrive
- Utilize hard and soft concepts to apply access control methodologies

Benefits to you

This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the ISSAP 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: Access control systems and methodology	• Apply access control concepts, methodologies, and techniques • Determine identity and access management architecture
Domain 2: Communications and network security	• Determine communications architecture • Determine network architecture • Protect communications and networks • Identify security design considerations and associated risks
Domain 3: Cryptography	• Identify requirements (e.g., confidentiality integrity, non-repudiation) • Determine usage (i.e., in transit, at rest) • Identify cryptographic design considerations and constraints • Define key management lifecycle (e.g., creation, distribution, escrow, recovery) • Design integrated cryptographic solutions (e.g., Public Key Infrastructure (PKI), API selection, identity system integration)
Domain 4: Security architecture analysis	• Identify security architecture approach • Perform requirements analysis • Design security architecture • Verify and validate design
Domain 5: Technology related Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)	• Incorporate Business Impact Analysis (BIA) (e.g., legal, financial, stakeholders) • Determine security strategies for availability and recovery • Design continuity and recovery solution
Domain 6: Physical security considerations	• Assess requirements • Integrate physical security products and systems • Evaluate Solutions

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04755699, October 2016, Rev. 3

Hewlett Packard
Enterprise