Hewlett Packard Enterprise

CISSP-ISSMP: Information Systems Security Management Professional H0DV0S

This Official (ISC)² course provides a comprehensive review of information security concepts and industry best practices, covering the 5 domains of the ISSMP CBK: Security leadership and management, security lifecycle management, security compliance management, contingency management, law, ethics, and incident management.

HPE course number	H0DV0S
Course length	5 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

Audience

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

- Chief information officer
- Chief information security officer
- Chief technology officer
- Senior security executive

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

- Understand and apply the fundamental security leadership and management skills and knowledge in managing an organizations information security program.
- Understand and apply the security lifecycle management processes and principles into new business initiatives, as well as the System Development Life Cycle (SDLC), including the operations and maintenance and disposal phases.
- Understand and apply the security compliance management skills in establishing, managing, and overseeing a process to help monitor, assess, and enforce compliance with security policies and procedures.
- Understand and apply contingency management practices in planning and implementing processes for reducing the impact of adverse events, such as natural and man-made disasters, virus outbreak, or equipment failure.

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

- Understand and apply the law, ethics, and incident management practices that apply to the organization and the necessary knowledge and skill in developing processes for managing security incidents, coordinating with law enforcement and legal authorities, identifying and applying guidelines, and keeping the organizations management informed of real or potential impacts.

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 ISSMP 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

This course provides a comprehensive review of information security concepts and industry best practices, covering the following 5 domains of the ISSMP CBK:

Domain 1: Security leadership and management	• Understand security's role in the organization's culture, vision, and mission • Align security program with organizational governance • Define and implement information security strategies • Manage data classification • Define and maintain security policy framework • Manage security requirements in contracts and agreements • Develop and maintain a risk management program • Manage security aspects of change control • Oversee security awareness and training programs • Define, measure, and report security metrics • Prepare, obtain, and administer security budget • Manage the security organization (e.g., define roles and responsibilities, determine FTEs, performance evaluation) • Understand project management principles (e.g., time, scope, and cost relationship, work breakdown structure)
Domain 2: Security lifecycle management	• Manage the integration of security into the System Development Life Cycle (SDLC) • Integrate new business initiatives into the security architecture • Define and Oversee Comprehensive Vulnerability Management Programs (e.g., vulnerability scanning, penetration testing, threat analysis)
Domain 3: Security compliance management	• Validate compliance with organizational security policies and procedures • Manage and document exceptions to the compliance framework • Coordinate with auditors and assist with the internal and external audit process
Domain 4: Contingency management	• Oversee development of contingency plans • Guide development of recovery strategies • Manage maintenance of the BCP and DRP plans (e.g., lessons learned, architecture changes)
Domain 5: Law, ethics, and incident management	• Understand the impact of laws that relate to information security • Develop and manage the incident handling and investigation processes • Understand management issues as they relate to the $(ISC)^2$ Code of Ethics

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04755726, October 2016, Rev. 4

Hewlett Packard
Enterprise