Hewlett Packard Enterprise

Information Security Essentials Plus HL946S

This course focuses on the application of ISO 27001 and regulations in specific areas of the information security lifecycle. It is a follow-on course to Information Security Essentials (HL945S) and provides the information you need to prepare for the Certified Information Security Management Principals (CISMP) certification by British Computer Society (BCS), the Chartered Institute for IT.

HPE course number	HL946S
Course length	2 days
Delivery mode	ILT, VILT
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

- IT Managers or members of Information Security Management Teams who will primarily operate from the ISO 27000 series of standards
- Security and Systems Managers who need to understand information security practices for BCS, the Chartered Institute for IT or operations in the UK
- Anyone working toward the BCS Certificate in Information Security Management Principles (CISMP) certification
- Security practitioners who want more depth about what constitutes a good security governance strategy

Certifications

This course, when combined with the 3-day Information Security Essentials (HL945S) course, provides the 5-day preparation training to prepare for challenging the CISMP certification by BCS.

Prerequisites

- Information Security Essentials (HL945S)

Course objectives

By the end of this course, you should be able to:

- Describe the standards related to security process management, roles, and responsibilities throughout your organization
- Identify the legal requirements that affect your security program
- List standards supporting your choice of controls and countermeasures
- Recognize software development practices that support integrating security requirements
- Describe and prepare for an audit
- List best practices in handling a security incident

Detailed course outline

Module 1: Information security governance	• List the checks and balances between organizational needs and security governance • Describe a holistic organizational approach to governance • Communicate the importance of board level support for information security • Show how information security needs percolate through tiers of management and implementation • List the organizational roles related to information security • Describe the policy development process
Module 2: Legal framework	• List applicable privacy legislation in different regions • Describe typical elements of privacy legislation • Identify potential privacy related offenses • Describe how companies with multiple locations can comply with differing legal requirements • List key organization responsibilities in monitoring employees
Module 3: Relevant standards	• List key standards bodies for various regions • Recognize ISO Standards and their relationships • List the steps in the ISMS cycle • List the elements of the ISMS document • Identify levels of assurance evaluation • Recognize certified products • Recognize key elements of NIST lineage • Describe the importance of encryption standards
Module 4: Software design for security	• Describe software development best practices to ensure security
Module 5: Security audit	• Define key audit related terms • Overview the audit process • List objectives for audits • List types of audit • Describe the auditor's role • List the elements of audit documentation
Module 6: Incident management	• Describe the steps to take during a security incident • List the elements of a security incident report • Describe the process to collect evidence related to an incident

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04570162, hl946S.A.02, February 2017

Hewlett Packard
Enterprise