Hewlett Packard Enterprise

Certificate in Information Security Management Principles (CISMP) HL949S

This training course bundle includes the Information Security Essentials (HL945S) and Information Security Essentials Plus (HL946S) courses. These will prepare you to take the industry recognized Certificate in Information Security Management Principles (CISMP) exam by the British Computer Society (BCS).

HPE course number	HL949S
Course length	5 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

- Anyone working toward the BCS Certificate in Information Security Management Principles (CISMP) certification
- IT managers or members of information security management teams
- Systems managers
- Anyone working towards an industry recognized certification such as ISO/IEC 27001, ISO/IEC 27002, CISMP, CISSP, Security+ or CCSK

Prerequisites

A basic understanding of operating systems and networks

Some experience with managing networks is helpful but not required

Some experience in project management or organizational management may be helpful but not required

Course Objectives

- Champion the security cause in your organization (business need, communicate what applies and relative importance, concrete high-level steps to take, desired outcome, interrelationships of risk assessment, business continuity planning, countermeasures, and policies)
- Describe an integrated approach to Governance, Risk and Compliance (GRC) that moves your organization ahead of mere compliance
- Describe generalized security lifecycle as starting point in organizational discussions, and how processes fit together
- Identify what aspect of security (CIA) is at risk from specific types of attack in your environment
- Outline types of threats, vulnerabilities, and regulations that affect your environment
- 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
- Begin to prepare for industry-recognized security and risk certifications, or a security administration position

Certification

This training prepares you for the CISMP certification from BCS. It also provides a stepping-stone to more advanced certifications, either managerial or technical (such as CISSP, Security+ and CCSK), and fits nicely with existing project management and service management progra

Detailed course outline

3-day Information security essentials outline

Module 1: Setting a secure foundation	• Champion the business case for the importance of information security • Describe how security/IA can become a business advantage • Discuss information assurance maturity models • Identify relevant sources of compliance requirements: legislative, regulatory, client
Module 2: Defining key tenets of information security	• Define information security and its key elements, Confidentiality, Integrity, and Availability • Map compliance requirements to securing information (CIA) • Differentiate between threats, vulnerabilities, and attacks • Apply definitions to an environment • Identify forms of threat • List common enterprise vulnerabilities • Describe what constitutes a security incident
Module 3: Managing information security in the organization	• Communicate the advantages of using an existing framework • Illustrate the security governance lifecycle • List the key roles, responsibilities, and interactions • Describe components of security professionalism and ethics • Differentiate between policy, standard, procedure, and guideline • Distinguish what makes a good security policy • Describe the importance of communicating policies
Module 4: Introduction to IT threats, vulnerabilities, and attacks	• Describe vulnerabilities in client/server communication • Describe why large organizations are vulnerable • Identify physical, technical, and social forms of security threat • Identify and describe the most common attacks • Discuss common examples of social engineering
Module 5: Assessing risk	• Describe the role of risk management in information security and how the elements fit with the security governance lifecycle • Estimate your organization's risk appetite in various key areas and begin a plan to verify • Distinguish business impact analysis from risk assessment • Distinguish quantitative and qualitative risk analysis • List applicable privacy legislation in different regions • List categories of intellectual property law • Define vulnerability scanning • List sample tools for port scanning and other vulnerability scanning • Identify tool selection and comparison criteria • Develop a useful report of outcome of scanning
Module 6: Controlling access	• Describe the importance of access control in implementing information security • Demonstrate how authentication and authorization work together to provide access control • Outline why technical and physical controls for access are both important
Module 7: Selecting controls	• List common controls for each category of threat • List/categorize countermeasures by strategy • Discuss the importance of patch management • Categorize physical controls • Discuss technical countermeasures • Identify firewall positioning in network architecture and the DMZ network • List actions a firewall can take in response to types of traffic • Describe use of intrusion prevention systems

	• Describe how an IPS detects an attack • Compare types of IPS • Describe how virtual private networking supports security objectives • Describe how encryption aids security • Describe how encryption is performed • Distinguish between symmetric and asymmetric encryption • Describe the positioning of virus scanners
Module 8: Planning security for consumerization of it and the cloud	• Describe the impact that the Consumerization of IT is having on IT • Discuss the threats and vulnerabilities in the mobile world • Summarize security interventions for mobile devices • Identify the risks of social media • Summarize controls for social media related threats • Describe the relationship between cloud computing and consumerization • Distinguish types of cloud based computing and services • Identify risks of different forms of cloud use • List controls for security in the cloud • Describe the impact on security of big data, internet of things, and dark web
Module 9: Secure Outsourcing	• Describe the difference between outsourcing and managed service providers • Develop polices, standards, procedures for third party vendors • Understand compliance requirements for working with third parties • List typical obligations for contractors • Champion controls on third party access • Describe security controls for information exchanged with contractors • Develop processes for managing information during supplier changes • Name business continuity management links to outsourced service providers • List investigation and forensics requirements for suppliers
Module 10: Business continuity and disaster recovery planning	• Describe the importance of continuity planning • List conditions that make it necessary • Define continuity planning and terms • Describe the relationship with risk management • Identify elements of a business continuity plan • Compare and contrast BCP and DRP • Define key elements of service level agreements • Describe verification techniques for redundancy • Explain redundancy considerations
Module 11: Implementing strategies for security success	• Address some of the most overlooked threats in IT Security • List best practices in hiring and educating employees

2-day Information security essentials plus 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 • Recognize and interpret a risk register chart
Module 2: Legal framework	• List data that must be kept private • 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 • Identify what constitutes an incident • Describe the process to collect evidence related to an incident
• **Module 7: Business Continuity Management**	• Describe the business continuity lifecycle • List elements of analysis for business impact • Describe considerations for returning to business operation

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04568284, HL949S.A.01, February 2017

Hewlett Packard
Enterprise