Course overview

Certificate in Information Security Management Principles (CISMP) (HL949)

This accredited training course bundle includes the 3-day Information Security Essentials (HL945S) and 2-day Information Security Essentials Plus (HL946S) course. This highly practical 5 days of learning has been accredited by the Information Systems Examination Board (ISEB) of the British Computer Society (BCS) and will prepare you to sit the industry recognized Certificate in Information Security Management Principles (CISMP) exam.

Course description

The Information Security Essentials training prepares you to look at your business through an information security lens, and to develop and implement a comprehensive information security strategy that will help your business to stay competitive. It covers key security concepts, providing real-world examples of how to implement security measures and risk mitigation methods in your organization. Whether you are in management or have a technical role in security, this training is essential for the context you need to understand information security management including risk management, technical and management controls, legal framework, people and physical security, security standards (e.g. ISO 27001/2), business continuity and much more.

During the Information Security Essentials Plus training you will focus on the application of ISO 27001 and regulations in specific areas of the information security lifecycle. You will learn legal requirements that affect your security program, software development practices that support integrating security requirements, best practices in handling a security incident, preparing for an audit and more.

This training 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 programs.

Course title:	Certificate in Information Security Management Principles (CISMP)
HP product number:	HL949
Category/Subcategory:	Information Security
Course length:	5 days
Level:	Introductory
Delivery language:	English
To order:	You can register your interest for this course online at **http://www.hp.com.au/education** .At the site, select the course under Security portfolio and you will see dates for the course. Register your interest for the date of your choice.

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

Accredited Training

This training has been accredited by:
• BCS The Chartered Institute for IT in preparation for the Certificate in Information Security Management Principles(CISMP) certification
• EXIN in preparation for the Information Security Foundation based on ISO/IEC 27002 (ISFS) certification
• APM Group Ltd (APMG) in preparation for the APMG-International ISO/IEC 27001 certification

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

Why education services from HP?

- Comprehensive curriculum of job-specific training leading to vendor certification
- More than 30 years of Education Consulting
- Streamlined purchase and management of training with HP Care Pack Services for Education
- Training you need, when and where you need it with our Remotely Assisted Instructional Learning (RAIL)
- Global training with more than 90 training locations worldwide
- Training provided by expert security practitioners
- Award winning Virtual classrooms and Virtual Labs for a real hands-on experience
- Recognized as an IDC MarketScape leader for IT education (IDC MarketScape: Worldwide IT Education and Training 2012 Vendor Analysis, doc #232870, February 2012)

Next steps

- Information Security Risk Management and Business Continuity Planning (HL947S) and
- Information Security Governance and Policies (HL948S) or
- CSA Certificate of Cloud Security Knowledge Foundation (H1L09S) or
- CSA Certificate of Cloud Security Knowledge Plus (H1L10S)

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
- 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
- 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

Module 9: 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 10: 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

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

For more information

To locate country contact information and to learn more about education services, please visit our worldwide web site at **http://www.hp.com.au/education** .

HL949S.A.00 - Created October 2013