

Information Security Essentials HL945S

HPE course number	HL945S
Course length	3 days
Delivery mode	ILT, VILT
View schedule, local pricing, and register	View now
View related courses	View now

This course 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.

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
- Security and Systems Managers
- Anyone working towards an industry recognized certification such as
 - ISO/IEC 27001, ISO/IEC 27002, CISM, 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

Certifications

This course has been accredited by EXIN for the ISO/IEC 27002 (ISFS) certification and prepares you for the APMG-International ISO/IEC 27001 certification. Also, attend the additional 2-day Information Security Essentials Plus (HL946S) and prepare to challenge the Certified Information Security Management Principles (CISM) exam by

BCS. This course 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 objectives

- Champion the security cause in your organization
- Describe an integrated approach to cyber security
- Move past compliance and to security as an advantage
- Integrate cyber security into the lifecycle of all services
- Understand confidentiality, integrity, and availability
- Improve risk assessment/risk management activities
- Gain knowledge regarding threats, vulnerabilities, and appropriate controls
- List regulations which may impact business goals
- Prepare for industry-recognized cyber security certifications
- Become a Chief Information Security Officer

Detailed course 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 policies, 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
-

Learn more at
hpe.com/ww/learnsecurity

Follow us:



© Copyright 2017 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community. Pivotal and Cloud Foundry are trademarks and/or registered trademarks of Pivotal Software, Inc. in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

c04568253, HL945S.B.02, February 2017