Hewlett Packard Enterprise

HPE Security Governance and Policies HL948S

HPE course number	HL948S
Course length	2 days
Delivery modes	ILT, VILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

This 2-day course shows IT professionals and security officers how to develop an effective security governance strategy for their organization. Students also learn how compliance regulations and industry standard best practices (frameworks) can guide the creation of suitable security policies. This course focuses on real-world implementation, but can also prepare students for Security+ and CISSP certification exams.

Prerequisites

HPE Security Foundation (HL945S), or equivalent knowledge, is required
HPE Risk Management (HL946s) is recommended

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

Detailed course outline

Module 1: Introduction	• Security Policy and Governance • Logistics • Student profile • A word on certifications
Module 2: Information security	• "Security is 10% product and 90% process" • Cost of cyber crime • Directives and legislation in United States, Canada, & APEC • Data privacy legislation in EU member states • CIA: Confidentiality, Integrity, Availability • Risk • The business impact analysis • Risk assessment & risk equation • Threats & vulnerabilities • Countermeasures • Determining the value of an asset
Module 3: Defining your security strategy	• Security strategy and the business • Compliance requirements: HIPAA security rule • Case study • Relationship between corporate mission, corporate culture and security strategy and policy • Applying security and risk concepts to business requirements • Refining business requirements to build a security strategy • Security governance strategy development process
Module 4: Security governance	• Security policy and governance • Strong Security as a Competitive Advantage • Making the case for the value proposition • Role of Chief Security Officer • Role of senior management in the success of your security plan • Other significant roles: Building your team
Module 5: Structure of a security policy	• Attributes of a good security policy • Difference between policies and procedures • Compliance • The HIPAA security rule • PCI data security standard • EU Directive 2009/136/EC • IT Act of India 2000 • Role of regulatory compliance in the development of polices

Module 6: Policies in your security strategy	• SANS top 10 list of policies
	• Selected Security Policies to Get You Started
	• Acceptable use policy
	• Network access policy
	• Remote access policy
	• Personal computing devices policy
	• Risk assessment policy
	• Contingency planning policy
	• Physical security policy
	• Access control policy
	• Data retention and destruction policy
	• Compliance considerations (HIPAA)
	• The 6 laws of compliance
	• Impact of regulatory compliance on specific policies
	• What security policies are required for your company?
Module 7: Policy building framework	• Why use a framework?
	• Framework to structure your collection of policies
	• ISC (2) 10 domains as a framework
	• ISO 17799:2000(E)
	• PCI
	• Policy identification
	• ISO27001
	• Developing basic security polices using industry standard best practices as framework

Security foundations capstone

• Integrating the information from several HPE Security courses

• Developing a security strategy for your company

Learn more at
hpe.com/ww/learnsecurity

Follow us:

f 𝕏 in 🔊 ✉

Hewlett Packard Enterprise