Hewlett Packard Enterprise

HPE Digital Learner (ISC)2 Training SSCP and CSSP Content Pack CP030S

HPE Content Pack number	CP030
Content Pack length	26 hours
Content Pack Category	Category 2
Learn more	**View now**

Why HPE Education Services?

- IDC MarketScape leader 5 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 SUSE
- 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

Both of these certifications will demonstrate that you have the technical skills and knowledge to implement, monitor and administer legacy and cloud IT infrastructure using security best practices, policies and procedures.

These courses are independent of each other but combined will send a powerful message to prospective employers about your skillset.

An employer will feel secure in the knowledge that they are ensuring the best possible training is being made available to fulfil the required roles and responsibilities of the organization.(ISC)2 are known as an industry leader in this space and these certifications will assist in demonstrating both ability and competency in the domains covered by the certifications.

Both courses will assist by practical, hands-on security knowledge in operational IT roles and will provide confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with your organisations Information Security policies and procedures that ensure data confidentiality, integrity and availability.

We highly recommended that you always supplement self paced study with additional material should you want to sit the examination.

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Audience

Security professionals looking to extend consolidate existing infrastructure skills and knowledge to incorporate Cloud technology and services

Prerequisites

- SSCP – Candidates are expected to prove at least one year's experience working in security with specific focus on one or more of the seven domains from the SSCP common body of knowledge (CBK)
- CSSP – Candidates are expected to have at least five years cumulative experience within IT of which 3 years within IT Security one year focused on one or more of the six domains of CCSP or a holder of the CISSP certification
- For security foundations training, refer to the Information Security Essentials course at hpe.com/ww/learnsecurity
- **Note: –** Candidates without the required experience may elect to become an Associate of (ISC)² by successfully passing either examination. As an Associate of (ISC)² you will have time to earn the required experience (please see the specific datasheets for more details

Certifications and related examinations

- SSCP – Single exam of 3 hours in duration with 125 questions to be answered (multiple choice and 4 choices)
- CCSP – Single exam of 3 hours in duration with between 100 and 150 questions to be answered (multiple choice and advanced innovative items)

Course Metadata

- Both of these certifications will demonstrate that you have the technical skills and knowledge to implement, monitor and administer legacy and cloud IT infrastructure using security best practices, policies and procedures

Detailed Content Pack outline

Systems Security Certified Practitioner: Access Controls	• Identify characteristics of authentication and the role it plays in access control • Describe best practices for implementing single/multifactor authentication • Describe best practices for implementing single sign-on authentication • Identify best practices for implementing device authentication • Describe characteristics of one-way trust relationships in internetwork trust architectures • Describe characteristics of two-way trust relationships in internetwork trust architectures • Identify characteristics of transitive trust in internetwork trust architectures • Describe characteristics of authorization as part of the identity management life cycle • Identify proofing best practices during the identity management life cycle • Describe provisioning activities as part of the identity management life cycle	• Identify maintenance best practices during the identity management life cycle • Describe entitlement activities during the identity management life cycle • Describe best practices when implementing mandatory access control • Describe best practices when implementing non-discretionary access control • Describe best practices when implementing discretionary access control • Describe best practices when implementing role-based access control • Describe best practices when implementing attribute-based access control • Identify appropriate access controls and best practices for implementation
Systems Security Certified Practitioner: Security Operations	• Identify characteristics of the (ISC)2 Code of Ethics and best practices for compliance • Identify best practices for compliance with organizational code of ethics • Describe characteristics of the concept of confidentiality • Identify characteristics of the concept of integrity • Identify characteristics of the concept of availability • Identify characteristics of the concept of accountability • Identify characteristics of the concept of privacy • Identify characteristics of the concept of non-repudiation	• Identify characteristics of the concept of least privilege • Identify characteristics of the concept of separation of duties • Describe best practices for deterrent security controls • Describe best practices for preventative security controls • Describe best practices for detective security controls • Describe best practices for corrective security controls • Describe best practices for compensating security controls • Identify appropriate best practices when implementing different types of operational security controls
Systems Security Certified Practitioner: Security Administration	• Identify best practices for life cycle asset management • Identify best practices for hardware asset management • Identify best practices for software asset management • Identify best practices for data asset management • Describe how to use technical controls to implement and assess compliance • Describe how to use operational controls to implement and assess compliance • Describe how to use managerial controls to implement and assess compliance • Identify activities in implementing a configuration management plan	• Identify activities in performing a security impact assessment • Identify system architecture and interoperability of systems activities in change management processes • Describe activities for implementing and testing patches, fixes, and updates • Identify security awareness and training activities • Identify physical security operations activities • Identify appropriate activities for participating in change management, security operations, and security administration processes

Systems Security Certified Practitioner: Risk Management	• Describe characteristics of risk visibility and reporting activities • Describe characteristics of risk management concepts • Identify risk assessment characteristics and options • Describe options for risk treatment • Identify how to use audit findings as part of the risk management process • Describe security testing and evaluation activities • Describe how to interpret and report scanning and testing results • Describe characteristics of events of interest as part of continuous monitoring activities	• Describe logging activities as part of operating and maintaining monitoring systems • Describe characteristics and purpose of source systems used in continuous monitoring activities • Use security analytics metrics and trends for analyzing monitoring results • Use visualization to analyze monitoring results • Describe characteristics and purpose of event data analysis activities • Identify best practices for communicating and reporting monitoring analysis results • Identify best practices for Identifying, monitoring, and analyzing risk
Systems Security Certified Practitioner: Incident Response and Recovery	• Describe incident discovery activities • Identify incident escalation activities • Identify lessons learned activities • Identify incident response best practices • Identify best practices when implementing countermeasures • Identify first responder best practices during forensic investigation activities • Identify best practices for evidence handling during forensic investigation activities • Describe characteristics and best practices of chain of custody during forensic investigation activities	• Describe characteristics and best practices for supporting emergency response plans and procedures • Describe interim or alternate processing strategies as part of business continuity activities • Identify best practices for restoration planning as part of business continuity activities • Describe characteristics and best practices for implementing backup and redundancy options • Describe characteristics and best practices for testing and drills for supporting emergency response plans and procedures • Identify best practices for handling incidents, supporting forensic investigations, and supporting business continuity activities
Systems Security Certified Practitioner: Cryptography	• Describe purpose and best practices for applying hashing • Describe purpose and best practices for applying salting • distinguish between symmetric and asymmetric encryption application • Describe characteristics and best practices for applying digital signatures • Describe characteristics and best practices for applying non-repudiation • Describe the purpose and role of data sensitivity in cryptography • Identify regulatory requirements for cryptography • Identify end-user training best practices related to cryptography	• Compare differences in implementation methodologies • Describe best practices for appropriate use of security protocols • Identify fundamental key management concepts of cryptographic systems • Describe how to use PKI as part of implementing and operating cryptographic systems • Describe administration and validation activities as part of operating and implementing cryptographic systems • Describe characteristics of Web of Trust • Identify best practices for implementing secure protocols • Identify best practices for implementing and operating cryptographic systems and controls

Systems Security Certified Practitioner: Network and Communications Security	• Distinguish between OSI and TCP/IP models and their role in network security issues • Identify the different types of network topographies and their role in network security • Describe commonly used ports and protocols and their role in network security • Describe best practices and benefits of converged communications • Describe common attacks and countermeasures for protecting telecommunications technologies • Distinguish between access control and monitoring techniques • Describe access control standards and protocols • Describe best practices for remote access operation and configuration • Describe common network access attacks and appropriate countermeasures • Describe data plane and control plane separation for managing LAN-based security	• Use segmentation for managing LAN-based security • Identify best practices for secure device management • Identify best practices for using firewalls and proxies • Identify best practices for using network intrusion detection and prevention systems • Identify best practices for using routers and switches securely on networks • Identify best practices for using traffic-shaping devices • Identify best practices for secure wireless transmission • Describe characteristics of wireless security devices • Identify common attack methods and countermeasures for wireless technologies • Identify best practices for securing networks, protecting telecommunications technologies, and implementing and operating secure wireless technologies
Systems Security Certified Practitioner: Systems and Application Security	• Describe characteristics of malicious code • Identify countermeasures for mitigating risk and damage from malicious code • Distinguish between different types of malicious activity • Identify countermeasures for mitigating risk and damage from malicious activity • Use HIDS for endpoint device security • Use host-based firewalls for endpoint device security • Use application whitelisting for endpoint device security • Use endpoint encryption for endpoint device security • Use trusted platform module for endpoint device security • Use mobile device management for endpoint device security • Identify secure browsing best practices for endpoint device security • Distinguish between cloud security operation models • Distinguish between cloud security service models • Describe characteristics of cloud virtualization • Identify the legal and privacy concerns associated with cloud security • Identify secure data storage and transmission options for cloud security	• Identify security requirements when outsourcing cloud services • Identify application vulnerabilities that apply to big data systems • Identify architecture and design vulnerabilities that apply to big data systems • Describe best practices for secure software-defined networking in virtual environments • Identify characteristics and role of hypervisors in virtual environments • Describe characteristics of virtual appliances and their role in virtual environments • Describe continuity and resilience in secure virtual environments • Identify the most common attacks on virtual environments and countermeasures for mitigating risk and damage • Describe best practices for shared storage in virtual environments • Describe best practices for implementing and operating systems and application security
TestPrep Systems Security Certified Practitioner (SSCP)	• To test your knowledge on the skills and competencies being measured by the vendor certification exam. TestPrep can be taken in either Study or Certification mode. Study mode is designed to maximize learning by not only testing your knowledge of the material, but also by providing additional information on the topics presented. Certification mode is designed to test your knowledge of the material within a structured testing environment, providing valuable feedback at the end of the test.	

Cloud System Architecture – Concepts and Design	• Define and Describe cloud components • Define cloud system participants: consumers, providers, partners, auditors, regulators • Outline the operational characteristics of cloud computing • Outline the supporting architectural components and infrastructure of cloud computing • Detail Cloud Computing Activities with reference to ISO/IEC 17789, Clause 9 • Define how cloud services are categorized based on supported services and capabilities • Describe the industry-Defined standard categories of cloud computing • Describe the Defined deployment models of the cloud services • Describe the additional operational aspects of the cloud service environment • Describe the encryption of cloud-hosted assets • Define access and access control to cloud-hosted assets (data, files, and resources) • Outline asset and media management with respect to deletion/removal/overwrite on a cloud platform • Define issues and solutions relating to cloud network structures	• Define issues and solutions relating to cloud virtualization infrastructures • List and Describe known and common threats to cloud infrastructure and data assets • Define security considerations and responsibilities on a per Cloud Model (Category basis – IaaS, PaaS, and SaaS plus their various derivatives) • Detail the security-based data life cycle of cloud-hosted assets (data, files, features) • Describe business continuity and disaster recovery as it applies to a cloud service • Define how a cloud deployment might be analyzed on a cost basis • Define and Describe focus areas relating to the functional security of the cloud service including vendor lock-in, interoperability, portability, migration, etc. • Describe methodologies for mapping cloud service requirements to service provider certification and product certifications • Outline methodologies for mapping cloud components to appropriate or required industry certifications or industry standards • Define Cloud Service roles, categories, and services; Describe data state and data asset classification with reference to security; and Outline the purpose of Common Criteria
Cloud Data Security	• Define the various life stages of cloud-hosted data assets • Define the various technologies associated with data asset security and protection • Define storage modes in a cloud computing environment, and be able to map data assets to appropriate storage mode • Define and Describe potential threats associated with storage types • Define threat mitigation technology and techniques • Define encryption as it applies to cloud-hosted data • Describe key-pair management as it applies to cloud-hosted data • Describe data masking and masking methodologies • Describe data tokenization technologies • Describe technology selection with respect to criteria • List active data privacy protection legislation by jurisdiction – Data Privacy Acts/Laws • Describe data discovery and its implementation methodologies	• Outline data classification and the classification of discovered sensitive data • Detail data asset mapping to data control types • Define data rights objects in terms of user access control, managing roles, and role-based access options • Define data retention policy principles and how to develop appropriate practices • Outline principles, and how to Define and manage data deletion procedure and methodologies • Outline principles, and how to Define and manage data archiving procedures and methodologies • List event sources and associated identity • Detail event recording, analyzing event data, and aspects of storage and protection of event data • Describe COC as it applies to data hosted on the cloud and understand how nonrepudiation is handled within a cloud hosting environment • Describe common storage media threats, data protection techniques and failover architectures

Cloud System Security - Platform and Infrastructure	• recognize the physical and virtual components within a cloud platform • define the networking and communication architecture of a cloud platform • define the compute service as it applies to the cloud platform • define the available virtualization options within a cloud platform • define storage and Storage as a Service (STaaS) within a cloud platform • Describe and define risk as it applies to cloud services and underlying infrastructure, and adopt a risk analysis and management posture regarding cloud computing • Describe and define known threats and attack vectors associated with cloud services and infrastructure • define virtualization-specific areas of focus with reference to security such as Hypervisor, VM files, and VM deletion • define and Describe threat mitigation and attack handling techniques including ACL, designing in security, and adopting security measures • design and deploy physical and environmental security mechanisms	• design and deploy security mechanisms to mitigate failure and threats, and avoid attack to the systems and communication hardware within a cloud platform • Describe and manage identification, system, and data access in addition to authentication and authority within the cloud service • define auditing techniques and responsibilities within key areas of focus, including asset access, asset status, deletions, archiving, and reporting • Describe and deploy DR and BC with respect to the cloud environment • Describe and deploy DR and BC with respect to operations and business requirements • define and Describe relevant DR and BC strategies • deploy DR and BC mechanisms • Describe cloud device platforms and associated risks; discuss vulnerabilities within the virtualized infrastructure and attack vectors in general; and finally, discuss available disaster recovery architectures
Cloud Application Security	• Describe awareness and required training to develop an understanding of security focus areas relating to cloud applications • Describe common issues relating to the development of cloud-based applications • Describe common security issues relating to Cloud-hosted applications. Define the importance of foreknowledge regarding cloud application vulnerabilities and OWASP research • Describe the application development life cycle with reference to cloud security • define functional testing as it relates to cloud-based application software • Describe application testing with reference to cloud security. Describe SAST, DAST, and Penetrative Testing methodologies • outline the deployment of verified and approved APIs • Describe the significance of surfacing the Supply-Chain with reference to cloud-hosted application software • define the mechanics, phases, and methodologies associated with application development • define how business requirements impact on application development and throughout the application life time	• Describe requirements and best practices for application configuration, and version management • define known threats and security issues that must be considered when developing cloud-hosted applications • define cloud-specific risks, and assimilate to mitigate threat within the design and during the operational phases of cloud-hosted applications • define how to analyze security threats and risks to an application • Describe associated hardware/software components related to the security of cloud applications • define security protocols and measures associated with application data and data packet protection • Describe isolation and sandboxing as it applies to cloud-hosted applications • Describe the virtualization technology associated with cloud-hosted applications • Describe Federated Identity and its deployment for cloud-hosted application authorization and access • define Single Sign-On/Off and its place within the cloud service security framework • Describe and deploy Multifactor Authentication within a cloud service security framework • Describe the phase of NIST's SDLC and define the difference between SDLF and S-SDLC

Cloud Service – Operations Management

- define the design and implementation of logical elements of a proposed cloud service, including tenant isolation, access control, etc.
- define the design and implementation of physical aspects of a proposed cloud service, including build or rent, location, management
- Describe the deployment and configuration of secured hardware with reference to BIOS, TMP, storage controllers, network controllers, etc.
- Describe the deployment and configuration of secured hardware with reference to BIOS, TMP, storage controllers, network controllers, etc.
- define local machine access controls, and deployment of secure KMV switches
- define techniques to secure network configuration and network support tools, including VLAN, TLS, DHPC and Authorized DHCP, DNS and Secure, and IPSec
- define techniques to secure the datacenter network and network access
- define operating system hardening techniques with reference to OS: Windows, Linux, VMware, etc.
- Describe standalone and cluster host availability, backup, and failover, in addition to load balancing, dynamic optimization (DO), maintenance mode, and general high availability best practice adoption
- Describe the mechanisms for deploying Remote Access, including RDP, Secure Terminal Access
- define the preservation of OS compliance with reference to monitoring and remediation
- Describe requirements and best practices with reference to fixes, patches, and updates
- Describe requirement to continuously monitor and report on host component performance
- Describe requirement to continuously monitor and report on host component performance
- Describe the implementation of back and restore policy with reference to cloud components, including data, configurations, etc.
- define the deployment of network security-related controls, including firewalls, IDS, IPS, honeypot deployment, and vulnerability assessment/threat mitigation
- define requirement for hardware event logging and reporting #1
- define requirement for hardware event logging and reporting #2
- Describe host maintenance, scheduled preventive hardware maintenance, planned backups, hardware redundancy strategy, and notification/continuity
- define the secure configuration of the virtual hardware, including network, storage and elastic expansion, memory, and external devices
- Describe the tolls associated with VM OS installation on the physical host
- Describe compliance and control principles and standards: Change and Continuity Management
- Describe compliance and control principles and standards: Information Security, Service Improvement, Incident, Problem, and Release Management
- Describe compliance and control principles and standards: Configuration, Service Level, Availability and Capacity Management
- Describe and implement risk management
- Describe best practice approach to the deployment of proactive and reactive forensic data collection methods
- Describe and deploy best practice systems that guarantee essential and open contact and communications with cloud system providers, vendors, cloud system consumers and users, partners, auditors, regulators, and any other key stakeholders
- detail datacenter operational design factors and define network component security control, define four system management categories and the NIST Forensic Evidence process, Describe Cloud Service Actor communications

Cloud Service – Legal and Compliance	• Describe areas of legislative conflict with respect to cloud-hosted services • appraise legal risks associated with the provision of cloud services • Describe how to apply control policy with respect to legal requirements • define eDiscovery and its impact on cloud service provision, requirements, and responsibilities • define the legislative requirement related to forensic data management • define PII, outline the difference between contractual and regulated PII, and Describe the differences between confidentiality, integrity, availability, and privacy • Describe the international variations that apply to PII and data privacy • define audit operations and auditor tasks with reference to cloud computing services, and outline distributed service issues with respect to auditing • Describe audit requirements, scope, and reporting as they apply to cloud services • outline challenges associated with auditing the virtualized infrastructure of a cloud-based service • define audit reporting against a background of prevailing standards, and outline audit scope and audit regulation requirements with respect to highly regulated industries • define gap analysis and audit planning with reference to cloud service auditing • Describe the deployment of Internal Information Security Management (ISMS) and Security Control Systems (ISCS) - ISO 27000 Series • Describe the deployment of ISMS and ISCS with reference to ISO, ITIL, and NIST	• Describe issues with obtaining details of a CSP's risk management data • Describe issues surrounding the importance of data ownership and define interrelationships between owner and custodian regarding responsibility • outline measures to mitigate risk • outline the integration of information security and risk management activities into a formal framework • outline the metrics that quantify and measure the extent of a risk associated with cloud service elements and components • define key areas of focus for risk assessment, including supplier, vendors, services, and so on • Describe business requirements with reference to the Service Level Agreement, GAAP guidelines, and standards • Describe the vendor and provider vetting process with reference to certifications, audit and event reporting, accreditations, and so on • Describe the deployment of supply-chain management in the context of cloud services • detail current legislation relating to PII and define a number of widely adopted auditing compliance frameworks and report types; outline available auditing standards and frameworks, Describe ISMS and applicable standards and guidance, and detail a number of cloud service adoption risks; and finally, outline some detail on available cloud service-related risk management frameworks

Interested in purchase of this Content Pack as a stand-alone WBT? Contact Us for information on purchasing this Content Pack for individual use.

Learn more at

www.hpe.com/ww/digitallearner

www.hpe.com/ww/digitallearner-contentpack

Follow us:

CP030S A.00, March 2019

Hewlett Packard Enterprise