Hewlett Packard Enterprise

HPE Digital Learner (ISC)2 Training CISSP and CSSLP Content Pack CP031

HPE Content Pack number	CP031
Content Pack lenght	31 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

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 organisation. (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 software controls in accordance with your organisations Information Security policies and procedures that ensure data confidentiality, integrity and availability are maintained at the highest levels.

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 security knowledge to incorporate the design and implementation of software and software products

Prerequisites

- CISSP – Candidates are expected to prove at least five years' experience working in security with specific focus on two or more of the seven domains from the SSCP common body of knowledge (CBK)
- CSSLP – Candidates are expected to have at least four years cumulative experience in the SDLC area
- 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

Content Pack Objectives

- To understand and articulate the common body of knowledge domains relating to CISSP and SSLP
- Provide the ability to demonstrate you have the technical skills and knowledge to implement, monitor and administer using security best practices, policies and procedures to support the SDLC (software development lifecycle)
- Indicate the preparation required for the SSLP examination
- **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

- CISSP – Single exam of 3 hours in duration with between 100 - 150 questions to be answered (multiple choice and advanced innovative items)
- CSSLP – Single exam of A single exam of 4 hours in duration with 175 multiple choice questions

Detailed Content Pack outline

CISSP 2018: (ISC)² AND SECURITY FUNDAMENTALS	• describe the (ISC)² organization • define the (ISC)² Code of Professional Ethics • recall the CISSP exam contents, format, and scoring • define the CIA triad • recall how information and assets are identified and classified • determine ownership of information and assets	• describe how to protect data privacy • ensure appropriate retention of assets • determine appropriate data security controls • establish information-handling and asset-handling requirements
CISSP 2018: CRYPTOGRAPHIC CLIENT-BASED SYSTEMS	• describe cryptology and cryptographic systems • define integrity and hashing in relation to cryptography • describe various cryptographic methods and techniques • identify cryptanalytic attacks • compare phases of the cryptographic life cycle	• define digital signatures • describe the use and function of public key infrastructure • recall various key management practices • describe key aspects of digital rights management
CISSP 2018 : COMMUNICATION AND NETWORK SECURITY	• identify secure design principles for networking • describe security for network components • define OSI TCP/IP models • compare multilayer and converged protocols • define transmission medium • describe NAC and endpoint security	• identify content-distribution networks • compare various types of unified communications • identify types of wireless network • describe remote access technology • secure virtualized networks
CISSP 2018: IDENTITY AND ACCESS MANAGEMENT (IAM)	• control physical and logical asset access • manage the identification and authentication of entities • integrate identity as a third-party service • implement and manage authorization mechanisms	• describe various access control models • recall how to implement identity management • describe access review and provisioning • describe various federated services
CISSP 2018: SITE AND FACILITY SECURITY CONTROLS	• describe wiring closets and intermediate distribution • identify security controls for server rooms and data centers • define media storage facilities • recall evidence storage techniques and practices	• recognize restricted work area security • describe how to protect utilities and HVAC • describe environmental controls • recall techniques for fire prevention, detection, and suppression
CISSP 2018: SECURITY AND RISK MANAGEMENT (PART 1)	• evaluate and apply security governance principles • determine contractual, legal, industry standard, and regulatory requirements • describe principles and requirements for privacy • recall legal and regulatory considerations • develop, document, and implement security policies, standards, procedures, and guidelines • develop and document scope, plan, and business impact analysis	• align security functions with business strategies and objectives • identify common security control frameworks • ensure compliance with due care and due diligence • identify and analyze cybercrimes and data breaches • compare import/export and transborder data controls • describe licensing, intellectual property, and privacy requirements

CISSP 2018: SECURITY AND RISK MANAGEMENT (PART 2)	• enforce personnel security policies and procedures • apply risk assessment and analysis techniques • respond to risks, including measurement and monitoring	• implement threat modeling concepts and methodologies • apply risk-based management concepts to the supply chain • establish and maintain a security awareness and training program
CISSP 2018: SECURITY ARCHITECTURE AND ENGINEERING (PART 1)	• describe engineering processes using secure design principles • compare various security models • select appropriate security controls based on systems security requirements	• compare security capabilities of various information systems • mitigate vulnerabilities in security architectures and designs
CISSP 2018: SECURITY ARCHITECTURE AND ENGINEERING (PART 2)	• assess vulnerabilities in web-based systems • describe common web-based attacks • reduce security vulnerabilities in various web-based systems • define enterprise mobility management • describe issues related to mobile security and privacy	• reduce security vulnerabilities in mobile systems • assess vulnerabilities in embedded devices • describe and compare common threats to embedded devices • reduce various embedded device vulnerabilities
CISSP 2018: SECURITY ASSESSMENT AND TESTING	• Course Outline: • specify steps that can be taken to support investigations • describe resource provisioning and protection • conduct logging and monitoring operations	• implement various tests of security controls and processes • design and validate audit strategies • conduct security audits • analyze test output and generate reports
CISSP 2018: SECURITY OPERATIONS (PART 1)	• recall various operations security principles • 6.5 Conduct or facilitate security audits • identify asset inventory measures • specify asset management controls	• manage configurations and changes • define and manage privileged accounts • describe security-related legal considerations • define SLAs
CISSP 2018: Security Operations (Part 2)	• describe continuous monitoring • define egress monitoring • recognize SIEM systems • describe IDS and IPS	• compare investigative techniques • collect and handle evidence • describe digital forensics tools, tactics, and procedures • report and document thoroughly
CISSP 2018: CONDUCTING INCIDENT MANAGEMENT	• conduct detective and preventative measures • implement patch and vulnerability management • participate in change management processes • implement recovery strategies • implement disaster recovery processes • test disaster recovery plans	• describe business continuity planning • describe perimeter physical security • describe enterprise physical security • utilize additional physical controls • address personnel safety and security concerns
CISSP 2018: SOFTWARE DEVELOPMENT SECURITY	• integrate security in the SDLC • identify software development phases • identify security controls for development • assess the effectiveness of software security	• assess the security impact of acquired software • apply secure coding techniques • describe secure coding best practices

TESTPREP CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)	• 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.	– This TestPrep is aligned to the 2018 Certification Exam Outline.
CSSLP: SECURE SOFTWARE CONCEPTS	• start the course • recognize the characteristics of confidentiality • identify the characteristics of integrity • identify the characteristics of availability • recognize the characteristics of authentication and authorization • recognize the characteristics of authentication and authorization • identify the role of accounting in assuring security • recognize the characteristics of non-repudiation • identify the characteristics of least privilege • recognize the characteristics of separation of duties • recognize the characteristics of defense in depth • recognize the characteristics of fail-safe • recognize the characteristics of economy of mechanism • recognize the characteristics of complete mediation • recognize the characteristics of open design	• recognize the characteristics of least common mechanism • recognize the characteristics of psychological acceptability • recognize the characteristics of the weakest link • recognize the characteristics of leveraging existing components • recognize the characteristics of privacy • distinguish between different privacy considerations • recognize characteristics of regulations and compliance • distinguish between legal issues to keep in mind during the software lifecycle • recognize characteristics of standards • distinguish between the steps of the general risk management model • identify secure software concepts in the Waterfall methodology • identify secure software concepts in the Agile methodology • recognize the principles and practices behind securing software
CSSLP: SECURE SOFTWARE REQUIREMENTS	• start the course • identify typical internal security requirements • identify typical external security requirements • identify data state categories • identify data usage categories • distinguish between the data owner and data custodian roles • distinguish between the different impact level definitions • distinguish between structured and unstructured data • distinguish between generation, retention, and disposal	• identify characteristics of role and user definitions • identify the role of the deployment environment within functional requirements • distinguish between objects, activities, and actions • identify best practices for sequencing and timing • identify characteristics of software deployment requirements • identify characteristics of operations requirements • identify characteristics of management requirements • recognize what is involved in securing software

CSSLP: SECURE SOFTWARE DESIGN	• distinguish between the different architectural forms and supporting elements of secured distributed computing • recognize best practices for securing service-oriented architecture • recognize best practices for securing rich Internet applications • recognize best practices for securing pervasive and ubiquitous computing • recognize best security practices when integrating with existing architectures • recognize best practices for securing cloud architectures • recognize best practices for securing mobile applications • distinguish between characteristics of authentication and identity management • recognize characteristics of credential management • distinguish between flow control methods	• recognize characteristics of logging • recognize characteristics of data loss prevention • identify benefits of virtualization in secure software design • recognize types of Rights Expression Language or REL in Digital Rights Management or DRM • recognize characteristics of trusted computing • distinguish between database security techniques • distinguish between compilers, interpreters, and hybrid source codes • recognize characteristics of operating systems • distinguish between control systems and firmware • identify best practices for designing secure software
CSSLP: SECURE SOFTWARE IMPLEMENTATION AND CODING	• start the course • recognize characteristics of declarative security • recognize characteristics of programmatic security • locate and list the Open Web Applications Security Project or OWASP "Top 10" • locate and list the Common Weakness Enumeration or CWE list of software weaknesses • recognize examples of using concurrency as a defensive coding practice • recognize examples of using configuration as a defensive coding practice • recognize examples of using cryptology as a defensive coding practice • recognize examples of using output sanitization as a defensive coding practice • recognize examples of using error handling as a defensive coding practice • recognize examples of using input validation as a defensive coding practice • recognize examples of using logging and auditing as a defensive coding practice • recognize examples of using session management as a defensive coding practice	• recognize examples of using exception management as a defensive coding practice • distinguish between safe and unsafe application programming interface or API coding practices • distinguish between examples of static and dynamic type safety enforcement • recognize characteristics of memory management as a defensive coding practice • recognize characteristics of configuration parameter management as a defensive coding practice • recognize examples of tokenizing as a defensive coding practice • recognize characteristics of sandboxing as a defensive coding practice • identify source code and versioning best practices • identify build environment best practices • recognize characteristics of peer-based code reviews • distinguish between static and dynamic code analysis • list the steps for code signing • identify techniques for defensive and secure coding
CSSLP: SECURE SOFTWARE TESTING	• start the course • recognize characteristics of testing artifacts • identify characteristics of functional testing • distinguish between nonfunctional testing methods • distinguish between white-, grey-, and black-box testing • identify environment best practices for ensuring secure software testing • distinguish between bug tracking states • recognize characteristics of attack surface validation for software testing • distinguish between testing standards for software quality assurance • identify the four steps in the penetration process	• recognize characteristics of the fuzzing method • recognize characteristics of scanning • recognize characteristics of simulation testing • recognize characteristics of testing for failure • recognize characteristics of cryptographic validation • recognize characteristics of regression testing • recognize characteristics of continuous testing • recognize characteristics of impact assessment • recognize options for addressing bugs • identify best practices in test data lifecycle management • identify best practices for securely testing software

CSSLP: SOFTWARE ACCEPTANCE, DEPLOYMENT, OPERATIONS, MAINTENANCE, AND DISPOSAL	• start the course • identify the characteristics of the pre-release testing process • list the six generic criteria for judging the suitability of a product • identify the characteristics of risk acceptance • identify characteristics of a post-release plan • recognize characteristics of validation and verification • recognize characteristics of independent testing • identify the role of bootstrapping in deployment activities • recognize characteristics of configuration management roles and plan • distinguish between the six configuration management process activities • recognize characteristics of release management activities	• recognize characteristics of monitoring during operations and maintenance • distinguish between the different activities of incident management • recognize characteristics of problem management • recognize characteristics of change management • recognize characteristics of backup, recovery, and archiving • identify the components of an effective software disposal plan • identify key activities during software disposal execution • identify best practices for software deployment, operations, maintenance, and disposal activities
CSSLP: SUPPLY CHAIN AND SOFTWARE ACQUISITION	• start the course • recognize characteristics of risk assessment for code reuse • identify best practices for creating a practical reuse plan • identify best practices for preventing intellectual property theft • recognize characteristics of legal compliance • identify best practices for supplier prequalification activities • distinguish between different security trade-offs in supplier sourcing • identify best practices for contractual integrity controls • identify best practices for vendor technical integrity controls • identify best secure control practices for managed services from a supplier • distinguish between the two rules service-level agreements or SLAs should provide • identify technical controls for software development and testing • identify code testing and verification options for software development and testing • list the eight steps to create a formal set of security testing controls	• identify software requirements verification and validation • identify chain of custody best practices • distinguish between licenses, encryption, and authentication as publishing and dissemination controls • identify characteristics of system-of-systems integration • identify software authenticity and integrity best practices during software delivery, operations, and maintenance • recognize best practices when integrating product deployment and sustainment controls • identify monitoring and incident management best practices • identify best practices for vulnerability management, tracking, and resolution activities • identify the purpose of Code Escrow during supplier transitioning • identify contracts best practices during supplier transitioning • identify best practices for assessing supplier risk, implementing supplier sourcing controls, and delivering software

Learn more at

www.hpe.com/ww/digitallearner

www.hpe.com/ww/digitallearner-contentpack

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

Follow us:

CP031 A.00, March 2019

Hewlett Packard Enterprise