301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

(ISC)²

CCSP Certification Training

This training highlights the security and policy requirements for cloud computing as well as the necessary skills for implementing cloud networks. With the growing popularity and migration to cloud computing environments, the demand for knowledgeable and experienced cloud IT professionals increases constantly.

Course Overview

Our 4-day, instructor-led CCSP (Certified Cloud Security Professional) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online is aimed at IT professionals who are involved with IT architecture, web, and cloud engineering, information security, governance, risk and compliance, or IT auditing. It covers six domains:

1. Architectural Concepts & Design Requirements
2. Cloud Data Security
3. Cloud Platform & Infrastructure Security
4. Cloud Application Security
5. Operations
6. Legal & Compliance

This course will fully prepare you for the (ISC)2® CCSP® Certification exam.
Prerequisites: Before enrolling in the course, you should have at least five years of experience in information technology, of which 3 years were in information security and one year in one or more of the six domains of the CCSP CBK.

Course Outline

Architectural Concepts and Design Requirements

- Introduction

- Cloud computing definitions
- Cloud computing roles
- Key cloud computing characteristics
- Cloud transition scenario
- Building blocks
- Cloud computing functions
- Cloud service categories
- Cloud deployment models
- Cloud cross-cutting aspects
- Network security and perimeter
- Cryptography
- IAM and access control
- Data and media sanitation
- Virtualization security
- Common threats
- Security considerations for different cloud categories
- Open web application security project top ten security threats
- Cloud secure data lifecycle
- Information and data goevrnance types
- Business continuity and disaster recovery planning
- Cost-benefit analysis
- Certification against criteria
- Systems and subsystem product certification
- Summary
- Review questions
- Notes

Cloud Data Security

- Introduction
- The cloud data lifecycle phases
- Location and access of data
- Functions, actors and controls of the data
- Cloud services, products and solutions
- Data storage
- Relevant data security technologies
- Application of security strategy technologies
- Emerging technologies
- Data discovery
- Data classification
- Data privacy acts
- Typical meanings for common privacy terms
- Privacy roles for customers and service providers

- Responsibility depending on the type of cloud services
- Implementation of data discovery
- Classification of discovered sensitive data
- Mapping and definition of controls
- Privacy level agreement
- PLA versus essential P&DP requirements activity
- Application of defined controls for PII
- Data rights management objectives
- Data protection policies
- Events
- Supporting continuous operations
- Chain of custody and non-repudiation
- Summary
- Review questions
- Notes

Cloud Platform and Infrastructure Security

- Introduction
- Network and communications in the cloud
- The compute parameters of a cloud server
- Storage issues in the cloud
- Management of cloud computing risks
- Countermeasure strategies across the cloud
- Physical and environmental protections
- Systems and communication protections
- Virtualization systems controls
- Managing identification, authentication, and authorization in the cloud infrastructure
- Risk audit mechanisms
- Understanding the cloud environment related to BCDR
- Understanding the business requirements related to BCDR
- Understanding the BCDR risks
- BCDR strategies
- Creating the BCDR plan
- Summary
- Review questions
- Notes

Cloud Application Security

- Introduction
- Determining data sensitivity and importance

- Understanding the API formats
- Common pitfalls of cloud security application deployment
- Awareness of encryption dependencies
- Understanding the software development lifecycle process
- Assessing common vulnerabilities
- Cloud-specific risks
- Threat modeling
- Identity and access management
- Federate identity management
- Multi-factor authentication
- Supplemental security devices
- Cryptography
- Tokenization
- Data masking
- Sandboxing
- Application virtualization
- Cloud-based functional data
- Cloud-secure development lifecycle
- Application security testing
- Summary
- Review questions
- Notes

Operations

- Introduction
- Modern data centers and cloud service offerings
- Factors that affect data center design
- Enterprise operations
- Secure configuration of hardware: specific requirements
- Installation and configuration of virtualization management tools for the host
- Securing the network configuration
- Identifying and understanding server threats
- Using standalone hosts
- Using clustered hosts
- Accounting for dynamic operation
- Using storage clusters
- Using maintenance mode
- Providing HA on the cloud
- The physical infrastructure for cloud environments
- Configuring access control for remote access
- Performing patch management
- Performance monitoring

- Backing up and restoring the host configuration
- Implementing network security controls: defense in depth
- Developing a management plan
- Building a logical infrastructure for cloud environments
- Running a logical infrastructure for cloud environments
- Managing the logical infrastructure for cloud environments
- Implementation of network security controls
- Using an ITSM solution
- Considerations for shadow IT
- Operations management
- Managing risk in logical and physical infrastructure
- The risk management process overview
- Understanding the collection and preservation of digital evidence
- Managing communications with relevant parties
- Wrap up: data breach example
- Summary
- Review questions
- Notes

Legal and Compliance

- Introduction
- International legislation conflicts
- Legislative concepts
- Frameworks and guidelines relevant to cloud computing
- Common legal requirements
- Legal controls and cloud service providers
- e-Discovery
- Cloud forensics and ISO/IEC 27050-1
- Protecting personal information in the cloud
- Auditing in the cloud
- Standard privacy requirements (ISO/IEC 27018)
- GAPP

  Internal ISMS
- Implementing ISMS
- Implementing policies
- Identifying and involving the relevant stakeholders
- Impact of distributed IT models
- Understanding the implication of the cloud to enterprise risk management
- Risk mitigation
- Understanding outsourcing and contract design
- Business requirements
- Vendor management

- Cloud computing certification
- Contract management
- Supply chain management
- Summary
- Review questions
- Notes

CCSP Certification Exam Information

CCSP Certification Exam Details:

- Number of Questions: 125
- Format: Multiple choice
- Passing grade: 700 out of 1000 points
- Length of test: 4 hours

CSSP Certification Training FAQs

What is the average salary for someone with their CCSP certification?

According to payscale.com, professionals with their CCSP certification earn on average $119,000 per year.

What is the CCSP certification?

The CCSP certification was created in to address challenges and issues that enterprises find themselves facing with cloud computing. We expanded on this question on our blog post, What is the CCSP Certification?

What do students say about the CCSP Certification Training course?

“Overall, highly satisfied with the facility, course, and instructor. I would say that the CCSP requires more than just a week of instruction due to breadth of material that must be covered.” *-Student from January 2019*

“Outstanding Instructor. Very knowledgeable about the subject area. I’ve learned a lot over this time period.” – *Student from July 2019*

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

This **CCSP Certification Training** course includes:

- 5 days instructor-led training
- CCSP Certification Training book
- (ISC)² CCSP practice exams
- (ISC)² CCSP official CBK
- Pre and post assessments
- CCSP onsite exam scheduling
- Certificate of completion for up to 40 CEUs/CPEs to be used toward renewing relevant certifications
- CCSP course retake guarantee
- CSSP classes can be delivered onsite for groups of 5 or more students
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

**denotes this benefit is only available at participating locations*

Cloud Security Triple Play

Take this CCSP course along with Security+ and Cloud Security to advance your cloud security career.

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Only $5,295 for all three courses!

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044