Cloud Security Specialist

Certification

Arcitura®
CERTIFIED
Cloud Security Specialist

Silver PLATYPUS

BOOKING
www.silverplatypus.com

Level 27, 101 Collins Street | Melbourne | VIC 3000
E: info@silverplatypus.com | T: + 61 3 8680 2357

Arcitura®
CERTIFIED
Cloud Security Specialist

CERTIFICATION

A Certified Cloud Security Specialist has detailed knowledge of common security threats, security controls, and associated technologies and practices related to securing cloud platforms, cloud services, and associated IT resources based on typical cloud technologies.

The Cloud Security Specialist track is comprised of CCP Modules 1, 2, 7, 8 and 9, the outlines for which are provided in the upcoming pages. Depending on the exam format chosen, attaining the Cloud Security Specialist certification can require passing a single exam or multiple exams. Upon achieving the accreditation, certification holders receive a formal digital certificate and an Acclaim/Credly digital badge with an account that supports the online verification of certification status.

For more information, visit www.arcitura.com/ccp/security

An honors designation is awarded when the exam(s) are completed with a grade that is least 10 or more percentage points higher than the standard passing grade.

Acclaim | Credly

Silver PLATYPUS

Fundamental Cloud Computing

MODULE
01

This foundational course module provides end-to-end coverage of fundamental cloud computing topics as they pertain to both technology and business considerations. The course content is divided into a series of modular sections, each of which is accompanied by one or more hands-on exercises.

The following primary topics are covered:

- Fundamental Cloud Computing Terminology and Concepts
- Basics of Virtualization
- Specific Characteristics that Define a Cloud
- Understanding Elasticity, Resiliency, On-Demand and Measured Usage
- Benefits, Challenges and Risks of Contemporary Cloud Computing Platforms and Cloud Services
- Cloud Resource Administrator and Cloud Service Owner Roles
- Cloud Service and Cloud Service Consumer Roles
- Understanding the Software as a Service (SaaS) Cloud Delivery Model
- Understanding the Platform as a Service (PaaS) Cloud Delivery Model
- Understanding the Infrastructure as a Service (IaaS) Cloud Delivery Model
- Combining Cloud Delivery Models
- Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud Deployment Models
- Business Cost Metrics and Formulas for Comparing and Calculating Cloud and On-Premise Solution Costs
- Formulas for Calculating and Rating SLA Quality of Service Characteristics

Cloud Technology Concepts

MODULE
02

This course module explores a range of the most important and relevant technology-related topics that pertain to contemporary cloud computing platforms. The course content does not get into implementation or programming details, but instead keeps coverage at a conceptual level, focusing on topics that address cloud service architecture, cloud security threats and technologies, virtualization and containerization.

Proven technologies are defined and classified as concrete architectural building blocks called “mechanisms”. The purpose of this course is to introduce cloud computing-related technology topics in a manner that is accessible to a wide range of IT professionals, as well as to empower participants with an understanding of the fundamental mechanics of a cloud platform, how the different “moving parts” can be combined, and how to address common threats and pitfalls.

The following primary topics are covered:

- Cloud Computing Mechanisms that Establish Architectural Building Blocks
- Virtual Servers, Containers, Ready-Made Environments, Failover Systems and Pay-Per-Use Monitors
- Automated Scaling Listeners, Multi-Device Brokers and Resource Replication
- Understanding How Individual Cloud Computing Mechanisms Support Cloud Characteristics
- An Introduction to Containerization, Container Hosting and Logical Pod Containers
- A Comparison of Containerization and Virtualization
- Cloud Balancing and Cloud Bursting Architectures
- Common Risks, Threats and Vulnerabilities of Cloud-based Services and Cloud-hosted Solutions
- Cloud Security Mechanisms used to Counter Threats and Attacks
- Understanding Cloud-Based Security Groups and Hardened Virtual Server Images
- Cloud Service Implementation Mediums (including Web Services and REST Services)
- Cloud Storage Benefits and Challenges, Cloud Storage Services, Technologies and Approaches
- Non-Relational (NoSQL) Storage Compared to Relational Storage
- Cloud Service Testing Considerations and Testing Types
- Service Grids and Autonomic Computing
- Cloud Computing Industry Standards Organizations

Fundamental Cloud Security

MODULE
07

This foundational course module provides a well-rounded, end-to-end presentation of essential techniques, mechanisms, patterns and industry technologies for establishing cloud-based security controls and security architectures. The cloud security fundamentals covered in Module 2 are continued by introducing threat categorizations and new cloud security mechanisms.

The course then delves into a series of cloud security mechanisms and associated architectural patterns that explore a variety of topics, including cloud network security, identity and access management, and trust assurance.

The following primary topics are covered:

- Cloud Security Basics
- Common Cloud Security Mechanisms
- Cloud Security Threats
- Cloud Security Threat Categorization Methodology
- Identification and Treatment of Common Threats
- Cloud Network Security Patterns and Supporting Mechanisms
- Securing Network Connections and Cloud Authentication Gateways
- Collaborative Monitoring and Logging
- Independent Cloud Auditing
- Cloud Identity and Access Management Patterns and Supporting Mechanisms
- Federating and Enabling Secure Interoperability among Cloud Consumers
- Trust Assurance Patterns and Supporting Mechanisms
- Trust Attestation and Establishing Trustworthiness

Advanced Cloud Security

MODULE
08

This advanced course module covers cloud security mechanisms and architectural design patterns that address data and access control security for virtual machines, as well as trust boundaries, geotagging and BIOS security.

The course also explains common methods used by attackers to breach organizational resources and provides a methodology for countering such attacks. The course concludes by demonstrating the relationship between threats, attacks, and risks via threat modeling.

The following primary topics are covered:

- Cloud Service Security Patterns and Supporting Mechanisms
- Virtual Machine Platform Protection Patterns
- Considerations for Setting Up Secure Ephemeral Perimeters
- Trusted Cloud Resource Pools and Cloud Resource Access Control
- Permanent Data Access Loss Protection
- Cloud Data Breach Protection
- Isolated Trust Boundaries
- The Attack Lifecycle and the Security Lifecycle
- Proactive Mitigation vs. Incidence Response
- Threats, Vulnerabilities, Impacts from Exploitation
- Threat Modeling, Threats and Mitigations

Cloud Security Lab

MODULE
09

This course module presents participants with a series of exercises and problems that are designed to test their ability to apply their knowledge of topics covered previously in course modules 7 and 8. Completing this lab will help highlight areas that require further attention and will further prove hands-on proficiency in cloud computing security practices, mechanisms and architectural patterns as they are applied and combined to solve real-world problems.

As a hands-on lab, this course provides a set of detailed exercises that require participants to solve a number of inter-related problems, with the ultimate goal of evaluating, designing and correcting cloud security technology architectures to fulfill specific sets of solution and business automation requirements.

The Certified Cloud Trainer works closely with participants to ensure that all exercises are carried out completely and accurately. Attendees can voluntarily have exercises reviewed as part of the class completion.

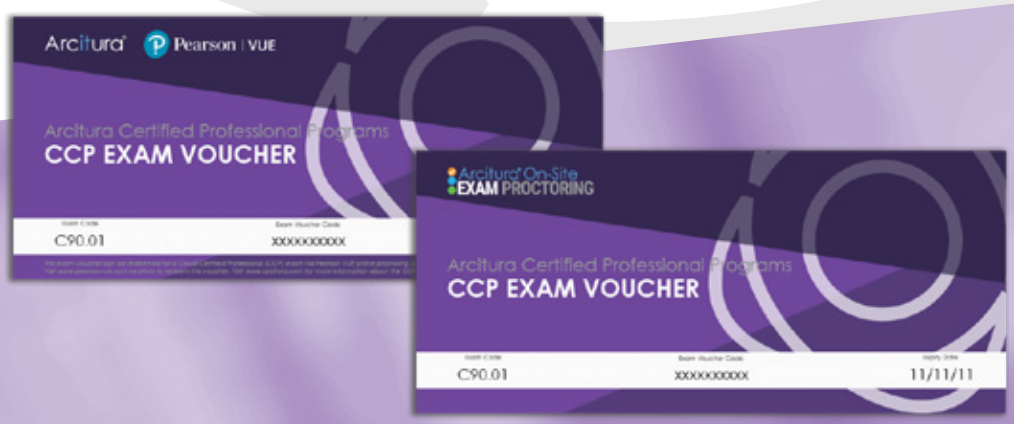
EXAMS

You can take exams anywhere in the world via Pearson VUE testing centers, Pearson VUE online proctoring and Arcitura on-site exam proctoring at your location.

For each certification, candidates have three flexible exam format options:

- Complete one module-specific exam for each course module in Cloud Security Specialist certification track. This is recommended for those who want to progress gradually through the track and who would like to be assessed after each course module before proceeding to the next.
- Complete a single combined exam for the entire Cloud Security Specialist certification track. Recommended for those who want to only take a single exam that encompasses all course modules within this track.
- Complete a partial exam. Recommended for those who have already obtained a CCP certification and would like to achieve the Cloud Security Specialist certification without having to be retested on CCP Modules 1 and 2.

Visit www.arcitura.com/exams for more information. (Note that not all exam formats may be available via all exam delivery options.)



Pearson | VUE | Arcitura On-Site EXAM PROCTORING

Silver PLATYPUS