CCP Module 7: Fundamental Cloud Security

This foundational course provides a well-rounded, end-to-end presentation of essential techniques, 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 patterns that explore a variety of topics, including cloud network security, identity and access management, and trust assurance.

The following topics are covered:

- Cloud Security Threats and 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

Duration: 1 Day

For more information, visit www.cloudschool.com.

Cloud Computing Design Patterns Text Book

This CCP course module covers a range of in-depth topics that are described in the course booklet and further elaborated by detailed technical coverage and case study examples in the accompanying Cloud Computing Design Patterns text book from the acclaimed Prentice Hall Service Technology Series from Thomas Erl.

Self-Study Kit

The materials for this course module can be purchased separately as part of the Module 7 Self-Study Kit, which includes additional materials and study aids. These materials are designed to prepare you for Exam C90.07 and are also suitable for general remote, self-paced study purposes.

For ordering information, visit www.cloudselfstudy.com.