



# CCSP® CERTIFIED CLOUD SECURITY PROFESSIONAL

**DURATION: 5 DAYS**



**CYBER  
SECURITY**

Attackers never rest, and along with all the traditional threats targeting internal networks and systems, an entirely new variety specifically targeting the cloud has emerged. As more organisations adopt cloud-based systems, new complexities and challenges surface and the risks increase. Organisations need cloud security professionals with the requisite knowledge, skills and abilities to be able to audit, assess and secure cloud infrastructures.

## WHO SHOULD ATTEND

**This course is designed for:**

- Enterprise architects, Security architects, Systems architects
- Security administrators, Security consultants. Security managers
- Systems engineers, Security engineers

## LEARNING OUTCOMES

- Identify and explain the Cloud Computing concepts and definitions based on the ISO/IEC 17788 and NIST standards.
- Identify and explain the Cloud Security Alliance's Treacherous 12.
- Understand and be able to differentiate between the various service delivery models, frameworks and hypervisor threats that are incorporated into the cloud computing reference architecture.
- Demonstrate the application of appropriate security strategies and be able to recommend appropriate controls for protecting data at rest and data in motion.
- Discuss strategies for data ownership, data sovereignty, data classification and implementing appropriate measures for assurance for ensuring privacy, compliance with regulatory agencies and working with authorities during legal investigations.
- Understand the challenges for data centre design, forensic analysis and cloud environment deployments and recommend appropriate risk mitigation strategies.
- Understand and apply Business Continuity Planning and Disaster Recovery procedures for disaster situations.
- Design appropriate identity and access management solutions.
- Comprehend and apply appropriate processes and frameworks including the Software Development Life-Cycle (SDLC) process, ITIL and ISO/IEC 20000

**GET AHEAD OF THE GAME  
GET CERTIFIED**

1300 767 592  
customerservice@alc-group.com  
alctraining.com.au

ALC.Training

@alcgroup

alc-training

## COURSE CONTENTS

### 1. CLOUD CONCEPTS, ARCHITECTURE & DESIGN

- Understand cloud computing concepts
- Describe cloud reference architecture
- Understand security concepts relevant to cloud computing
- Understand design principles of secure cloud computing
- Evaluate cloud service providers

### 2. CLOUD DATA SECURITY

- Describe cloud data concepts
- Design and implement cloud data storage architectures
- Design and apply data security technologies and strategies
- Implement data discovery
- Implement data classification
- Design and implement Information Rights Management (IRM)
- Plan and implement data retention, deletion and archiving policies
- Design and implement auditability, traceability and accountability of data events

### 3. CLOUD PLATFORM & INFRASTRUCTURE SECURITY

- Comprehend cloud infrastructure and platform components
- Design a secure data centre
- Analyse risks associated with cloud infrastructure
- Design and plan of security controls
- Plan Disaster Recovery (DR) and Business Continuity (BC)

### 4. CLOUD APPLICATION SECURITY

- Advocate training and awareness for app security
- Describe & Apply the Secure Software Development Life Cycle (SDLC) process
- Apply cloud software assurance and validation
- Use verified secure software
- Comprehend the specifics of cloud application architecture
- Design appropriate Identity and Access Management (IAM) solutions

### 5. CLOUD SECURITY OPERATIONS

- Build and implement physical and logical infrastructure for cloud environment
- Operate and maintain physical and logical infrastructure for cloud environment
- Implement operational controls and standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 20000-1)
- Support digital forensics
- Manage communication with relevant parties & ops

### 6. LEGAL & COMPLIANCE

- Articulate legal requirements and unique risks within the cloud environment
- Understand privacy issues
- Understand audit process, methodologies, and required adaptations for a cloud environment
- Understand implications of cloud to enterprise risk management
- Understand outsourcing and cloud contract designVendor management