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. INTRO & COURSE OVERVIEW
2. ARCHITECTURAL CONCEPTS & DESIGN REQUIREMENTS
   - Important cloud computing concepts
   - Cloud reference architecture
   - Security concepts relevant to cloud computing
   - Security design principles of cloud computing
   - Trusted cloud services
3. CLOUD DATA SECURITY
   - The cloud data lifecycle
   - Design and implementation of cloud data storage architectures
   - Design and application of data security strategies
   - Implementation of data discovery and classification technologies
   - Implementation of data protection for personally identifiable information (PII)
   - Design and implementation of Data Rights Management
   - Design and implementation of data retention,deletion and archiving policies
   - Auditability, traceability and accountability of data events
4. CLOUD PLATFORM & INFRASTRUCTURE SECURITY
   - Comprehend cloud infrastructure components
   - Analyse risks associated to cloud infrastructure
   - Design and plan security controls
   - Plan disaster recovery and business continuity management
5. CLOUD APPLICATION SECURITY
   - Training and awareness for application security
   - Cloud software assurance and validation
   - Use of verified secure software
   - Understand and apply the Software Development Life-Cycle (SDLC) process
   - Comprehend the specifics of Cloud
   - Application Architecture
   - Design appropriate Identity and Access Management (IAM) solutions
6. OPERATIONS
   - Support the planning process for the data centre design
   - Build, run and manage physical infrastructure for cloud environment
   - Build, run and manage logical infrastructure for cloud environment
   - Ensure compliance with various regulations and control requirements
   - Conduct risk assessments for logical and physical infrastructure
   - Collection, acquisition and preservation of digital evidence
   - Manage communication with relevant parties
7. LEGAL & COMPLIANCE
   - Legal requirements and unique risks within the cloud environment
   - Privacy issues, including jurisdictional variation
   - The audit process and methodologies adapted for the cloud environment
   - Implications of cloud to enterprise risk management
   - Outsourcing and cloud contract design
   - Vendor management