CLS | Learning Solutions

Why Learn Certified Cloud Security Professional CCSP?

The Industry's Premier Cloud Security Certification.

Earning the globally recognized CCSP cloud security certification is a proven way to build your career and better secure critical assets in the cloud.

Audience Profile :

- Security Consultants
- Security Engineers
- Cloud Infrastructure Architects
- Cloud Computing Professionals
- Security Managers
- System Architects
- Enterprise Architects
- Security Administrators
- Security Architects
- System Engineers

Prerequisites:

- A minimum 5 years of work experience in information technology .
- Earning a CISSP certification from ISC2 can be used as a substitute for the CCSP prerequisite/experience requirement .
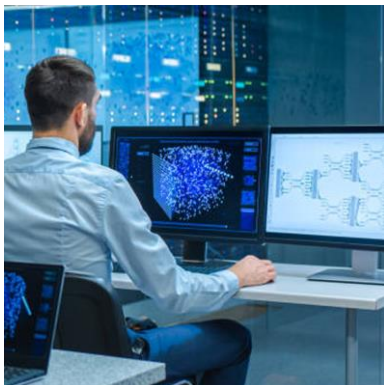
Course Overview:

- Certified Cloud Security Professional CCSP certification validates the advanced technical skills needed to design, manage, and secure data, applications, and infrastructure in the cloud.
- The CCSP shows you have the advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity experts at (ISC)².
- CCSP empowers individuals and organizations with the highest level of mastery in cloud security.
- In This Certified Cloud Security Professional CCSP Training Course you'll gain the technical knowledge and skills you need to expertly design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity authorities at (ISC)².

Certified Cloud Security Professional CCSP Outline:

- Domain 1: Cloud Concepts, Architecture and 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
- Domain 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
- Domain 3: Cloud Platform and Infrastructure Security
- Comprehend cloud infrastructure components
- Design a secure data center
- Analyze risks associated with cloud infrastructure
- Design and plan security controls
- Plan Disaster Recovery (DR) and Business Continuity (BC)
- Domain 4: Cloud Application Security
- Advocate training and awareness for application security
- Describe the Secure Software Development Life Cycle (SDLC) process
- Apply the Secure Software Development Life Cycle (SDLC)
- 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
- Domain 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
- Manage security operations
- Domain 6: Legal, Risk and 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 design

CLS | Learning Solutions

Training businesses and people Since 1995