MERCURY

Certified Cloud Security Professional (CCSP)

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Certified Cloud Security Professional (CCSP)

Introduction:

The Certified Cloud Security Professional CCSP certification is a globally recognized credential designed for IT and security professionals seeking to demonstrate their expertise in cloud security. As organizations increasingly migrate their operations to cloud environments, the need for specialized knowledge in cloud security has never been more critical. The CCSP certification validates an individual's ability to implement and manage cloud security architectures, ensuring compliance with regulatory frameworks while protecting sensitive data.

This Certified Cloud Security Professional CCSP course provides a comprehensive overview of the CCSP domains, including cloud architecture, governance, risk management, compliance, and security operations. Participants will learn to assess cloud security risks, develop effective security strategies, and implement best practices tailored to cloud environments. By the end of the course, attendees will be well-prepared to take the CCSP exam and advance their careers in the rapidly evolving field of cloud security.

Targeted Groups:

- IT security professionals.
- Cloud architects.
- Security compliance officers.
- Risk management professionals.
- System administrators.
- Cloud service providers.
- Information security managers.
- Network security engineers.
- Chief Information Security Officers CISOs.
- DevOps professionals.
- Security consultants.
- Data protection officers.
- IT Auditors.
- Compliance analysts.

Course Objectives:

At the end of this course, the participants will be able to:

- Understand cloud computing concepts and service models.
- Gain knowledge of cloud security architecture and design principles.
- Learn to assess and manage cloud security risks effectively.
- Develop skills to ensure compliance with relevant regulations and standards.
- Implement identity and access management controls in cloud environments.
- Master data security practices specific to cloud computing.
- Acquire techniques for incident response and recovery in cloud settings.
- Explore security governance frameworks applicable to cloud services.
- Enhance capabilities in monitoring and detecting security threats in the cloud.
- Understand vendor risk management strategies for cloud service providers.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Targeted Competencies:

- Cloud security architecture design.
- Risk assessment and management.
- Compliance and regulatory requirements.
- Data security and privacy management.
- Identity and access management.
- Incident response and recovery.
- Security governance and policy development.
- Secure software development lifecycle.
- Cloud infrastructure and operations security.
- Security monitoring and threat detection.
- Vendor risk management.
- Cloud service models and deployment strategies.

Course Content:

Unit 1: Cloud Concepts and Architecture:

- Define cloud computing and its service models IaaS, PaaS, SaaS.
- Understand the characteristics and benefits of cloud environments.
- Identify different deployment models public, private, hybrid, community.
- Explore cloud computing frameworks and standards.
- Discuss cloud service provider roles and responsibilities.
- Analyze the shared responsibility model in cloud security.

Unit 2: Cloud Data Security:

- Learn data classification and its importance in cloud security.
- Understand data encryption methods for cloud storage.
- Explore data loss prevention strategies.
- Implement access controls for sensitive data.
- Discuss data lifecycle management in the cloud.
- Examine the challenges of data residency and sovereignty.

Unit 3: Cloud Platform and Infrastructure Security:

- Assess security requirements for cloud infrastructures.
- Understand secure network architecture in cloud environments.
- Learn about secure configurations and hardening techniques.
- Implement virtualization security measures.
- Explore container security best practices.
- Discuss the importance of monitoring and logging in cloud infrastructure.

Unit 4: Cloud Application Security:

- Understand the security challenges associated with cloud applications.
- Learn secure coding practices for cloud development.
- Discuss application security testing methodologies.
- Implement identity and access management controls for applications.
- Explore API security measures for cloud services.
- Understand the implications of third-party integrations.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

Unit 5: Compliance and Security Operations:

- Learn about regulatory frameworks relevant to cloud security GDPR, HIPAA, etc..
- Understand the importance of compliance in cloud environments.
- Discuss the role of security policies and procedures.
- Explore incident response planning and execution in the cloud.
- Implement security monitoring and threat detection tools.
- Assess vendor risk management strategies in cloud procurement.