Cloud Security Professional (CCSP) Training Course



19 - 23 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CYB6640_88303

Course Introduction / Overview:

This intensive training course is designed to provide a comprehensive and deep understanding of cloud security principles and practices. In an era where cloud adoption is accelerating, securing data, applications, and infrastructure in the cloud has become a paramount concern for organizations worldwide. This program covers the six core domains of the Certified Cloud Security Professional (CCSP) body of knowledge, ensuring participants gain the expertise needed to design, manage, and secure cloud environments effectively. Drawing on foundational concepts from experts like Ronald L. Krutz, author of "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", the curriculum balances theoretical knowledge with practical application. Participants will explore everything from cloud architecture and design to data security, platform protection, secure operations, and legal compliance. BIG BEN Training Center has meticulously structured this course to empower professionals with the advanced skills required to address complex cloud security challenges, making them invaluable assets in the modern digital landscape. This course is the definitive step for professionals aiming to master cloud security and validate their expertise in this critical field.

Target Audience / This training course is suitable for:

- Enterprise Architects.
- Security Administrators.
- Systems Engineers.
- Security Architects.
- Security Consultants.
- Security Engineers.
- Security Managers.
- System Architects.
- Information Technology Directors.
- Cloud Security Professionals.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Information Technology and Telecommunications.
- Retail and E-commerce.
- Governmental and Public Sector Agencies.
- Consulting and Professional Services.
- Energy and Utilities.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT).
- Information Security (InfoSec).
- Cybersecurity Operations.
- Risk Management and Compliance.
- Internal Audit and Governance.
- Cloud Engineering and Architecture.
- Legal and Regulatory Affairs.
- Software Development and DevOps.

Course Offerings:

By the end of this course, the participants will have able to:

- Articulate cloud computing concepts and reference architectures.
- Design and implement secure cloud architectures.
- Manage and secure the entire cloud data lifecycle.
- Implement robust data encryption and key management strategies.
- Secure cloud infrastructure components, including networks and storage.
- Conduct comprehensive risk assessments for cloud platforms.
- Integrate security into the cloud application development lifecycle.
- Manage identity and access control for cloud services effectively.
- Oversee security operations and incident response in the cloud.
- Navigate complex legal, risk, and compliance issues in the cloud.
- Develop and implement business continuity and disaster recovery plans for cloud environments.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly effective. This course moves beyond traditional lecture-based learning by integrating a dynamic blend of expert-led instruction, real-world case study analysis, and collaborative group discussions. Participants will engage in practical exercises that simulate genuine cloud security challenges, allowing them to apply theoretical concepts in a controlled, hands-on environment. Our approach emphasizes peer-to-peer learning, where professionals from diverse backgrounds can share insights and strategies. Interactive sessions, Q&A panels, and problem-solving workshops are central to the learning experience, ensuring that every participant is actively involved. The instructor will provide continuous feedback and facilitate discussions that connect course material to the specific challenges and objectives of the attendees. This comprehensive and engaging methodology ensures that participants not only grasp the technical details of cloud security but also develop the critical thinking and strategic skills needed to excel in their roles.

Course Agenda (Course Units):

Unit One: Cloud Concepts, Architecture, and Design Principles

- Understand the fundamentals of cloud computing and its service models (IaaS, PaaS, SaaS).
- Explore cloud reference architecture and key security principles.
- Analyze the security implications of different cloud deployment models.
- Learn to design secure cloud architectures from the ground up.
- Evaluate cloud service providers based on security criteria.
- Understand the principles of secure network design in the cloud.
- Apply the concept of shared responsibility in security.

Unit Two: Securing Cloud Data and Information

- Master the cloud data lifecycle from creation to disposal.
- Design and implement secure cloud storage architectures.
- Apply advanced data encryption and key management techniques.
- Implement Data Loss Prevention (DLP) and data discovery strategies.
- Understand and manage data sovereignty and localization requirements.
- Implement robust Identity and Access Management (IAM) for data.
- Explore emerging technologies for data protection in the cloud.

Unit Three: Protecting Cloud Platform and Infrastructure

- Secure the physical and virtual components of cloud infrastructure.
- Conduct comprehensive risk assessments of the cloud environment.
- Implement security controls for compute, network, and storage resources.
- Manage changes and configurations securely in the cloud.
- Develop a robust business continuity and disaster recovery plan.
- Understand the security challenges of virtualization and containerization.
- Implement logging, monitoring, and auditing for infrastructure security.

Unit Four: Cloud Application Security and Secure Operations

- Integrate security into the Software Development Lifecycle (SDLC).
- Apply secure coding practices for cloud-native applications.
- Manage identity, authentication, and authorization for cloud applications.
- Implement threat modeling and vulnerability assessments for applications.
- Understand the principles of DevSecOps in a cloud context.
- Manage security operations and incident response procedures.
- Utilize automation to enhance security monitoring and enforcement.

Unit Five: Legal Frameworks, Risk Management, and Compliance

- Navigate the legal and regulatory landscape of cloud computing.
- Understand privacy issues and data protection regulations like GDPR.
- Conduct audits and ensure compliance with industry standards (e.g., ISO 27001).
- Apply a structured risk management framework to the cloud.
- Manage vendor relationships and third-party risk.
- Understand the process of eDiscovery and digital forensics in the cloud.
- Address ethical considerations in cloud security practices.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As cloud environments become increasingly complex and federated, how can organizations balance the need for agile innovation with the stringent requirements of zero-trust security architecture?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself through its holistic and strategic approach to cloud security education. Unlike programs that focus narrowly on specific vendor platforms or tools, this course is built upon the universally recognized CCSP framework, providing a vendor-neutral and comprehensive understanding of cloud security principles. Our curriculum emphasizes the "why" behind the "how," empowering participants with the critical thinking skills needed to design and implement security solutions that are both effective and resilient, regardless of the underlying technology. The course content is meticulously curated to blend foundational theory with practical, real-world scenarios, moving beyond rote memorization to foster true mastery. We focus on developing a strategic mindset, enabling professionals to not just respond to threats but to proactively architect secure, compliant, and efficient cloud ecosystems. The interactive methodology, combined with expert instruction, ensures that participants leave with a deep, applicable knowledge base that directly translates into enhanced capability and value for their organizations.