

KOENIG SOLUTIONS • COURSE OUTLINE

Certified Cloud Security Professional (CCSP)

Learn to secure cloud environments across architecture, data, infrastructure, applications, operations, and legal compliance domains.

5 Days

40 HOURS

6

MODULES

41

TOPICS

COURSE OVERVIEW

The Certified Cloud Security Professional (CCSP) course is a globally recognized certification program designed for IT and security professionals to validate their expertise in cloud security. It encompasses a comprehensive curriculum that addresses the best practices and standards for securing cloud environments. Through lessons on cloud computing concepts, Cloud reference architecture, and Security principles, learners gain a deep understanding of the architectural concepts and design requirements of cloud systems. The course also delves into Cloud data security, teaching students about Data lifecycle management, protection strategies, and compliance with data protection laws for sensitive information like PII. Further, it covers cloud platform & infrastructure security, emphasizing the importance of disaster recovery and risk management. In Cloud application security, participants learn about Secure software development life-cycle and IAM solutions. The operations module prepares learners to manage cloud infrastructure, ensure Regulatory compliance, and handle digital evidence. Lastly, the legal & compliance section provides insights into legal risks, privacy issues, and Vendor management in the cloud. This comprehensive course equips professionals with the necessary skills to safeguard cloud environments effectively.

WHO THIS COURSE IS FOR

The Certified Cloud Security Professional (CCSP) course is designed for IT professionals seeking specialized skills in cloud security. Job roles and audience for the course:

IT Security Professionals

Cloud Security Architects

Cybersecurity Analysts

Cloud Engineers

IT Auditors

Security Consultants

Network Architects

System Engineers

Security Architects

Enterprise Architects

Risk Compliance Managers

Chief Information Security Officers (CISO)

Data Privacy Officers

Cloud Consultants

IT Directors/Managers

What You Will Learn

- Explain cloud computing concepts and reference architecture
- Apply design principles of secure cloud computing
- Design data security strategies across the cloud data lifecycle
- Implement jurisdictional data protections for PII
- Analyse risks associated with cloud infrastructure
- Plan disaster recovery and business continuity management
- Apply the secure software development life-cycle
- Design IAM solutions for cloud applications

COURSE SYLLABUS

6 Modules, 41 Topics

01

Architectural Concepts & Design Requirements

Cloud computing concepts & definitions based on the ISO/IEC 17788 standard; security concepts and principles relevant to secure cloud computing.

TOPICS

- Understand Cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
- Identify Trusted Cloud Services

02

Cloud Data Security

Concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability in cloud environments.

TOPICS

- Understand Cloud Data Lifecycle
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Strategies
- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)
- Design and Implement Data Rights Management
- Plan and Implement Data Retention, Deletion, and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

03

Cloud Platform & Infrastructure Security

Knowledge of the cloud infrastructure components, both the physical and virtual, existing threats, and mitigating and developing plans to deal with those threats.

TOPICS

- Comprehend Cloud Infrastructure Components
- Analyze Risks Associated to Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery and Business Continuity Management

04

Cloud Application Security

Processes involved with cloud software assurance and validation; and the use of verified secure software.

TOPICS

- Recognize the need for Training and Awareness in Application Security
- Understand Cloud Software Assurance and Validation
- Use Verified Secure Software
- Comprehend the Software Development Life-Cycle (SDLC) Process
- Apply the Secure Software Development Life-Cycle
- Comprehend the Specifics of Cloud Application Architecture
- Design Appropriate Identity and Access Management (IAM) Solutions

05

Operations

Identifying critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it; requirements of cloud architecture to running and managing that infrastructure; definition of controls over hardware, media, and the operators with access privileges as well as the auditing and monitoring are the mechanisms, tools and facilities.

TOPICS

- Support the Planning Process for the Data Center Design
- Implement and Build Physical Infrastructure for Cloud Environment
- Run Physical Infrastructure for Cloud Environment
- Manage Physical Infrastructure for Cloud Environment
- Build Logical Infrastructure for Cloud Environment
- Run Logical Infrastructure for Cloud Environment
- Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls (e.g., ITIL, ISO/IEC 20000-1)
- Conduct Risk Assessment to Logical and Physical Infrastructure
- Understand the Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

06

Legal & Compliance

Addresses ethical behavior and compliance with regulatory frameworks. Includes investigative measures and techniques, gathering evidence (e.g., Legal Controls, eDiscovery, and Forensics); privacy issues and audit process and methodologies; implications of cloud environments in relation to enterprise risk management.

TOPICS

- Understand Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues, Including Jurisdictional Variation
- Understand Audit Process, Methodologies, and Required Adaption's for a Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design
- Execute Vendor Management

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com