INFOSECTRAIN

cloud security alliance℠

CCSK v5

CERTIFICATE OF CLOUD SECURITY KNOWLEDGE

TRAINING & CERTIFICATION

INFOSECTRAIN

Program Highlights

The CCSK v5 Certification Training covers cloud computing concepts, governance strategies, risk management, and audit processes. This latest version of the CCSK program includes identity and access management, security monitoring, infrastructure and network security, and cloud workload security. Participants will also learn data, application security strategies, and incident response best practices. The CCSK Orb chatbot supports this program, combining theoretical knowledge with practical insights for continuous learning and assistance.

INFOSECTRAIN

Course Highlights

- **30-Hour LIVE** Instructor-led Training
- Learn from Industry Experts
- Highly Interactive and Dynamic Sessions
- CSA Authorized Training Partner
- Learn with Real-World Scenarios
- Access to Recorded Sessions
- Extended Post Training Support
- Career Guidance and Mentorship
- Immersive Learning

Target Audience

IT Professionals	Developers	IT Operations	Audit Compliance/ Managers

Pre-Requisites

No official experience is required; however, it is highly recommended to have a basic understanding of security fundamentals, including firewalls, secure development, encryption, and identity and access management.

INFOSECTRAIN

Exam Information

Certification Body	**Certificate of Cloud Security Knowledge (CCSK v5)**
Exam Format	Multiple-choice questions
Number of Questions	60
Exam Duration	120 minutes
Passing Score	80%
Open/Close Book Exam	Open Book Exam
Language	English, Spanish, and Japanese

INFOSECTRAIN

Course Objectives

- Define cloud computing, set baseline terminology, and detail controls, deployment, and architectural models.
- Focus on cloud security, risk management, audit processes, and compliance.
- Evaluate service providers and establish risk registries.
- Manage and secure the entire cloud footprint, including service provider deployments.
- Understand and manage IAM between organizations, cloud providers, and services.
- Address monitoring challenges, integrate advanced tools, and manage cloud telemetry and logs.
- Secure software and data units deployable on various infrastructures or platforms.
- Apply strategies, tools, and practices to protect data in transit and at rest.
- Develop best practices for incident response and resilience in cloud environments.
- Understand and apply Zero Trust and AI in strategic cybersecurity approaches.

How many questions are pulled for each domain?

Domains	Domains Name	No. of Questions
1	Cloud Computing Concepts & Architectures	5
2	Cloud Governance	5
3	Risk, Audit & Compliance	5
4	Organization Management	5
5	Identity & Access Management	4
6	Security Monitoring	4
7	Infrastructure & Networking	6
8	Cloud Workload Security	7
9	Data Security	5
10	Application Security	6
11	Incident Response & Resilience	5
12	Related Technologies & Strategies	3

INFOSECTRAIN

Learning Outcome

Domain 1: Cloud Computing Concepts & Architectures

- Introduction
- Learning Objectives
- 1.1 Defining Cloud Computing
  - 1.1.1 Abstraction & Orchestration
- 1.2 Cloud Computing Models
  - 1.2.1 Essential Characteristics
  - 1.2.2 Cloud Service Models
    - 1.2.2.1 Infrastructure as a Service (IaaS)
    - 1.2.2.2 Platform as a Service (PaaS)
    - 1.2.2.3 Software as a Service (SaaS)
  - 1.2.3 Cloud Deployment Models
  - 1.2.4 CSA Enterprise Architecture Model
- 1.3 Cloud Security Scope, Responsibilities, & Models
  - 1.3.1 Shared Security Responsibility Mode

Domain 2: Cloud Governance

- Introduction
- Learning Objectives
- 2.1. Cloud Governance
- 2.2 The Governance Hierarchy
  - 2.2.1 Cloud Security Frameworks
  - 2.2.2 Policies

INFOSECTRAIN

Domain 3: Risk, Audit, & Compliance

- Introduction
- Learning Objectives
- 3.1. Cloud Risk Management
  - 3.1.1 Cloud Risks
  - 3.1.2 Understanding Cloud Risk Management
  - 3.1.3 Assessing Cloud Services
  - 3.1.4 The Cloud Register
- 3.2 Compliance & Audit
  - 3.2.1 Jurisdictions
  - 3.2.2 Cloud-Relevant Laws & Regulations Examples
  - 3.2.3 Compliance Inheritance
  - 3.2.4 Artifacts of Compliance
- 3.3 Governance, Risk, Compliance Tools & Technologies

INFOSECTRAIN

Domain 4: Organization Management

- Introduction
- Learning Objectives
- 4.1 Organization Hierarchy Models
  - 4.1.1 Definitions
  - 4.1.2 Organization Capabilities Within a Cloud Service Provider
  - 4.1.3 Building a Hierarchy Within a Provider
- 4.2 Managing Organization-Level Security Within a Provider
  - 4.2.1 Identity Provider & User/Group/Role Mappings
  - 4.2.2 Common Organization Shared Services
- 4.3 Considerations for Hybrid & Multi-Cloud Deployments
  - 4.3.1 Organization Management for Hybrid Cloud Security
  - 4.3.2 Organization Management for Multi-Cloud Security
  - 4.3.3 Organization Management for SaaS Hybrid & Multi-Cloud

INFOSECTRAIN

Domain 5: Identity & Access Management

- Introduction
- Learning Objectives
- 5.1 Fundamental Terms
- 5.2 Federation
  - 5.2.1 Common Federation Standards
  - 5.2.2 How Federated Identity Management Works
  - 5.2.3 Managing Users & Identities for Cloud Computing
- 5.3 Strong Authentication & Authorization
  - 5.3.1 Authentication & Credentials
  - 5.3.2 Entitlement & Access Management
  - 5.3.3 Privileged User Management

INFOSECTRAIN

Domain 6: Security Monitoring

- Introduction
- Learning Objectives
- 6.1 Cloud Monitoring
  - 6.1.1 Logs & Events
- 6.2 Beyond Logs - Posture Management
- 6.3 Cloud Telemetry Sources
  - 6.2.1 Management Plane Logs
  - 6.2.2 Service & Application Logs
  - 6.2.3 Resource Logs
  - 6.2.4 Cloud Native Tools
- 6.4 Collection Architectures
  - 6.4.1 Log Storage & Retention
  - 6.4.2 Cascading Log Architecture
- 6.5 AI for Security Monitoring

INFOSECTRAIN

Domain 7: Infrastructure & Networking

- Introduction
- Learning Objectives
- 7.1 Cloud Infrastructure Security
  - 7.1.1 Foundational Infrastructure Security Techniques
  - 7.1.2 CSP Infrastructure Security Responsibilities
  - 7.1.3 Infrastructure Resilience
- 7.2 Cloud Network Fundamentals
  - 7.2.1 Cloud Networks are Software-Defined Networks
  - 7.2.2 Cloud Connectivity
- 7.3 Cloud Network Security & Secure Architecture
  - 7.3.1 Preventative Security Measures
  - 7.3.2 Detective Security Measures
- 7.4 Infrastructure as Code (IaC)
- 7.5 Zero Trust for Cloud Infrastructure & Networks
  - 7.5.1 Software-Defined Perimeter & ZT Network Access
- 7.6 Secure Access Service Edge (SASE)

INFOSECTRAIN

Domain 8: Cloud Workload Security

- Introduction
- Learning Objectives
- 8.1 Introduction to Cloud Workload Security
  - 8.1.1 Types of Cloud Workloads
  - 8.1.2 Impact on Workload Security Controls
- 8.2 Securing Virtual Machines
  - 8.2.1 Virtual Machine Challenges & Mitigations
  - 8.2.2 Creating Secure VM Images with Factories
  - 8.2.3 Snapshots & Public Exposures/Exfiltration
- 8.3 Securing Containers
  - 8.3.1 Container Image Creation
  - 8.3.2 Container Networking
  - 8.3.3 Container Orchestration & Management Systems
  - 8.3.4 Container Orchestration Security
  - 8.3.5 Runtime Protection for Containers
- 8.4 Securing Serverless and Function as a Service
  - 8.4.1 FaaS Security Issues
  - 8.4.2 IAM for Serverless
  - 8.4.3 Environment Variables & Secrets
- 8.5 Securing AI Workloads
  - 8.5.1 AI-System Threats
  - 8.5.2 AI Risk Mitigation and Shared Responsibilities

INFOSECTRAIN

Domain 9: Data Security

- Introduction
- Learning Objectives
- 9.1 Primer on Cloud Storage
  - 9.1.1 Volume/Block Storage
  - 9.1.2 Object Storage
  - 9.1.3 Database Storage
  - 9.1.4 Other Types of Storage
- 9.2 Data Security Tools and Techniques
  - 9.2.1 Data Classification
  - 9.2.2 Identity and Access Management
  - 9.2.3 Access Policies
  - 9.2.4 Encryption and Key Management
  - 9.2.5 Data Loss Prevention
- 9.3 Cloud Data Encryption at Rest
  - 9.3.1 Cloud Data Key Management Strategies
  - 9.3.2 Data Encryption Recommendations
- 9.4 Data Security Posture Management
- 9.5 Object Storage Security
- 9.6 Data Security for Artificial Intelligence
  - 9.6.1 AI as a Service

INFOSECTRAIN

Domain 10: Application Security

- Introduction
- Learning Objectives
- 10.1 Secure Development Lifecycle
  - 10.1.1 SDLC Stages
  - 10.1.2 Threat Modeling
  - 10.1.3 Testing: Pre-Deployment
  - 10.1.4 Testing: Post Deployment
- 10.2 Architecture's Role in Secure Cloud Applications
  - 10.2.1 Cloud Impacts on Architecture-Level Security
  - 10.2.2 Architectural Resilience
- 10.3 Identity & Access Management and Application Security
  - 10.3.1 Secrets Management
- 10.4 Dev Ops & DevSecOps

INFOSECTRAIN

Domain 11: Incident Response & Resilience

- Introduction
- Learning Objectives
- 11.1 Incident Response
  - 11.1.1 Incident Response Lifecycle
- 11.2 Preparation
  - 11.2.1 Incident Response Preparation & Cloud Service Providers
  - 11.2.2 Training for Cloud Incident Responders
- 11.3 Detection & Analysis
  - 11.3.1 Cloud Impact on Incident Response Analysis
  - 11.3.2 Cloud System Forensics
- 11.4 Containment, Eradication, & Recovery
  - 11.4.1 Containment
  - 11.4.2 Eradication
  - 11.4.3 Recovery
- 11.5 Post Incident Analysis

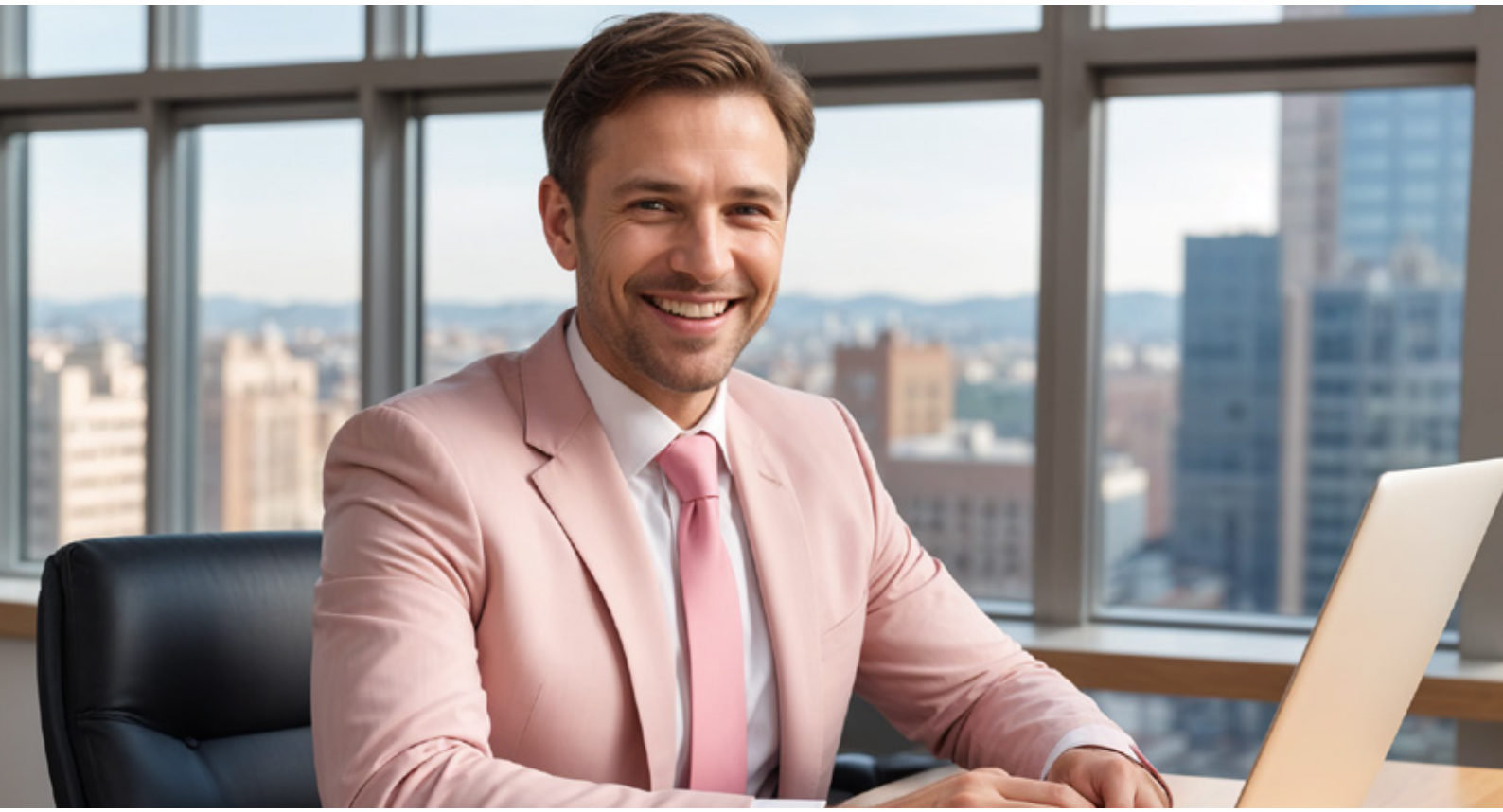
INFOSECTRAIN

Domain 12: Related Technologies & Strategies

- Introduction
- Learning Objectives
- 12.1 Zero Trust
  - 12.1.1 Technical Objectives of Zero Trust
  - 12.1.2 Zero Trust Pillars & Maturity Model
  - 12.1.3 Zero Trust & Cloud Security
- 12.2 Artificial Intelligence
  - 12.2.1 Characteristics of AI Workloads
  - Next Steps.

INFOSECTRAIN

Educate. Excel. Empower.



www.infosectrain.com | sales@infosectrain.com