INFOSECTRAIN

Accredited by

CSA cloud security alliance® | ISACA

ADVANCED

CLOUD SECURITY GOVERNANCE

ACE **CCAK** & **CCSK** CERTIFICATIONS

INFOSECTRAIN

Course Highlights

- **50-Hour** Instructor-led Training
- Real-world Case Studies
- Hands-on Labs
- Scenario-based Learning
- Extended Post-training Support
- Access Recorded Sessions
- Resume Optimization
- 100% Job Assistance
- Certified Trainer **(18+ Yrs. Exp.)**

INFOSECTRAIN

About Course

The Advanced Cloud Security Governance Course from InfosecTrain provides participants with an in-depth understanding of the diverse aspects of cloud security. This comprehensive course encompasses governance, risk management, identity management, data security, compliance, incident response, network security, cloud infrastructure security, legal considerations, cost management, and more.

Participants will acquire practical insights and hands-on experience in securing cloud environments and preparing for the **Certified Cloud Audit Knowledge (CCAK)** and **Certificate of Cloud Security Knowledge (CCSK)** exams. Tailored to meet the evolving demands of the cloud security landscape, this curriculum is essential for professionals aiming to excel in cloud security governance.

Course Objectives

- Master the fundamentals of cloud security and risk assessment methodologies.
- Implement compliance controls and audit principles within cloud environments.
- Designed and managed robust Identity and Access Management (IAM) solutions for the cloud.
- Develop comprehensive data security and encryption strategies to safeguard sensitive information.
- Secure cloud networks through network segmentation and advanced architectural designs.
- Prepare for incident response and conduct cloud forensics during security breaches.
- Evaluate cloud security using established methodologies and achieve recognized certifications.
- Make informed budgeting decisions while maintaining high-security standards.
- Navigate legal frameworks, contracts, and electronic discovery specific to cloud settings.
- Understand the significance of the CSA STAR Program for cloud security and its application.

INFOSECTRAIN

Target Audience

- Information Security Professionals
- Cloud Security Architects
- Enterprise Risk Management Professionals
- Cloud Managers
- GRC Professionals

Pre-requisites

- Basic understanding of cloud computing and security concepts.
- Some experience in information security or risk management is beneficial but not mandatory.

INFOSECTRAIN

KRISH

18+ Years of Experience

Cloud Audit | CCSP | CCSK | CCAK | AWS CS-S | AWS CAN–S | AWS CSA-P | AWS CDE-P | MCT | CCAK | Azure Adv. Architect & Security | GCP PCA | GCP PCSE | CEH | RHCE

- 18+ years of experience and proven expertise in deploying, migrating, auditing and securing various public cloud platforms including AWS, GCP, Azure etc.
- Trained over 1000+ students globally including those from fortune 500 companies and recognized as a Microsoft Certified Trainer.
- Performing as an Enterprise Cloud Security Architect, Cloud GRC Expert, Auditor & Cloud Migration Strategist for over 15 years and served over 60+ enterprises worldwide.
- Actively contributing as a Technical Writer and Subject Matter Expert for various magazines, websites & organizations worldwide.

INFOSECTRAIN

Course Content

Module 1 Cloud Computing Concepts & Architecture

- Cloud Computing Overview
- Essential characteristics, benefits, and challenges
- Abstraction & Orchestration
- Cloud Service Models: IaaS, PaaS & SaaS
- Deployment Models: Public, Private, Hybrid & Community
- CSA Enterprise Architecture Model
- Cloud Security Overview
- Shared Security Responsibility Model
- Scope, Responsibilities & Models
- Threat landscape and new attack vectors in cloud

Module 2 Introduction to Cloud Security Governance

- Understanding cloud security governance
  - ✓ Defining cloud security governance and its objectives
  - ✓ Differentiating between security and governance in cloud environments
  - ✓ Enterprise risk governance in cloud
  - ✓ Cloud Security Frameworks & Policies

- Complexities in Cloud Security Governance
  - ✓ Exploring the role of cloud security governance in overall risk management
  - ✓ Establishing the linkage between cloud security governance and business value
  - ✓ Impact of Cloud Service and Deployment Models
  - ✓ Cloud Risk Trade-offs and Tools
- Leveraging key tools for governance in cloud & Shared Security Responsibility Model
  - ✓ Contracts, SLAs, and PLAs
  - ✓ Elevating Cloud as a business enabler through governance
  - ✓ Critical stakeholders in cloud security governance
- Analysing cloud-specific threats and attack vectors
  - ✓ Threats specific to cloud computing (CSA Top Threats: Pandemic 11)
  - ✓ The threat landscape and defence-in-depth approach

CASE STUDY: Capital One Data Breach and its Timeline

Module 3 Cloud Risk Assessment and Management

- Identifying cloud-specific risks and threats
  - ✓ Common cloud security risks (Eg: data breaches, data loss, multi tenancy etc.)
  - ✓ Cloud Specific Threat Vectors (Eg: shared resources, misconfigurations)

CASE STUDY: Cloud Security incident real case discussion

- Risk assessment methodologies for cloud environments
  - Cloud Risk assessment
  - NIST Cybersecurity Framework for Cloud Risk Assessment
  - The Risk Register
- Developing risk management strategies
  - Risk mitigation strategies in cloud.
  - Risk Treatment (acceptance, avoidance, transfer, and mitigation)
  - Selecting appropriate cloud security controls
  - Vendor risk assessment
- Cloud risk monitoring and continuous improvement
  - Cloud Security metrics and KPIs
  - SIEM tools in cloud environments
  - Incident Management in Cloud
  - Developing a cloud security policy & key element to include

CASE STUDY: Conducting a Cloud Risk Assessment & Creating a sample risk assessment report

Module 4 Cloud Compliance & Audit

- Cloud Compliance Program Overview
- Design & Build a Cloud Compliance Program
- Cloud-Relevant Laws & Regulations Examples
- Implementing compliance controls in cloud environments
- Compliance Inheritance
- Artifacts of Compliance

- Defining controls and evaluating the effectiveness
- Audit characteristics, principles and criteria in Cloud
  - Types of Auditing
  - Auditing Core Principles
  - Audit steps
  - Defining the Objectives & Scope
- Auditing and reporting in the cloud
- Auditing standards for cloud computing

CASE STUDY: Enabling PCI DSS Compliance on AWS

Module 5 Organization Management

- Organization Hierarchy Models
  - Organization Capabilities Within a Cloud Service Provider
  - Building a Hierarchy Within a Provider
- Managing Organization-Level Security Within a Provider
  - Identity Provider & User/Group/Role Mappings
  - Common Organization Shared Services
- Considerations for Hybrid & Multi-Cloud Deployments
  - Organization Management for Hybrid Cloud Security
  - Organization Management for Multi-Cloud Security
  - Organization Management for SaaS Hybrid & Multi-Cloud

Module 6 Identity and Access Management (IAM) in the Cloud

- Principles of IAM in cloud environments
  - ✓ IAM fundamentals, terminologies & concepts
  - ✓ Criticality of IAM in cloud & IAM Governance
  - ✓ IAM Components in various cloud service providers (AWS IAM, Azure AD, GCP IAM etc)
  - ✓ RBAC, ABAC & PBAC
    - → Defining roles and permissions
    - → Role hierarchy and inheritance
    - → Least privilege and avoiding authorization creeps
    - → Demonstrating RBAC on AWS & Azure
- Federation, Single sign-on (SSO) and multi-factor authentication (MFA) in the cloud
  - ✓ Federated Identity management and cloud
  - ✓ SAML, OpenID & OAuth
  - ✓ SSO integration with cloud
  - ✓ Multifactor authentication and Federation best practices
  - ✓ Managing Users & Identities for Cloud Computing
  - ✓ Managing Identity and FIM across hybrid cloud architectures
- Zero Trust Model (ZTMF)
  - ✓ Introduction to Zero Trust Model (ZTM)
  - ✓ Zero Trust principles and assumptions
  - ✓ Implementing zero trust in cloud approach
  - ✓ Continuous authentication and least privilege access

LABS

- Securing AWS Root User Accounts
- Creating Users & Configuring IAM Policies
- Conditional Access
- AWS Roles & STS

CASE STUDY

Best Practices & Baselining Identity & Access Management in AWS

Module 7 Cloud Data Security and Encryption

- Primer on Cloud Storage
  - Volume/Block Storage
  - Object Storage
  - Database Storage
  - Other Types of Storage
  - Choosing the proper cloud storage with use cases
- Data Security Tools & Techniques
  - Data Classification
  - Identity & Access Management
  - Access Policies
  - Encryption & Key Management
  - Data Loss Prevention
- Building a proper data classification program for the cloud
  - Establish data classification policies in cloud services
  - Monitoring and enforcement

- Data dispersion and resiliency
  - Data Dispersion strategies
  - Data replication, Multi region and DR planning
  - Governance concern for business regarding location & data access
  - Tools available for addressing including contracts, SLAs & Auditing
- Data Encryption and Key Management best practices
  - Encryption algorithms and key management
  - Key management, and lifecycle
  - Cloud provider services and comparison
  - Cloud Key management best practices.
  - Data Security for Artificial Intelligence & AI as a Service

CASE STUDY DISCUSSION: Ensure data security for AWS S3 hosting sensitive data.

- Data retention, deletion, and archiving policies for cloud
  - Data retention policies overview and components
  - Defining data retention periods and protection requirements
  - Secure data erasure in cloud
  - Data archiving and Lifecycle management
- Data Sovereignty & Legal hold challenges and preparation
  - Understanding data sovereignty
  - Legal & compliance considerations and its implications on cloud
  - Data residency and geofencing
  - Understanding Legal hold
  - Preparing cloud storage for legal hold
  - cloud provider cooperation and support requirements

CASE STUDY DISCUSSION: Enforce legal hold in AWS S3 to make immutable data

LABS

- Configuring EBS Volume
- Encrypting an EBS Volume & Snapshot
- AWS KMS Key Management

SCENARIO DISCUSSION

Data encryption strategies, 3rd party integration, and practical architecture

Module 8 Cloud Infrastructure & Networking

- Securing virtual networks in the cloud
  - Cloud network architecture overview
  - Security groups, NACLs and other firewall concepts
  - Networking services in various vendors (AWS VPC, Azure VNET etc.)
  - Isolation and segmentation
  - Software Defined Networks
- Network segmentation and isolation strategies
  - Network segmentation concepts and zoning
  - Implementation of segmentation policies in cloud environments
  - Zero Trust Network Access (ZTNA) for segmentation
- Application and network-level firewalls for cloud environments
  - Cloud-Based Firewall Services (e.g., AWS WAF, Azure Firewall)
  - Web Application Firewall (WAF) for Application Layer Protection

- Attack distribution and DDoS protection in the cloud
  - Understanding Distributed Denial of Service (DDoS) Attacks
  - Cloud DDoS Mitigation Services (e.g., AWS Shield, Azure DDoS Protection)
  - DDoS Attack Detection and Response Strategies
- Zero Trust for Cloud Infrastructure & Networks
  - Software Defined Perimeter & ZT Network Access
- Secure Access Service Edge (SASE)

LABS

- Configure Virtual Private Network (VPC) on AWS
- Configuring Security Groups & NACLs
- Understanding Route Tables
- AWS Inspector Overview

Module 9 Cloud Workload Security

- Types of Cloud Workloads
- Impact on Workload Security Controls
- Securing Virtual Machines
  - Virtual Machine Challenges & Mitigations
  - Creating Secure VM Images with Factories
  - Snapshots & Public Exposures/Exfiltration

- Securing Containers
  - Container Images
  - Container Network architecture
  - Container Orchestration & Management Systems
  - Container Orchestration Security
  - Runtime Protection for Containers
- Securing Serverless and Function as a Service
  - FaaS Security Issues
  - IAM for Serverless
  - Environment Variables & Secrets
- Securing AI Workloads
- AI-System Threats
- AI Risk Mitigation and Shared Responsibilities

Module 10 Security Monitoring

- Cloud Monitoring
  - Logs & Events
- Beyond Logs - Posture Management
- Cloud Telemetry Sources
  - Management Plane Logs
  - Service & Application Logs
  - Resource Logs
  - Cloud Native Tools

- Collection Architectures
  - Log Storage & Retention
  - Cascading Log Architecture
- AI for Security Monitoring

LABS

- Configure Baseline Security Monitoring
- Configure CloudTrail Logs
- Alerting using EventBridge & SNS
- Open Source CSPM Tool

Module 11 Application Security

- Secure Development Lifecycle
  - Secure SDLC Stages
  - Threat Modelling
  - Testing: Pre-Deployment
  - Testing: Post Deployment
- Architecture's Role in Secure Cloud Applications
  - Cloud Impacts on Architecture-Level Security
  - Architectural Resilience
- Identity & Access Management and Application Security
  - Secrets Management

- Dev Ops & DevSecOps
- Microservices

Module 12 Incident Response and Cloud Forensics

- Incident Response Lifecycle
- Preparation
  - Incident Response Preparation & Cloud Service Providers
  - Training for Cloud Incident Responders
- Detection & Analysis
  - Cloud Impact on Incident Response Analysis
  - Cloud System Forensics
- Containment, Eradication, & Recovery
  - Containment
  - Eradication
  - Recovery
- Post Incident Analysis
- Developing a cloud-specific incident response plan
  - Testing strategies for plan effectiveness
- Investigating security incidents in the cloud
  - Cloud incident triaging
  - Evidence collection and forensics
  - Data preservation and chain of custody
  - Logs and artifacts

- Digital forensics challenges and best practices in cloud environments
  - ✓ Digital forensics and challenges in cloud
  - ✓ Best practices for cloud forensics

SCENARIO DISCUSSION: Creating an Incident Response Runbook

Module 13 Cloud Security Assurance and Assessment

- Cloud security assessment methodologies
- Security controls testing and validation in the cloud
- Cloud security certifications and their significance
- CCM and CAIQ
- CCM Domains & Controls
- Architecture Relevance
- Mapping standards and frameworks

SCENARIO DISCUSSION: Creating an assessment report on Cloud based on CCM & CAIQ

Module 14 Cost Management and Security

- Understanding cost implications of security decisions
- Budgeting for cloud and cloud security initiatives
- Cost optimization without compromising security
- Cost-benefit analysis, and return on investment for Cloud services

Module 15 Security Trust Assurance and Risk (STAR) Program

- CSA STAR Program
- Security & Privacy Implications of STAR
- STAR Program Components
- STAR Levels

INFOSECTRAIN

Testimonials

Suraj Abhiany

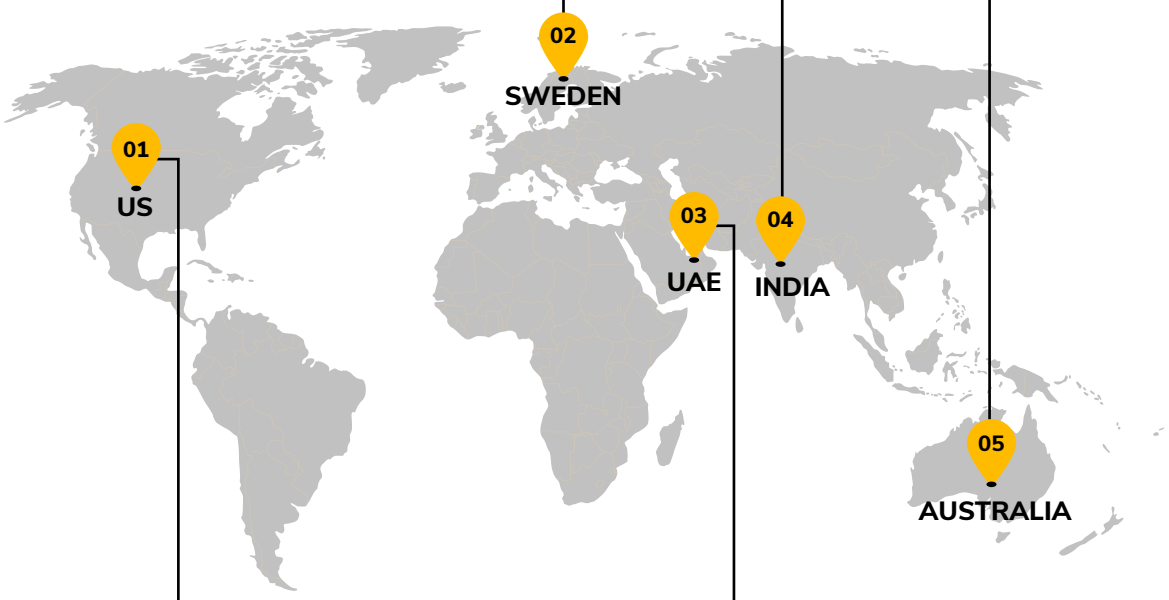
I appreciated the training provided by InfosecTrain for the Advanced Cloud Security Governance Course. The trainer was very knowledgeable and offered excellent guidance on all my queries. Many thanks for the valuable support!

Sonal Shukla

The entire Advanced Cloud Security Governance course was very informative and detail-oriented, with all concepts explained through practical examples. The training at InfosecTrain was excellent, and the trainers were knowledgeable, making the learning experience great.

Babitha Nair

The Advanced Cloud Security Governance Course by InfosecTrain was excellent. The trainer explained concepts clearly, even in recordings. Despite odd hours, I gained valuable insights. Thanks to the InfosecTrain Team for their efforts!



Shantel Flowers

The Advanced Cloud Security Governance course was outstanding. InfosecTrain's skilled trainers made the experience highly educational and beneficial.

Srinivas Acharjya KB

The training session for the Advanced Cloud Security Governance course provided by InfosecTrain was very good. Thank you very much for the valuable instruction and guidance.

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on