INFOSECTRAIN

Advanced Cloud

Security Governance Course

Elevate your expertise in cloud security with our Advanced Cloud Security Governance Course covering governance, risk management, identity management, data security, and more. Prepare for the CCAK and CCSK exams with tailored content to master cloud security governance.

COURSE HIGHLIGHTS

1 40 Hrs of Instructor-led Training

2 Post Training Support

3 Get CPE Certificate

4 Learn from Industry Experts

COURSE OBJECTIVES

- Master cloud security fundamentals and risk assessment methodologies.
- Implement compliance controls and audit principles in cloud environments.
- Design and manage Identity and Access Management solutions in the cloud.
- Develop data security and encryption strategies to protect sensitive information.
- Secure cloud networks through network segmentation and advanced architectures.
- Prepare for incident response and cloud forensics in case of security breaches.
- Assess cloud security through recognized methodologies and certifications.
- Make informed budgeting decisions without compromising security.
- Navigate legal frameworks, contracts, and electronic discovery in cloud settings.

Target Audiences:

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

Prerequisites:

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

COURSE CONTENT

Module 1: Cloud Computing Fundamentals

Module 2: Cloud Security Fundamentals

Module 3: Introduction to Cloud Security Governance

Module 4: Cloud Risk Assessment and Management

Module 5: Cloud Compliance Program, Frameworks and Regulations

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

Module 7: Cloud Data Security and Encryption

Module 8: Network Security in Cloud Environments

Module 9: Cloud Infrastructure Security

Module 10: Incident Response and Cloud Forensics

Module 11: Cloud Security Assurance and Assessment

Module 12: Cost Management and Security

Module 13: Legal Issues, Contracts and Electronic Discovery

Module 14: Security Trust Assurance and Risk (STAR) Program

Module 1: Cloud Computing Fundamentals

- Cloud Computing Overview
- Benefits and Challenges
- Cloud Service Models: IaaS, PaaS & SaaS
- Deployment Models: Public, Private, Hybrid & Community
- Cloud Shared Responsibility Matrix

Module 2: Cloud Security Fundamentals

- Cloud Security Overview
- Benefits and Challenges
- Cloud Policy and Governance models
- Threat Landscape and New Attack Vectors in the Cloud

Module 3: 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

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

- 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

Analyzing Cloud-Specific Threats and Attack Vectors

- Threats Specific to Cloud Computing (CSA Top Threats: Pandemic 11)
- The Threat Landscape and Defense-in-Depth Approach

Case Study: Capital One Data Breach and its Timeline

Module 4: Cloud Risk Assessment and Management

Identifying Cloud-Specific Risks and Threats

- Common Cloud Security Risks (e.g., 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
- ENISA Document

Developing Risk Management Strategies

- Risk Mitigation Strategies in the 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

  - SIEM Tools in Cloud Environments
  - Incident Management in the Cloud
  - Developing a Cloud Security Policy & Key Elements to Include
- **Case Study: Conducting a Cloud Risk Assessment & Creating a Sample Risk Assessment Report**
- **ENISA Recommendations**

Module 5: Cloud Compliance Program, Frameworks and Regulations

- Cloud Compliance Program Overview
- Design & Build a Cloud Compliance Program
- Overview of Major Cloud Compliance Standards (e.g., GDPR, HIPAA, PCI DSS)
- Cloud-Specific Compliance Challenges and Considerations
- Implementing Compliance Controls in Cloud Environments
- 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 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 Components in Various Cloud Service Providers (AWS IAM, Azure AD, GCP IAM, etc.)

Role-Based Access Control (RBAC) and Privilege Escalation

- Understanding RBAC in a Cloud Environment
- 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
- SSO Integration With Cloud
- Multifactor Authentication and Federation Best Practices.
- Managing Identities Across Different Cloud Providers
- 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 the Cloud Approach
- Continuous Authentication and Least Privilege Access

Case Study: Best Practices & Baselining Identity & Access Management in AWS

Module 7: Cloud Data Security and Encryption

Information Governance

- Data Security Lifecycle
- Data Security Function, Actors & Controls

Data Classification and Sensitivity Labeling in the Cloud

- Data Classification and its Importance
- Impact of Misclassified Data Defining Sensitivity Labels

Building a Proper Data Classification Program for the Cloud

- Establish Data Classification Policies in Cloud Services
- Monitoring and Enforcement

Data Sovereignty Requirements and Controls in the Cloud

- Understanding Data Sovereignty
- Legal &amp: Compliance Considerations and its Implications on Cloud
- Data Residency and Geofencing
- Compliance with Regional Regulations (e.g., GDPR)

Data Dispersion and Resiliency

- Data Dispersion Strategies
- Data Replication, Multi-Region, and DR Planning
- Governance Concerns for Business Regarding Location & Data Access
- Tools Available for Addressing Including Contracts, SLAs & Auditing

Key Cloud Storage Services in the Cloud

- Cloud Storage Types Overview and Various Provider Options
- Choosing the Proper Cloud Storage With Use Cases
- Governance Concern For Business, Including Access Levels & Security Controls Integration
- Tools & Technologies For Storage Security & Monitoring

Data Encryption and Key Management Best Practices

- Data Encryption Fundamentals
- Encryption Algorithms and Key Management
- Key Management and Lifecycle
- Cloud Provider Services and Comparison
- Cloud Key Management Best Practices.
- Case Study Discussion: Ensure Data Security For AWS S3 Hosting Sensitive Data.

Data Loss Prevention (DLP) Strategies For the Cloud

- DLP Fundamentals
- DLP Phases, Policies, and Rules
- Cloud DLP Solutions and Integrations

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 the Cloud
- Data Archiving and Lifecycle Management

Legal Hold Challenges and Preparation

- 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

Scenario Discussion: Data Encryption Strategies, 3rd Party Integration, and Practical Architecture

Module 8: Network Security in Cloud Environments

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

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

Advanced Network Security Architectures (SDP, ZTNA) For Cloud

- ✓ Software-Defined Perimeter (SDP) Principles
- ✓ Zero Trust Network Access (ZTNA) Concepts
- ✓ The Architecture of SDP and ZTNA in Cloud Environments

Implement a Secure Segmented Virtual Private Network on AWS/Azure

Module 9: Cloud Infrastructure Security

- Cloud Network Virtualization
- Virtual Networks and Appliances
- Software Defined Networking (SDN)
- Microsegmentation and Software-Defined Parameter
- Hybrid Cloud Strategy
- Workload Security
- Hardening Cloud Virtual Machines and Containers
- Secure Configuration Management in Cloud Platforms
- Scenario Discussion: Baselining With CIS Benchmarks & Continuous Assurance
- Case Study: VM Hardening Best Practices in Cloud
- Business Continuity & Disaster Recovery in the Cloud
- Architect For Failure
- Management Plane Security

Module 10: Incident Response and Cloud Forensics

Developing a Cloud-Specific Incident Response Plan

- Introduction to Incident Management and IR in Cloud
- Key Difference in Cloud and On-Premises, Shared Responsibilities
- Developing an Incident Response Team
- Cloud-Specific IR Scenarios Discussion
- Testing Strategies For Plan Effectiveness

Cloud Incident Detection and Monitoring Tools

- Cloud Security Monitoring
- CSPM Tools
- Cloud Native Security Tools

- **Playbooks vs. Runbooks**
  - Understanding Playbooks and Runbooks
  - Common Elements in IR Playbooks

  - Role of Runbooks in Incident Resolution
  - Runbook automation tools
- **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 the Cloud
  - Best Practices For Cloud Forensics
- **Scenario Discussion: Creating an Incident Response Runbook**

Module 11: 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 12: 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 13: Legal Issues, Contracts and Electronic Discovery

Legal Frameworks Governing Data Protection and Privacy

- Cross-Border Data Transfer
- Regional Considerations

Contracts and Provider Selection

- Contracts & SLAs
- Due Care & Due Diligence
- Third-Party Audits and Attestations

Electronic Discovery

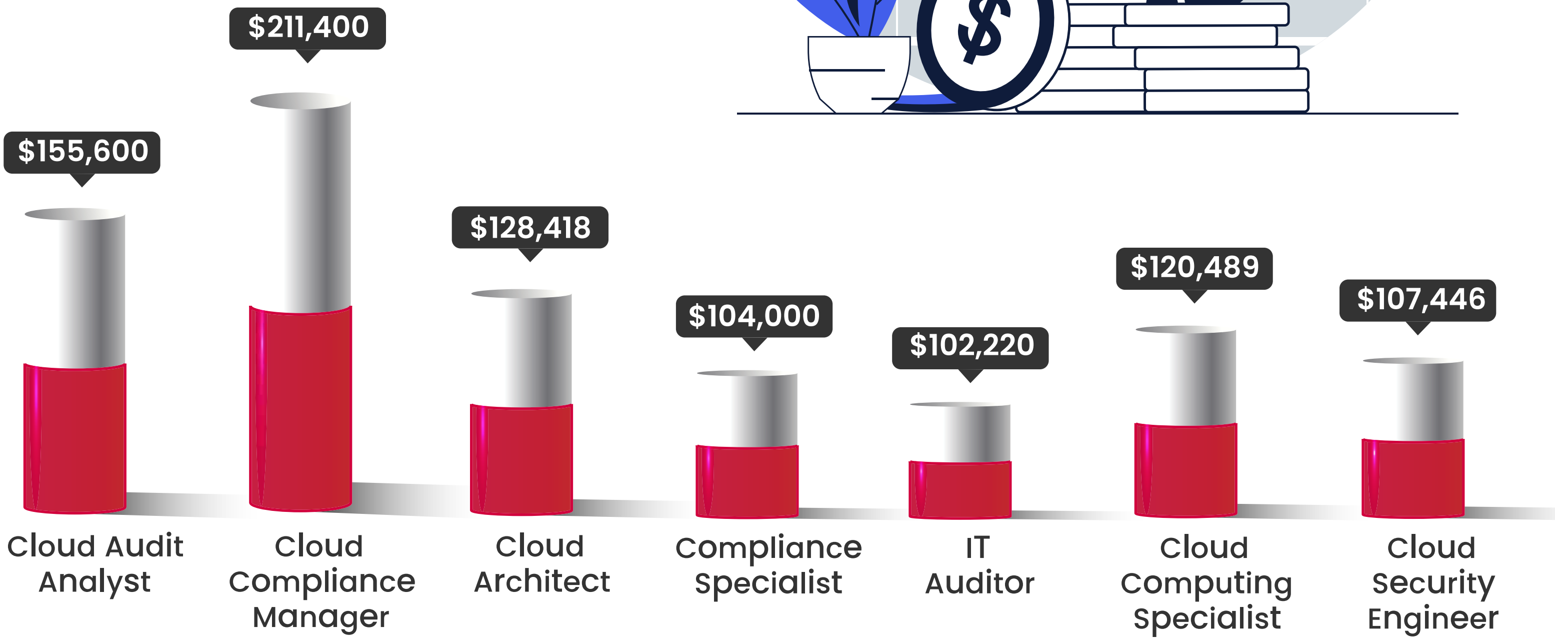
- **Data Custody**
- **Data Preservation**
- **Data Collection**
- **Subpoena Response**

Module 14: Security Trust Assurance and Risk (STAR) Program

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

INFOSECTRAIN

Career Benefits of a
Cloud Certification



Hiring Companies

WNS accenture amazon Shell vmware Capgemini

snowflake CYBERARK Informatica cisco salesforce

INFOSECTRAIN

www.infosectrain.com I sales@infosectrain.com