INFOSECTRAIN
Educate. Excel. Empower.

AI Powered Course

Enterprise Cloud & AI Governance

Professional Training

INFOSECTRAIN

Course Highlights

70-Hour LIVE Instructor-Led Training

Real-World Enterprise Scenarios & Use Cases

Practical Approach

Highly Interactive & Dynamic Sessions

Telegram Support Group

Learn from Industry Experts

Career Guidance & Mentorship

Extended Post Training Support

Access to Recorded Sessions

INFOSECTRAIN

About Course

Enterprise Cloud Security & AI Governance Professional is an advanced program designed to build comprehensive governance expertise across two core domains: Cloud Security Governance and AI Governance. The course provides structured coverage of cloud GRC and AI governance concepts while emphasizing how they come together in real enterprise environments where AI systems operate on cloud platforms. Participants will learn how cloud governance controls, risk management, and compliance frameworks extend into AI workloads, and how AI-specific risks, ethics, and regulatory requirements must be governed within cloud operating models. This program equips professionals to integrate Cloud and AI governance into a unified enterprise approach, enabling secure, compliant, and trustworthy AI adoption aligned with business and regulatory expectations.

Course Objectives

Upon successful completion of the training, participants will be able to:

- Develop a holistic governance perspective covering both Cloud and AI systems
- Gain the ability to design and operate enterprise-wide Cloud & AI governance programs aligned with business objectives and regulatory expectations
- Learn how to translate cloud security, risk, and compliance controls into AI-enabled environments
- Build expertise in cloud & AI risk management
- Understand cloud governance models, shared responsibility, and compliance inheritance in enterprise environments
- Learn GRC aspects specific to cloud, including data security, IAM, visibility, and infrastructure governance.
- Gain clarity on AI governance principles, including accountability, transparency, explainability, and oversight
- Learn how to govern data used by AI systems across its lifecycle, including privacy, bias, and data protection
- Understand global AI regulations and standards and their impact on enterprise AI adoption
- Strengthen skills in audit, assurance, and evidence readiness for both cloud platforms and AI systems
- Position yourself as a Cloud & AI Governance professional capable of supporting regulated, large-scale enterprise initiatives

INFOSECTRAIN

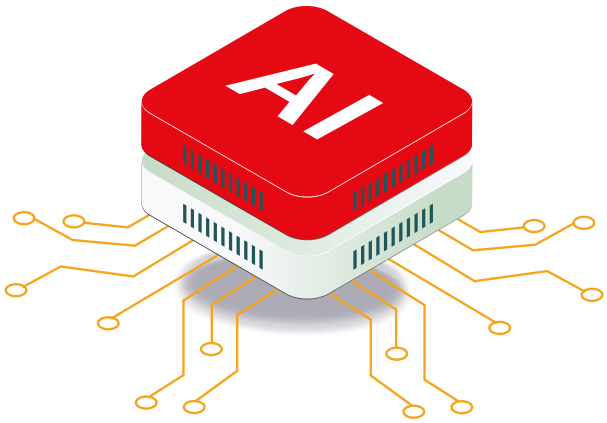
Target Audience

This training is ideal for:

- Cloud Security & Governance Professionals
- AI Governance, GRC & Risk Professionals
- Security Architects & Enterprise Architects
- IT & Security Leaders overseeing AI adoption
- Consultants, Auditors, and Assessors
- Compliance, Privacy & Policy Managers
- Cloud & AI Program Managers

Pre-Requisites

- Basic understanding of cloud computing and security concepts.
- Some experience in information security, risk management, & Governance is beneficial but not mandatory.
- Exposure to AI, data, or digital transformation initiatives will be helpful, but no tech/programming background is required.



INFOSECTRAIN

Course Content

PART 1: Cloud Security Governance

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
- Complexities in Cloud Security Governance
- Leveraging key tools for governance in the cloud & Shared Security Responsibility Model
- Building & integrating an effective cloud governance strategy
- Analyzing cloud-specific threats and attack vectors

Case Study: Capital One Data Breach and its Timeline

Module 3 Cloud Risk Assessment and Management

- Identifying cloud-specific risks and threats
- Risk assessment methodologies for cloud environments
- Developing risk management strategies
- Cloud risk monitoring and continuous improvement

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 effectiveness
- Audit characteristics, principles, and criteria in Cloud
- Auditing standards for cloud computing

Case Study: Enabling PCI DSS Compliance on AWS

Case Study: Perform a practical Cloud Auditing

Module 5 Organization Management

- Organization Hierarchy Models
- Managing Organization-Level Security Within a Provider
- Considerations for Hybrid & Multi-Cloud Deployments

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

- Principles of IAM in cloud environments
- Federation, Single sign-on (SSO) and multi-factor authentication (MFA) in the cloud
- Zero Trust Model (ZTMF)
- Architecting for zero trust

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

Module 7 Cloud Data Security and Encryption

- Primer on Cloud Storage
- Data Security Controls, Tools & Techniques
- Building a proper data classification program for the cloud
- Data dispersion and resiliency
- Data Encryption and Key Management best practices
- Data retention, deletion, and archiving policies for cloud
- Data Sovereignty & Legal hold challenges and preparation

Scenario Discussion: Data encryption strategies, 3rd party integration, and practical architecture

Module 8 Cloud Infrastructure & Networking

- Securing virtual networks in the cloud
- Network segmentation and isolation strategies
- Application and network-level firewalls for cloud environments
- Attack distribution and DDoS protection in the cloud
- Zero Trust for Cloud Infrastructure & Networks
- Secure Access Service Edge (SASE)

Module 9 Cloud Workload Security

- Types of Cloud Workloads
- Impact on Workload Security Controls
- Virtual Machines, Containers, Serverless Security Strategies
- Securing AI Workloads
- AI-System Threats
- AI Risk Mitigation and Shared Responsibilities

Module 10 Security Monitoring

- Cloud Monitoring
- Beyond Logs - Posture Management
- Cloud Telemetry Sources
- Collection Architectures
- AI for Security Monitoring

Module 11 Application Security

- Secure Development Lifecycle
- Architecture's Role in Secure Cloud Applications
- Identity & Access Management and Application Security
- DevOps & DevSecOps
- Microservices

Module 12 Incident Response and Cloud Forensics

- Incident Response Lifecycle
- Preparation
- Detection & Analysis
- Containment, Eradication, & Recovery
- Post Incident Analysis
- Developing a cloud-specific incident response plan
- Investigating security incidents in the cloud
- Digital forensics challenges and best practices in cloud environments

Scenario Discussion: Creating an Incident Response Runbook

Module 13 Cloud Security Assurance and Assessment & STAR

- Cloud security assessment methodologies
- Security controls testing and validation in the cloud.
- Cloud security certifications and their significance
- CCM and CAIQ
- CCM Domains & Controls
- Mapping standards and frameworks
- CSA STAR Program
- Security & Privacy Implications of STAR
- STAR Program Components

Scenario Discussion: Creating an assessment report on Cloud-based on CCM & CAIQ

Module 14 Cost Management and Security

- Understanding the 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

PART 2: AI Governance

Module 1 AI Foundations

- Types of AI (Functionality & Capabilities)
- Branches & Applications of AI across industries
- AI Technology Stack
- Machine Learning Components, Processes, and Types
- Generative AI & Large Language Models (LLMs)
- Common AI Attacks & Mitigation
- Ethical Considerations

Module 2 Ethics, Responsible AI & Societal Impact

- Principles of Responsible AI
- Bias, Fairness, and Discrimination
- Privacy & Security Concerns
- Job Displacement & Economic Impact
- Bias: Use Cases
- Types of AI Discrimination
- Addressing algorithmic bias and fairness
- Privacy concerns and data protection
- Responsible AI Development and Deployment
- Key principles of Responsible AI

Case Studies

Module 3 Global AI Laws & Regulations

- Overview of existing AI laws and regulations
- Legal and ethical considerations: Data privacy, bias, transparency, accountability
- Emerging trends in AI legislation
- How do AI regulations affect the adoption of AI in different industries
- Categories of AI Law
- Legal and ethical considerations: Data privacy, bias, transparency, accountability
- OECD AI Principles: Fairness, transparency, and accountability
- EU AI Act
- ISO/IEC 42001:2021 for Artificial Intelligence
- Assessing the regulatory impact on AI systems
- Managing cross-border compliance
- Intellectual Property Rights
- Liability and Accountability

Module 4 AI Governance

- Governance & Types
- Enterprise AI Governance Vs. Responsible AI Governance
- AI Governance Models (Centralized, Decentralized, Federated)
- Trustworthy AI
- Responsible Artificial Governance (RAG)
- Transparency, explainability & Liability
- Designing AI Governance Committees & Councils
- Aligning AI with Business Objectives
- Building & Measuring AI Governance Programs
- Identifying and Engaging Stakeholders
- Aligning Stakeholder Interests with Governance Objectives
- Managing Expectations & Communication
- Role-Based Exercises

Module 5 AI Models, Architecture & Lifecycle

- Key Layers of AI Architecture (Data, Model, Application, Security)
- Governance in AI Architecture
- AI System Lifecycle & Governance Integration
- AI in the Cloud
- Understanding AI Models
- Model Evaluation & Interpretability (LIME, SHAP, Rule-Based, Visualizations)
- Explainability & Accountability (GDPR Right to Explanation)
- RAG & Prompt Engineering
- Agentic AI & Automation
- Model Drift, Degradation, Monitoring
- Model Cards & Documentation

Module 6 AI Risk Management

- AI Risk Categories: Ethical, Operational, Societal
- NIST AI RMF & MIT AI Risk Repository
- AI Risk Register & AI Impact Assessment (AIIA)
- Risk Assessment Methodologies (FMEA, FTA)
- EU AI Act Risk Tiers
- Bias Identification & Mitigation
- Third-Party AI Risk Management
- AI Governance Maturity Models

Case Study: AI-Powered Chatbot Risks

Module 7 Data Governance for AI

- Data Strategy for AI
- Data Governance Policy
- Data quality, Data Gathering
- Data Cleansing
- Data Labelling, Data Privacy & Security, Data Ethics
- Data Bias
- Data Validation and Testing Data
- Data lifecycle management for AI projects
- Data collection, processing, storage, and use for AI systems
- Data exfiltration
- Data Anonymization, Pseudonymization, and Differential Privacy techniques

Case Study: AI recommendation engine

- Implementing data governance frameworks for AI
- AI data security

Module 8 AI Model Validation & Testing

- Understanding AI Models
- Model Evaluation & Interpretability (LIME, SHAP, Rule-Based, Visualizations)
- Explainability & Accountability (GDPR Right to Explanation)
- Retrieval Augmented Generation (RAG) & Prompt Engineering
- Model Drift, Degradation, and Monitoring
- Model Validation & Testing (Bias, Robustness, Failures)
- Model Cards & Documentation

Module 9 AI on Cloud

- Role of Cloud in AI
- AI Hosting Models on Cloud
- Key considerations for choosing CSP for AI Workloads
- Leveraging Native Cloud Security for AI
- Addressing AI-Specific Security Vectors in the Cloud
- Integrating AI Governance into Cloud Infrastructure

Case Study: AI Application Lifecycle

Module 10 AI Security

- AI Threat Landscape
- Security Controls Across AI Lifecycle
- Encryption, IAM, and Intrusion Detection
- AI Red Teaming & Adversarial Attacks
- Incident Response for AI Systems

Module 11 Auditing AI Systems

- AI Audit Frameworks & Standards
- Key Audit Areas & Techniques
- Challenges in AI Auditing (Methodologies, Data Access)
- AI Audit Simulation Exercise

Module 12 SDLC for AI Systems

- SDLC Methodologies (Agile, DevOps, Waterfall)
- Governance in Each SDLC Phase
- Planning, Design, Development, Testing, Deployment, Maintenance

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on