INFOSECTRAIN
Educate. Excel. Empower.

AI Powered Course

Certified AI Governance Specialist

Training

INSTRUCTOR

KRISH

18+ Years Of Experience

AIGP | TAISE | CCZT | CCSP | CCSK
AWS Sec | MCT | Azure Adv. Architect
& Security | GCP | CEH

INFOSECTRAIN

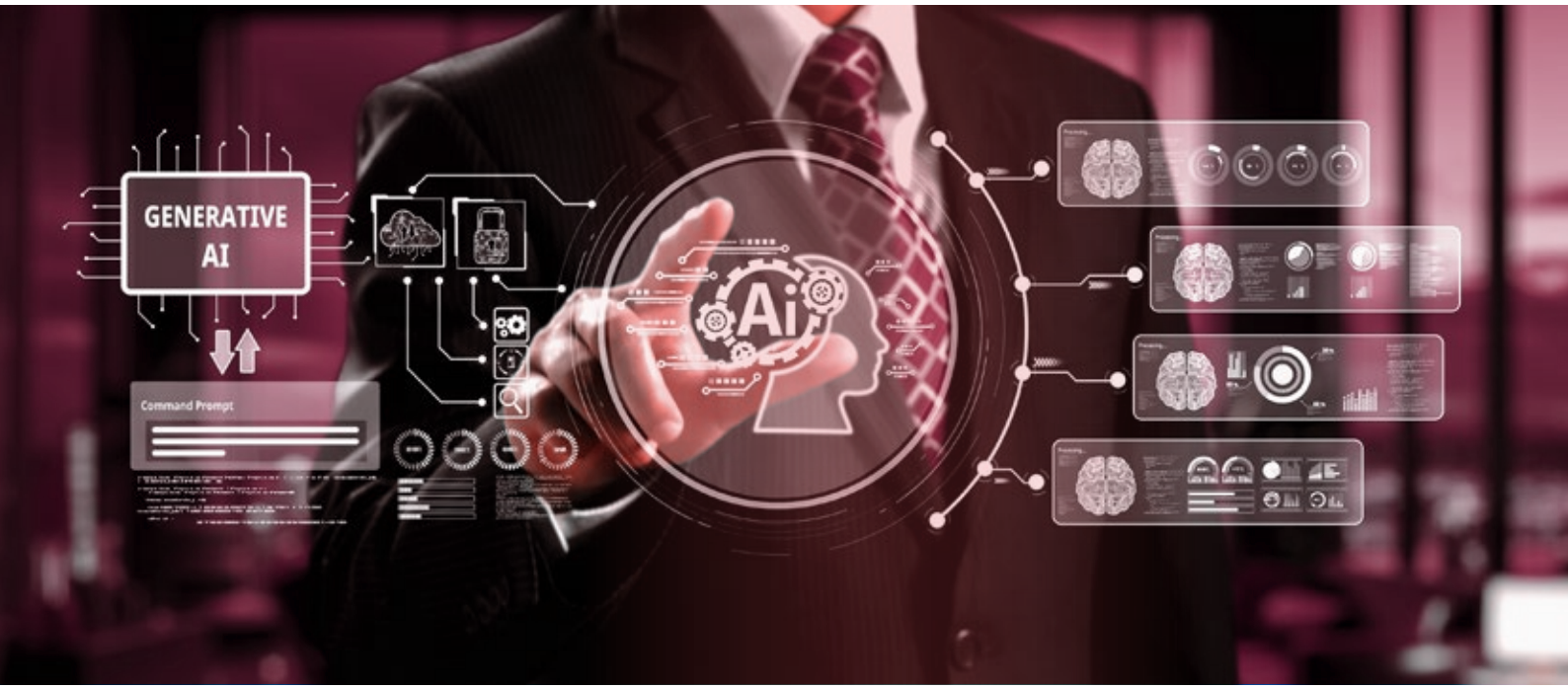
Course Highlights

- **48-Hour LIVE** Instructor-Led Training
- Real-World AI Use Cases & Governance Scenarios
- Practical Approach
- Highly Interactive and Dynamic Sessions
- Telegram Support Group
- Learn from Industry Experts
- Career Guidance and Mentorship
- Extended Post Training Support
- Access to Recorded Sessions

INFOSECTRAIN

About Course

Certified AI Governance Specialist (CAIGS) is an advanced, end-to-end program designed to help professionals master the frameworks, tools, and strategies needed to govern Artificial Intelligence systems responsibly, securely, and at scale. This 48-hour intensive program covers the full lifecycle of AI governance, from ethical foundations, legal and regulatory compliance, data governance, risk management, assessment, and model accountability to the integration of AI systems within cloud environments. Participants will gain practical expertise in aligning AI adoption with business goals while ensuring fairness, transparency, security, and compliance with global standards. By combining theoretical knowledge and real-world case studies, this course equips professionals to design and operationalize trustworthy AI governance programs that are both future-proof and business-ready.



INFOSECTRAIN

Course Objectives

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

- Understand the AI governance lifecycle, from data and models to risk, ethics, law, and compliance
- Drive Responsible AI Adoption
- Learn how to navigate and comply with fast-evolving global AI regulations
- Utilize frameworks for identifying, assessing, and managing ethical, operational, and compliance risks in AI
- Integrate Governance with Cloud AI

INFOSECTRAIN

Target Audience

This training is ideal for:

- IT & Security Leaders
- Information Security Professionals
- Cloud Security Professionals
- Security Architects & Engineers
- GRC Professionals
- Consultants & Auditors
- Legal, Policy, & Risk Managers
- Data & AI Project Managers
- Business & Technology Leaders

Pre-Requisites

The training has no set prerequisites.

INFOSECTRAIN

Our Expert Instructor

KRISH

18+ Years of Experience

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

Krish is a cloud security and GRC expert with over 18 years of experience in deploying, auditing, and securing AWS, Azure, and GCP environments. He has trained 1000+ professionals globally and served 60+ enterprises as a cloud architect, auditor, and migration strategist. A Microsoft Certified Trainer, Krish is also an active technical writer and SME, with expertise in platform security, Linux hardening, and enterprise-wide cloud compliance and governance.

INFOSECTRAIN

Course Content

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:
  - Copyright and patent issues related to AI models and data.
  - Ownership of AI-generated content
- Liability and Accountability:
  - Determining liability for AI-related harms.
  - Ensuring accountability for AI decisions.
- Algorithmic Accountability
  - Establishing mechanisms for auditing and reviewing AI systems.

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
- 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

- Cloud Computing Fundamentals
- 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