INFOSECTRAIN
Educate. Excel. Empower.

AI Powered Course

Certified AI Governance Specialist

Training

INSTRUCTOR

KRISH

19+ Years Of Experience

AI GRC | AIGP | CISA | CISM
AAIA | AAISM | TAISE | CCZT
CCSP | CCSK | CCAK

INFOSECTRAIN

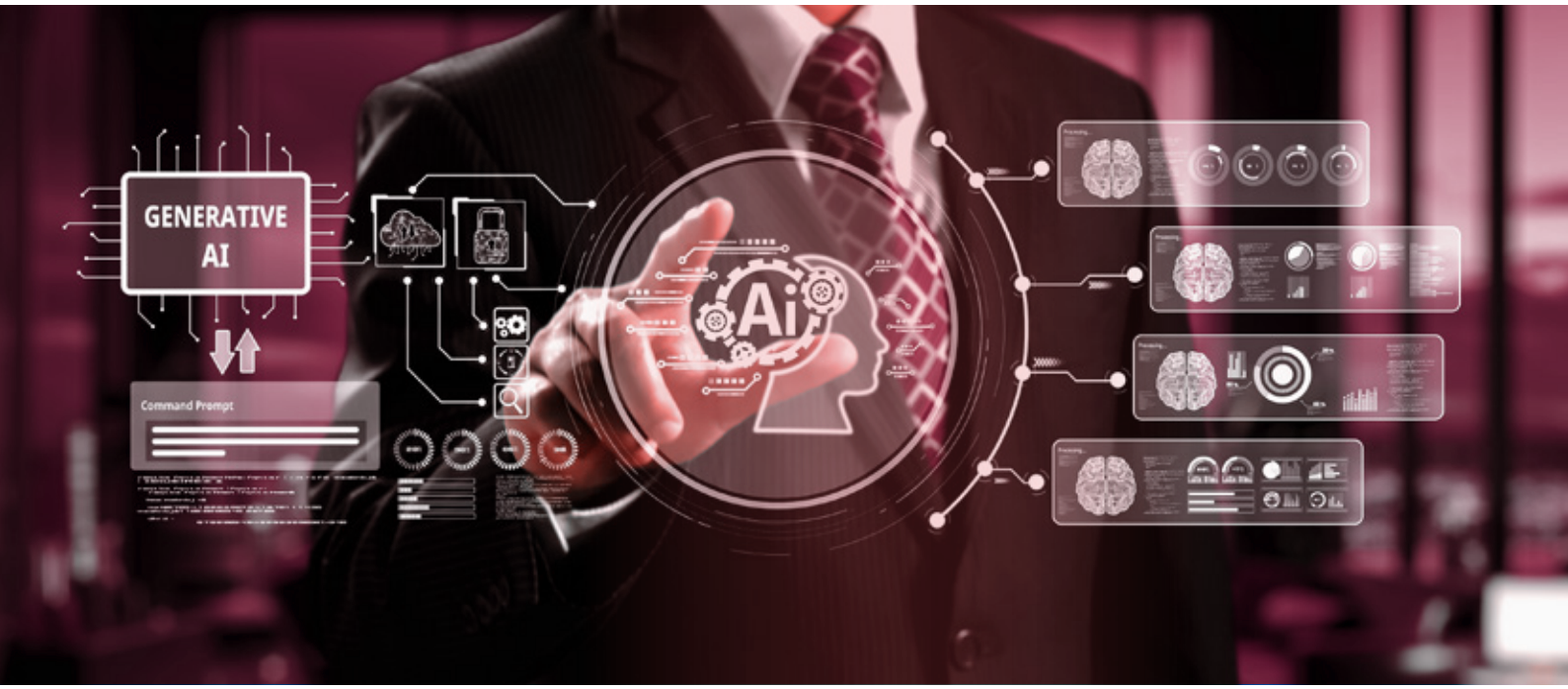
Course Highlights

- **48-Hour LIVE** Instructor-Led Training
- Real-World AI Use Cases & Governance Scenarios
- Master Full AI Governance Lifecycle
- Navigate Global AI Regulations: EU AI Act & NIST AI RMF
- Govern GenAI, LLMs, RAG & more
- Integrate AI Governance into Cloud
- AI Audit Simulation Exercise
- AI Risk Register & AI Impact Assessment (AIIA)
- Scenario-Based Online Exam Included

INFOSECTRAIN

About Course

The Certified AI Governance Specialist (CAIGS) training from InfosecTrain is a 48-hour live program that equips professionals to govern AI systems responsibly, securely and at scale, across the full AI lifecycle from ethical foundations and regulatory compliance to model accountability, data governance and cloud integration. Taught by a certified AIGP and cloud security expert with 19+ years of enterprise experience across AWS, Azure and GCP, the course covers the EU AI Act, NIST AI RMF, AI risk registers, impact assessments, model validation, bias mitigation, adversarial attacks and AI audit simulation: combining 12 content-rich modules with real-world case studies so you can design, implement and audit trustworthy AI governance programs from day one.



Course Objectives

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

- Master the full AI governance lifecycle from data and models to ethics, risk and regulation
- Understand the EU AI Act & other common regulations & standards applicable for AI
- Develop an AI Risk Register and conduct AI Impact Assessments (AIIA) for your organisation
- Practical risk assessment aligned with NIST AI RMF
- Understand the ethical dimensions of AI: bias, fairness, privacy, and societal impact, and apply responsible AI principles in practice
- Govern GenAI, LLMs, RAG and prompt engineering within an enterprise compliance context
- Integrate AI governance into cloud environments
- Conduct AI audits using established frameworks, key audit areas and simulation exercises
- Develop real-world AI governance policies, frameworks, and documentation applicable to your organisation
- Design and operationalise an enterprise AI governance structure, including committees, roles, and stakeholder alignment

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

Exam Details

Certification Body	InfosecTrain
Exam Format	Multiple-choice Questions and Scenario-based Questions
Number of Questions	30 Questions
Exam Duration	60 Minutes
Exam Language	English
Passing Score	70%
Testing Mode	Online

INFOSECTRAIN

Our Expert Instructor

KRISH

19+ Years of Experience

AI GRC | AIGP | CISA | CISM | AAIA | AAISM
TAISE | 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 | VCP-DCV | CEH | RHCE | NCA | DCHN

Krish is a seasoned Cloud Security Architect and AI Governance specialist with 19+ years of experience in securing, architecting, and migrating enterprise workloads across major public cloud platforms. Recognized as a Microsoft and Cloud Security Alliance (CSA) Authorized Instructor, he has trained 2000+ professionals globally. With strong expertise in Cloud Security, GRC, and AI Governance, he helps organizations design responsible AI frameworks, manage AI risks, and implement secure, compliant cloud and AI adoption strategies.

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