INFOSECTRAIN
Educate. Excel. Empower.

EXAM INCLUDED

AI Powered Course

# Certified AI Governance Specialist

## Training

## INSTRUCTOR

# KRISH

**19+ Years Of Experience**

AI GRC | AIGP | CISA | CISM
AAIA | AAISM | TAISE | CCZT
CCSP | CEH

INFOSECTRAIN

# Course Highlights

- **48-Hour LIVE** Instructor-Led Training
- Real-world AI Projects
- Hands-on Case Studies
- AI Governance Lifecycle
- Globally Recognized Certification
- Certified Experts
- Dedicated Telegram Support Group
- Access to Recorded Sessions
- Career Guidance & Mentorship

INFOSECTRAIN

# About Course

Certified AI Governance Specialist (CAGS) 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 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, 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

By the end of this Program, the 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 and Security Leaders
- Information Security Professionals
- Cloud Security Professionals
- Security Architects and Engineers
- GRC Professionals
- Consultants and Auditors
- Legal, Policy, and Risk Managers
- Data and AI Project Managers
- Business and Technology Leaders

## Pre-Requisites

The training has no set prerequisites.

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

## Module 2 Ethics, Responsible AI and Societal Impact

- Responsible AI Principles
- Bias, Fairness, and Discrimination
- Privacy, Data Protection and Security Concerns
- Job Displacement and 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
- Responsible AI Case Studies

## Module 3 Global AI Laws and 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 Laws
- OECD AI Principles: Fairness, transparency, and accountability.
- EU AI Act
- ISO/IEC 42001:2021 for Artificial Intelligence
- AI Liability and Accountability
- Assessing the regulatory impact on AI systems
- Copyright and AI-generated content
- Cross-border AI Compliance

INFOSECTRAIN

## Module 4 Enterprise AI Governance and Governance Operations

- Enterprise AI governance models
- Enterprise AI Governance Vs. Responsible AI Governance
- AI Governance Models (Centralized, Decentralized, Federated)
- Trustworthy AI
- Responsible Artificial Governance (RAG)
- Governance Committees and Operating Model
- Aligning AI with Business Objectives
- Building and Measuring AI Governance Programs
- Identifying and Engaging Stakeholders
- Aligning Stakeholder Interests with Governance Objectives
- AI documentation (Model Cards, AI Impact Assessments, Risk Registers, Policies)
- Governance metrics, KRIs/KPIs and executive reporting
- Governance Maturity Assessment
- Continuous Governance and Monitoring

## Module 5 AI Systems, Models and Lifecycle Governance

- AI architecture and system components (Data, Model, Application, Security)
- Foundation models, LLMs and multimodal models
- Governance in AI Architecture
- Model Governance and Model Registry
- Explainability (LIME, SHAP)
- RAG Fundamentals and Prompt Engineering
- Model Validation and Testing
- Bias, Robustness, Safety and Hallucination Testing
- Model Drift, Data Drift and Continuous Monitoring
- Model Cards and Documentation

## Module 6 Agentic AI Governance

- Introduction to Agentic AI
- AI assistants vs AI agents
- Multi-agent systems
- Enterprise agent architecture
- Agent identity and autonomy
- Governance risks for autonomous agents
- Prompt injection and memory poisoning
- Tool governance and permission management
- Human-in-the-loop controls
- Guardrails, monitoring and kill switches
- Agent lifecycle governance
- Enterprise case study

INFOSECTRAIN

## Module 7 AI Risk Management

- Introduction To AI Risks
- AI Risk Categories
- NIST AI RMF and MIT AI Risk Repository
- AI Impact Assessment (AIIA)
- AI Risk Register
- EU AI Act Risk Tiers
- Risk Assessment Methodologies (FMEA and FTA)
- Third-Party AI Risk Management
- Governance Maturity Models
- Risk Treatment Strategies
- Practical AI Risk Assessment Case Study

## Module 8 Data Governance for AI

- Data Strategy for AI
- Data Governance Policy
- Data Quality, Data Gathering
- Data Lifecycle
- Data Cleansing and Data Labelling
- Data Privacy and Security, Data Ethics
- Data Validation
- Data Lifecycle Management for AI Projects
- Data Collection, Processing, Storage, And Use for AI Systems
- Data Exfiltration
- Data Anonymization, Pseudonymization, and Differential Privacy Techniques
- Implementing Data Governance Frameworks for AI
- AI Data Security and Pets
- Case Study

## Module 9 AI on Cloud

- Cloud Computing Fundamentals for AI
- AI Hosting Models on Cloud
- Key considerations for choosing CSP for AI Workloads
- Leveraging Native Cloud Security for AI
- Shared Responsibility Matrix
- Integrating AI Governance into Cloud Infrastructure
- Reference architectures
- Case study

## Module 10 AI Security

- AI Threat Landscape
- Security Controls Across AI Lifecycle
- OWASP GenAI risks
- RAG security
- Model theft and data poisoning
- AI Red Teaming
- Incident Response for AI Systems

## Module 11 Auditing AI Systems

- AI Audit Frameworks and Standards
- Key Audit Areas and Techniques
- Audit planning
- Evidence collection
- Control validation
- AI assurance
- Audit reporting
- Continuous assurance
- Audit simulation
- Challenges in AI Auditing (Methodologies, Data Access)
- AI Audit Simulation Exercise

INFOSECTRAIN

## Module 12 SDLC for AI Systems

- SDLC Methodologies (Agile, DevOps, Waterfall)
- Secure AI SDLC
- Governance in Each SDLC Phase
- Planning, Design, Development, Testing, Deployment, Maintenance
- Change Management
- Model Retirement

INFOSECTRAIN

Educate. Excel. Empower.

## Contact us

www.infosectrain.com
sales@infosectrain.com

## Follow us on