

C|RAGE

**Certified Responsible AI Governance and Ethics
Certification Training**



Course Highlights



40-Hour LIVE
Instructor-Led
Training



Learn from Certified &
Industry-Experienced
Trainers



Career Guidance &
One-on-One
Mentorship



Hands-on Case
Studies & Practical
Applications



Flexible Schedule
with Live Sessions



Coverage of NIST AI
RMF & ISO/IEC
42001 Standards



Exam Preparation
& Mock
Assessments



Post-Training Support
from Subject Matter
Experts

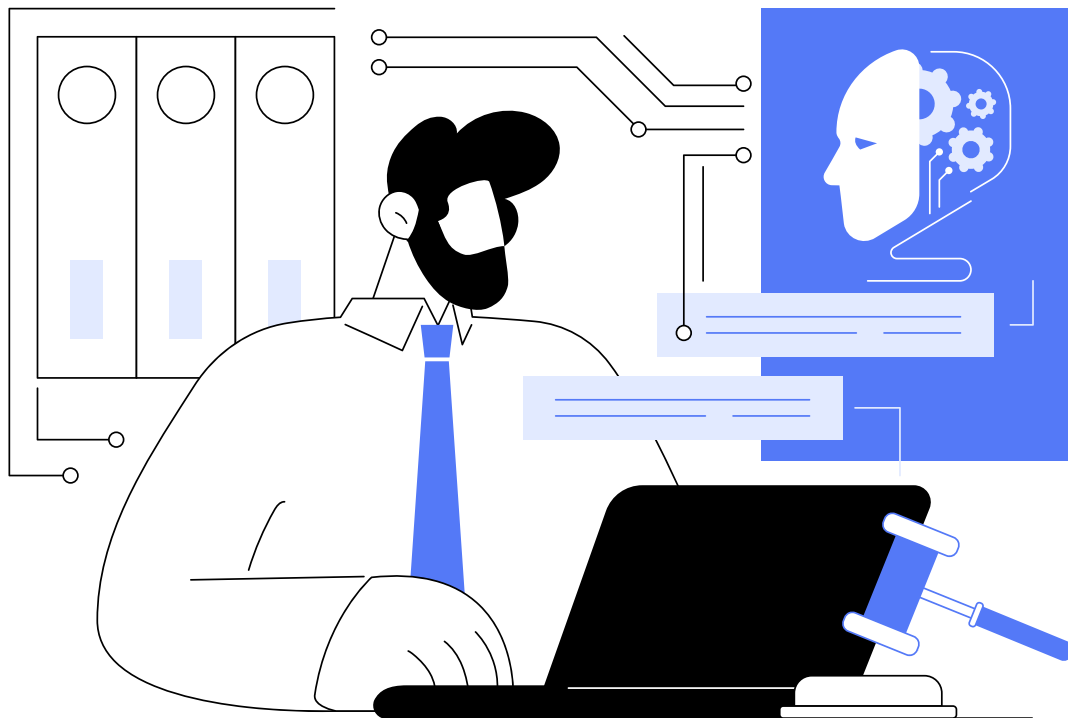


Access to Session
Recordings

About Course

InfosecTrain's **C|RAGE Certification Training** course is designed for professionals responsible for guiding AI initiatives with accountability and ethics. The course covers AI foundations, governance frameworks, ethical principles, regulatory compliance, risk management, and security controls.

By the end of the course, participants will be able to embed responsible AI practices across the AI lifecycle, manage third-party risks, ensure privacy and safety, and lead audit-ready AI programs. The course also prepares learners for the C|RAGE certification exam with practical insights and real-world case studies.



Course Objectives

After completing this training, you will be able to:

- ✔ Operationalize AI governance frameworks aligned with NIST AI RMF and ISO/IEC 42001 standards
- ✔ Lead AI governance initiatives and embed accountability across teams
- ✔ Implement ethical AI practices that ensure fairness, transparency, and explainability
- ✔ Conduct AI risk assessments, identify threats, and implement mitigation strategies
- ✔ Design and enforce AI security controls and privacy-by-design principles
- ✔ Ensure regulatory compliance across AI systems, including audit readiness
- ✔ Evaluate and manage third-party AI vendors and supply chain risks
- ✔ Build AI incident response plans and business continuity procedures
- ✔ Develop audit-ready AI assurance, testing, and validation processes
- ✔ Enhance organizational trust in AI systems by integrating privacy, safety, and ethical safeguards

Target Audience

- ✓ Head of Governance, Risk & Compliance (GRC)
- ✓ GRC Manager
- ✓ Head of Enterprise Risk Management (ERM)
- ✓ Operational Risk Manager
- ✓ Risk and Compliance Managers
- ✓ DPOs and Chief Privacy Officer
- ✓ Privacy Program Manager
- ✓ Data Governance Manager
- ✓ Regulatory Compliance Manager
- ✓ Internal Audit Manager (Technology/IT)

Pre-Requisites

- ✓ 3 years of cybersecurity experience

Exam Details

Certification Name	Certified Responsible AI Governance & Ethics Professional (C RAGE)
Exam Code	612-51
Exam Format	Multiple-Choice Questions
Number of Questions	100
Exam Duration	180 Minutes
Exam Language	English
Exam Availability	ECC Exam Portal

Note: To maintain the quality and fairness of certification exams, the exams are offered in multiple sets with different question banks. Each question is assigned a difficulty rating, which helps determine the passing score, also known as the “cut score.” Since some exam sets may be slightly more difficult than others, the cut score is determined separately for each set to ensure fair evaluation standards. Therefore, the passing score can range from 70% to 80%, depending on the exam version taken.

Course Content

Module 1 AI Foundations and Technology Ecosystem

- ✓ Understand core principles, evolution, and components of AI
- ✓ Apply real-world AI applications across industries
- ✓ Apply the AI project life cycle, MLOps, and DataOps
- ✓ Apply AI technology stack, infrastructure, and deployment models

Module 2 AI Concerns, Ethical Principles, and Responsible AI

- ✓ Understand key ethical, societal, privacy, and security concerns in AI
- ✓ Understand fundamental AI ethics principles and global standards
- ✓ Apply Responsible AI usage practices for safe and accountable AI
- ✓ Apply the Responsible AI development life cycle and governance integration

Module 3 AI Strategy and Planning

- ✓ Set an AI vision and assess organizational readiness
- ✓ Prioritize use cases and develop an AI roadmap
- ✓ Modernize data, technology, and infrastructure
- ✓ Manage AI pilots, scaling strategies, culture, and performance

Module 4 AI Governance and Frameworks

- ✓ Understand AI governance concepts, operating models, and roles
- ✓ Define AI governance policies, decision rights, and controls
- ✓ Apply global AI governance frameworks and life cycle governance
- ✓ Manage AI asset management, documentation, human oversight, and tooling

Module 5 AI Regulatory Compliance

- ✓ Understand global and sector-specific AI regulatory requirements
- ✓ Understand accountability, liability, and user rights in AI systems
- ✓ Apply operational compliance, reporting, and audit readiness
- ✓ Implement continuous compliance monitoring and legal risk management

Module 6 AI Risk and Threat Management

- ✓ Understand the AI threat landscape, vulnerabilities, and adversarial attacks
- ✓ Apply AI risk identification, assessment, and prioritization methods
- ✓ Apply AI risk management frameworks and standards
- ✓ Conduct threat modeling and attack surface analysis for AI systems

Module 7

Third-Party AI Risk Management and Supply Chain Security

- ✓ Understand third-party AI risk categories and supply chain threats
- ✓ Conduct AI vendor due diligence, evaluation, and contract governance
- ✓ Apply regulatory obligations and vendor compliance requirements
- ✓ Implement continuous vendor monitoring, assurance, and incident response

Module 8

AI Security Architecture and Controls

- ✓ Understand AI security architecture principles and frameworks
- ✓ Apply secure AI design patterns and defense-in-depth strategies
- ✓ Implement secure coding, model protection, and deployment controls
- ✓ Apply runtime security, API protection, and continuous monitoring

Module 9

Building Privacy, Trust, and Safety in AI Systems

- ✓ Understand privacy-enhancing technologies and data protection techniques
- ✓ Apply AI privacy risk assessment and mitigation strategies
- ✓ Apply transparency, explainability, and trust-building mechanisms
- ✓ Implement ethical design, fairness assurance, and trust monitoring

Module 10 AI Incident Response and Business Continuity

- ✓ Understand AI-focused incident response frameworks and workflows
- ✓ Conduct AI incident detection, containment, recovery, and reporting
- ✓ Develop AI business continuity and disaster recovery planning
- ✓ Apply testing, simulations, and continuous readiness improvement

Module 11 AI Assurance, Testing, and Auditing

- ✓ Understand AI assurance principles, frameworks, and governance models
- ✓ Apply AI testing strategies across data, models, and systems
- ✓ Conduct validation, verification, bias, fairness, and robustness testing
- ✓ Apply AI auditing methodologies, evidence management, and reporting



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

