



## CRAGE – Certified Responsible AI Governance & Ethics (e-Learning)

EC-Council

Com certificação

- **Nível:**
- **Duração:** 18h

---

### Sobre o curso

[Spring Deals: Cursos EC-Council com 5% de desconto até 30 de abril](#)

**Be EN-RAGED by the Chaos. Lead the Mandate for Responsible AI Governance.**

Enterprises need leaders who can embed governance throughout the AI life cycle, from ideation to deployment. This credential validates your ability to operationalize governance aligned with NIST AI RMF and ISO/IEC 42001, helping enterprises scale AI with accountability.

- 11 Comprehensive Modules
- Framework-Driven, Regulation-Aligned Curriculum
- Scenario-Based Governance and Risk Analysis

#### **What is the CRAGE certification?**

CRAGE (Certified Responsible AI Governance & Ethics) trains governance professionals to lead AI oversight, ensure compliance, and build audit-ready programs. It's aligned with the 'Govern' pillar of the ADG framework and prepares leaders to own responsible AI governance across the full AI life cycle.

#### **Enterprises Need Certified AI Governance Professionals**

AI is moving from experimentation to infrastructure. Enterprises need leaders who can embed governance throughout the AI life cycle, from ideation to deployment, so they can scale AI with accountability and meet regulatory requirements.

When AI fails, leadership is accountable.

CRAGE certifies professionals who can stand behind AI decisions.

## The Problem

AI governance gaps expose organizations to regulatory, reputational, and operational risks. Without certified governance professionals, enterprises deploy AI without accountability.

- No verified AI governance skills in the market
- Organizations deploy AI without accountability
- Audit failures waiting to happen

## CRAGE Credential Validates

The CRAGE certification equips you to lead AI governance end-to-end, from policy design to audit readiness. Master compliance frameworks, risk management, and ethical oversight.

- Validate your ability to embed governance across the AI life cycle
- Verify skills in building audit-ready programs from ideation to deployment
- Prove you can help enterprises scale AI with accountability

**Nearly 80% of organizations deploy AI without a defined governance** owner or operating model\*.

Regulations are tightening. They need professionals with verified skills to build audit-ready programs.

**This credential validates the governance skills** organizations desperately need; professionals who can own AI accountability, compliance, and risk management.

*Source: McKinsey Global AI Survey*

The CRAGE program equips you with comprehensive expertise across AI governance, risk management, and ethical oversight, from regulatory compliance to organizational accountability.

You'll learn to design, implement, and manage AI governance frameworks that ensure regulatory compliance, mitigate risks, and build stakeholder trust across the enterprise.

---

## Destinatários

CRAGE is designed for CISOs, GRC professionals, Data Protection Officers, AI Program Managers, Internal Auditors, and anyone responsible for AI governance, compliance, or policy in their organization.

#### **Who is CRAGE Ideal For**

##### **GRC & Risk Management**

Head of Governance, Risk & Compliance (GRC)  
GRC Manager  
Director, Risk Management  
Risk Manager  
Head of Enterprise Risk Management (ERM)  
Operational Risk Manager

##### **Compliance & Regulatory**

Director, Compliance  
Compliance Manager  
Director, Regulatory Affairs  
Regulatory Compliance Manager

##### **Privacy & Data Governance**

Chief Privacy Officer  
Director of Privacy  
Privacy Program Manager  
Data Protection Officer (DPO)  
Data Governance Manager  
Director, Data Governance

##### **Audit**

Internal Audit Manager (Technology / IT)  
Technology Audit Manager  
Director, Internal Audit

---

## Pré-requisitos

### **Do I need technical AI experience?**

CRAGE is designed for governance professionals, not technical practitioners. You'll learn enough about AI technology to govern it effectively, but the focus is on frameworks, compliance, and accountability.

---

## Metodologia

### Is this certification theoretical or operational?

**CRAGE is implementation-focused and audit-oriented.** It prepares professionals to design, document, operate, and defend AI governance programs in real enterprise environments, including accountability mapping, regulatory alignment, evidence generation, and assurance readiness.

### Is the CRAGE certification recognized globally?

Yes, CRAGE is designed for global relevance and aligns with international AI governance, risk, and compliance frameworks, including widely adopted standards and regulatory expectations across regions.

---

## Programa

- AI Foundations and Technology Ecosystem
- AI Concerns, Ethical Principles, and Responsible AI
- AI Strategy and Planning
- AI Governance and Framework
- AI Regulatory Compliance
- AI Risk and Threat Management
- Third-Party AI Risk Management and Supply Chain Security
- AI Security Architecture and Controls
- Building Privacy, Trust, and Safety in AI Systems
- AI Incident Response and Business Continuity
- AI Assurance, Testing, and Auditing

### AI Foundations and Technology Ecosystem

- AI assurance principles, frameworks, and governance models
- AI testing strategies across data, models, and systems
- Validation, verification, bias, fairness, and robustness testing
- AI auditing methodologies, evidence management, and reporting

### AI Concerns, Ethical Principles, and Responsible AI

- Key ethical, societal, privacy, and security concerns in AI
- Fundamental AI ethics principles and global standards
- Responsible AI usage practices for safe and accountable AI
- Responsible AI development lifecycle and governance integration

### AI Strategy and Planning

- AI vision setting and organizational readiness assessment
- Use-case prioritization and AI roadmap development
- Data, technology, and infrastructure modernization
- AI pilots, scaling strategies, culture, and performance management

### **AI Governance and Framework**

- AI governance concepts, operating models, and roles
- AI governance policies, decision rights, and controls
- Global AI governance frameworks and lifecycle governance
- AI asset management, documentation, human oversight, and tooling

### **AI Regulatory Compliance**

- Global and sector-specific AI regulatory requirements
- Accountability, liability, and user rights in AI systems
- Operational compliance, reporting, and audit readiness
- Continuous compliance monitoring and legal risk management

### **AI Risk and Threat Management**

- AI threat landscape, vulnerabilities, and adversarial attacks
- AI risk identification, assessment, and prioritization methods
- AI risk management frameworks and standards
- Threat modeling and attack surface analysis for AI systems

### **Third-Party AI Risk Management and Supply Chain Security**

- Third-party AI risk categories and supply chain threats
- AI vendor due diligence, evaluation, and contract governance
- Regulatory obligations and vendor compliance requirements
- Continuous vendor monitoring, assurance, and incident response

### **AI Security Architecture and Controls**

- AI security architecture principles and frameworks
- Secure AI design patterns and defense-in-depth strategies
- Secure coding, model protection, and deployment controls
- Runtime security, API protection, and continuous monitoring

### **Building Privacy, Trust, and Safety in AI Systems**

- Privacy-enhancing technologies and data protection techniques

- AI privacy risk assessment and mitigation strategies
- Transparency, explainability, and trust-building mechanisms
- Ethical design, fairness assurance, and trust monitoring

### **AI Incident Response and Business Continuity**

- AI-focused incident response frameworks and workflows
- AI incident detection, containment, recovery, and reporting
- AI business continuity and disaster recovery planning
- Testing, simulations, and continuous readiness improvement

### **AI Assurance, Testing, and Auditing**

- AI assurance principles, frameworks, and governance models
- AI testing strategies across data, models, and systems
- Validation, verification, bias, fairness, and robustness testing
- AI auditing methodologies, evidence management, and reporting