Certified Responsible AI Governance & Ethics (CRAGE)

Category: AI, Data & Analytics | **Vendor:** EC-Council

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Certified Responsible AI Governance & Ethics (CRAGE)
Related Exam:	CRAGE

Who Should Attend

GRC (Governance, Risk & Compliance) Leaders, Risk Managers / Enterprise Risk Professionals; Compliance Officers / Regulatory Specialists, Data Privacy Officers (DPOs), Internal Auditors (IT / Technology)

Prerequisites & Entry Requirements

General Prerequisites:

Recommended experience 3 years of cybersecurity or related experience recommended experience in risk, compliance, or governance

Detailed Course Outline

Module 01: AI Foundations and Technology Ecosystem

- Explain the foundational principles, evolution, and core components of Artificial Intelligence
  - Artificial Intelligence (AI)
  - Benefits and Limitations of AI
  - Evolution of AI
  - What is Machine Learning?
  - Machine Learning Algorithms
  - Limitations of Machine Learning
  - Neural Networks
  - Layers, Nodes, and Weights in Neural Networks
  - Deep Learning (DL)
  - How DL Overcomes Limitations of ML
  - Working of DL
  - DL Algorithms
  - Computer Vision
  - Natural Language Processing (NLP)
  - Why NLP is Important in AI
  - How NLP Processes Human Language
  - Processing Text for NLP Tasks
  - Key NLP Tasks
  - Sentiment Analysis in NLP
  - Text Summarization in NLP
  - Language Translation in NLP
  - Challenges in NLP
  - What is Generative AI?
  - Traditional AI vs Generative AI
  - Foundation Models of Generative AI
  - Popular GenAI Tools
  - Large Language Models (LLMs)
  - Small vs. Large Language Models
  - Key Terms for GenAI and Language Models

Emerging Trends in AI
    - Technological Advancements Driving AI
    - The Road Ahead: Opportunities and Challenges

- Identify real-world applications of AI across industries and their transformative impact
    - AI Applications

- Understand the AI project lifecycle and the role of MLOps and DataOps in operationalizing AI solutions
    - Data Operations (DataOps) in AI Technology Stack
    - AI Development and Operations (MLOps) Lifecycle
    - AI Project Lifecycle Phases and Gates
    - Initiation and Concept Development
    - Data Collection and Preparation
    - Model Development and Experimentation
    - Model Training, Validation, and Testing
    - Deployment and Release Management
    - Monitoring and Performance Tracking
    - Maintenance and Model Retraining Schedules
    - Retirement and Decommissioning Procedures
    - Post-deployment Evaluation and Success Metrics
    - Version Management and Rollback Procedures
    - Integration of DataOps, MLOps, and DevSecOps in AI

- Describe the key layers, tools, and infrastructure that form the AI technology ecosystem
    - AI Technology Stack
    - Data Infrastructure and Pipelines
    - Model Architectures and Algorithms
    - Computing Resources and Infrastructure
    - APIs and Integration Layers
    - Monitoring and Observability Systems
    - Version Control and Model Registries

Cloud Computing and Infrastructure for AI Systems

- Edge vs. Cloud Deployment Considerations
- Data Science and Analytics as AI Enablers
- Scalability, Performance, and Computational Requirements
- Integration with Existing IT Systems and Legacy Infrastructure
- Module Summary

Module 02: AI Concerns, Ethical Principles, and Responsible AI

- Identify key concerns associated with AI and understand their implications
  - Concerns, Challenges, and Implications with AI
  - AI Concerns
  - AI Ethical Concern: Bias and Discrimination
  - AI Ethical Concern: Lack of Transparency
  - AI Ethical Concern: Accountability and Responsibility
  - AI Ethical Concern: Intellectual Property and Copyright Violations
  - Ethical Concerns Introduced by GenAI
  - Privacy and Security Concern: Privacy and Surveillance
  - Real-world Privacy and Data Protection Implications
  - Privacy and Security Concern: Phishing with AI-Generated Messages
  - Privacy and Security Concern: Scamming through AI-Generated Deepfakes
  - Societal Concern: Job Displacement
  - Societal Concern: Mental Health Impact
  - Societal Concern: Hallucinations
  - Societal Concern: Misinformation
  - Long-Term Concerns: Autonomous Weapons
  - Long-Term Concerns: Emergence of AGI
- Explain the fundamental ethical principles that guide the responsible and fair development and use of AI systems
  - AI Ethics
- Describe major global AI ethics standards and frameworks and understand how they inform ethical governance
  - OECD
  - UNESCO
  - IEEE
  - DoD AI Ethical Principles

Module 03: AI Strategy and Planning

- Explain the purpose and importance of AI strategy and planning in guiding responsible and value-driven AI adoption
  - AI Strategy and Planning
  - The Need for an AI Strategy
  - AI Strategy and Planning Components
- Develop the ability to design a clear AI vision and assess organizational readiness across data, technology, skills, and culture
  - Setting an AI Vision
  - Crafting and Communicating AI Vision
  - Aligning AI With Business Goals
  - Assessing Organizational Readiness
  - Data Maturity Assessment
  - ROI Assessment for AI
  - AI Maturity Models and Organizational Readiness Assessment
- Learn to identify high-value AI opportunities and prioritize them using structured criteria to build an effective AI roadmap
  - Building Use Cases for AI Investment
  - Use Case Identification and Prioritization
  - Creating an AI Use-Case Portfolio
  - Creating an AI Roadmap
- Understand how to modernize data ecosystems and AI infrastructure to support scalable, secure, and production-ready AI systems
  - Technology Selection and Evaluation
  - Technology Selection and Evaluation Criteria
  - Building Data Strategy for AI
- Design, run, and evaluate AI pilots to validate feasibility, performance, business value, and associated risks
  - Purpose of the Pilot Phase
  - Steps in Pilot Development

Pilot Evaluation Criteria

- Pilot Outcomes and Decision Making

Module 04: AI Governance and Frameworks

- Understand the concept, scope, purpose, and foundational need for AI governance within organizations
  - What Is AI Governance?
  - AI Governance Hierarchy?
  - Why AI Governance is Needed
  - Scope of AI Governance
  - Traditional IT Governance vs. AI Governance
  - Governance vs. Management vs. Compliance
- Understand how AI governance roles, committees, and operating structures collaborate to manage and oversee AI initiatives
  - AI Governance Operating Model
  - AI Governance Structure
  - AI Governance Meeting Frequency
- Identify key governance roles across the AI lifecycle and understand their responsibilities in ensuring accountable AI operations
  - Key AI Governance Roles
  - Cross-Functional Collaboration Requirements
  - Chain of Responsibility and Escalation
- Understand the policy framework and decision-making authority required to establish structured, controlled, and transparent AI governance
  - Governance Policies
  - Decision Rights Matrix
  - Define AI Policy Goals and Objectives
  - AI Policy Implementation Challenges
  - AI Governance Policies
  - Model Development Policies
  - AI Usage Policies
  - Bias Mitigation Policies
  - AI Lifecycle Management Policies

    - Policy on Ethics Review Boards and AI Audits
    - Continuous Review and Adaptation of Policies
- Compare various AI governance models and understand how organizations choose and implement the right model for their ecosystem
    - AI Governance Models
    - Ethical AI Governance
    - Best Practices for AI Governance Models
- Understand major global AI governance frameworks and their principles to guide responsible and trustworthy AI adoption
    - OECD AI Principles for Governance
    - EU AI Act for Governing AI
    - The AIGA AI Governance Framework
    - IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems
    - The Montreal Declaration of Responsible AI
    - Choose a Governance Framework to Guide your Process
- Understand how governance is applied across the AI model lifecycle to ensure transparency, quality, and controlled evolution
    - Model Lifecycle Governance
    - Problem De?nition Governance
    - Design Governance
    - Data Preparation Governance
    - Training Governance
    - Evaluation Governance
    - Deployment Governance
    - Monitoring Governance
    - Change Control Governance
    - Retirement Governance
- Understand how managing AI assets ensures proper ownership, tracking, and governance across the AI lifecycle

The Role of Asset Management in Governance
    - AI Asset Management
    - Governance for AI Assets
    - Categories of AI Assets
    - Key Elements of AI Asset Management
    - AI Asset Inventory and Classification
    - Dataset Lifecycle Management
    - Model Lifecycle Management
    - Role of Model Cards in Asset Management
    - Metadata and Lineage Tracking
    - Performance Monitoring and Asset Health Tracking
    - Documentation, Versioning, and Auditability
    - Asset Versioning Best Practices
- Understand the role of documentation, transparency mechanisms, and stakeholder engagement in AI governance
    - Importance of Documentation in AI Governance
    - Governance Playbook
    - Stakeholder Engagement
    - Stakeholder Mapping
    - Emphasize Training and Awareness for All Stakeholders
    - Integrating Third-Party Oversight in AI Governance
- Understand the importance of human oversight in AI systems and how escalation, intervention, and review processes ensure trustworthy outcomes
    - Human Oversight
    - Human Oversight Escalation Framework
    - Decision Intervention Protocols
    - Human Review Checklists
    - Sample Human Review Checklist
    - Oversight Workflows

Identify key tools and platforms that support AI governance through model tracking, documentation, and workflow automation
    - Governance Tools
    - Model Registry
    - Experiment Tracking Tools
    - Documentation Portals
    - Governance Automation Tools
- Understand how organizations implement AI governance frameworks and integrate them with broader technology governance mechanisms
    - Implementing AI Governance Frameworks
    - Integrating AI Governance
    - Integration of AI Governance with IoT, Blockchain, and 5G
    - Integration of AI Governance with Other Technologies
- Recognize key challenges in AI governance and apply best practices to strengthen governance maturity and effectiveness
    - Governance Challenges
    - Governance Best practices
    - Module Summary

Module 05: AI Regulatory Compliance

- Explain the purpose of AI regulatory compliance and understand its organizational benefits and challenges
  - AI Compliance Management
  - Benefits and Challenges of AI Compliance
  - Components of an AI Compliance Program
- Describe major global and regional AI regulations, including their requirements, risk classifications, and data protection obligations
  - EU AI Act and Regulatory Classifications
  - U.S. Regulatory Frameworks and Guidelines
  - Global Data Protection Regulations
  - Emerging Regulatory Trends by Region
- Identify key AI compliance requirements across critical sectors such as healthcare, ?nance, justice, telecommunications, education, and transportation
  - Need for Sector-Specific AI Regulations
  - Healthcare AI Compliance
  - Financial Services Compliance
  - Criminal Justice System Compliance
  - Telecommunications Compliance
  - Education Sector Compliance
  - Transportation/Autonomous Systems Compliance
- Understand how accountability, liability, and user rights shape legal duties and safeguard individuals in AI-driven systems
  - Why Accountability, Liability, and Rights Matter
  - Consumer Protection
  - Algorithmic Accountability
  - Intellectual Property Rights (IPR)
  - Liability and Responsibility Frameworks
  - Right to Explanation
  - Explainability and Interpretability Requirements

Explain operational compliance expectations, including record-keeping, reporting, contractual requirements, labor considerations, and incident response obligations
    - Operational Compliance
    - Employment and Labor Law Considerations
    - Contractual Compliance Clauses
    - Record-keeping Requirements
    - Reporting and Notification Procedures
    - Legal Incident Response
    - Whistleblower Protections
- Apply continuous compliance practices such as audits, monitoring, regulatory change management, and third-party verification to maintain alignment with evolving AI regulations
    - Compliance Assessment and Gap Analysis
    - Maintain Audit Trails and Monitoring Systems
    - Regulatory Change Management
    - Compliance Training and Certification
    - Third-party Compliance Verification
    - Remediation and Corrective Actions
    - AI Compliance Management Tools
- Evaluate legal risks across the AI lifecycle and understand mechanisms such as insurance, indemnification, and dispute resolution for effective risk mitigation
    - Legal Risks Management
    - Legal Risks in AI Lifecycle
    - Role of Insurance in AI Risk Management
    - Role of Indemnification in Legal Risk Management
    - Best Practices for Implementing Insurance and Indemnification
    - Dispute Resolution
    - Litigation Preparedness
    - Legal Holds and e-Discovery Readiness
    - Best Practices for AI Legal Holds

- AI Legal Governance Strategies
- Module Summary

Module 06: AI Risk and Threat Management

- Identify and explain the key risks, threats, attacks, and vulnerabilities associated with AI systems
  - Threat Landscape for AI Systems
  - Common Vulnerabilities in AI Systems
  - Adversarial Attacks
- Understand and apply core AI risk assessment techniques for identifying, analyzing, and prioritizing AI-related risks
  - AI Risk Assessment
  - Risk Identification
  - Key Techniques for Risk Identification
  - Risk Identification Tools
  - Role of KPIs and KRAs in AI Risk Identification
  - Failure Modes and Effects Analysis (FMEA)
  - Monte Carlo Simulation
  - Bow-Tie Analysis
  - Risk Assessment Tools
  - Risk Scoring and Prioritization Methods
  - Likelihood and Impact Matrix
  - Quantitative vs. Qualitative Risk Analysis
  - Establishing Risk Thresholds and Tolerance Levels
  - Continuous Risk Monitoring Systems
  - Data Drift Detection Techniques
  - Model Performance Tracking
  - Anomaly Detection Techniques
  - Risk Dashboards
  - Reporting
  - Escalation Procedures
  - Risk Communication Strategies
  - Risk Escalation Best Practices
- Describe major AI risk management frameworks and principles used to guide safe, compliant, and

responsible AI deployment
    - AI Risk Management Frameworks
    - NIST AI Risk Management Framework (AI RMF)
    - AI Risk Frameworks: ISO/IEC 42001
    - AI Risk Frameworks: ISO/IEC 23894
    - OECD AI Principles for Risk Evaluation
- Explain how threat modeling and attack surface analysis support effective identification and mitigation of AI-specific threats
    - Threat Modeling
    - Attack Surface Analysis
    - Module Summary

Module 07: Third-Party AI Risk Management and Supply Chain Security

- Understand the importance of third-party AI risks and how vendor dependencies can impact business operations, security, compliance, and organizational accountability.
  - Why Third-Party AI Risk Matters
  - Key Risks in Vendor Relationships
  - Organizational Responsibility for AI Systems
  - Types of Third-Party AI Vendors
  - Complex AI Supply Chains Increase Third-Party Risk
  - Business Impact of Poor Vendor Risk Management
- Learn how to apply a structured TPRM framework to identify, assess, mitigate, and monitor risks associated with third-party AI vendors
  - Third-Party AI Risk Management (TPRM)
  - TPRM Framework
  - TPRM Tools
- Understand regulatory obligations and legal responsibilities organizations must meet when procuring or deploying third-party AI systems
  - Regulations Affect Vendor Selection
  - Organizations Obligations Under AI Regulations
  - Vendor Compliance Alignment
  - Legal Responsibility for Vendor AI Systems
- Learn the end-to-end procurement lifecycle for selecting, evaluating, contracting, and deploying AI vendor solutions
  - Stages of AI Procurement
  - Executive Role in Procurements
  - Key Questions Before Choosing a Vendor
  - Criteria for Shortlisting Vendors
- Develop the ability to evaluate vendor maturity, trustworthiness, technical capabilities, and risk posture through comprehensive due-diligence processes
  - Vendor Due Diligence
  - Building a Comprehensive Vendor Inventory

Vendor Role Mapping
    - Risk Profiling and Categorization
    - Evaluate Vendor Maturity to Mitigate AI Risks
    - Areas to Examine in Due Diligence
    - Technical Evaluation of Vendor AI
    - Data Handling Evaluation
    - Responsible AI and Ethics Evaluation
    - Legal and IP Evaluation
    - Vendor Performance Tracking Using KPIs and KRIs
    - KRAs and KPIs Best Practices
    - Red Flags Requiring Caution
    - Supplier Due Diligence Best Practices
- Understand how to create effective AI vendor contracts that include appropriate clauses for data rights, security, AI-specific risks, SLAs, and liability allocation
    - Contracts in AI Vendor Relationships
    - Data Rights and Control Clauses
    - Security and Privacy Clauses
    - AI-Specific Risk Clauses
    - High-Risk Use Case Clauses
    - Drafting SLAs and SLOs
    - Best Practices for Drafting SLAs and SLOs
    - Best Practices for AI Vendor Contracts
    - Liability Allocation and Risk Sharing in AI Contracts
    - Best Practices for Liability Allocation and Risk Sharing
- Learn how to continuously monitor AI vendors through KPIs, KRIs, audits, assurance activities, and structured lifecycle oversight mechanisms
    - Monitoring and Lifecycle Oversight in AI Vendor Risk Management
    - Continuous Monitoring Expectations
    - Executive Reporting Dashboard Items

Ongoing Review Requirements
    - Assurance Requirements
    - Independent Validation and Testing for Vendor Assurance
    - Best Practices for Vendor Assurance and Independent Validation
    - Incident Response Expectations
    - Responsible Offboarding and Exit Strategy
    - Vendor Renewal Decision-Making
    - Integration of Compliance, Performance, and Risk in Vendor Renewal
    - Aligning Vendor Oversight with Enterprise Risk
- Analyze real-world AI vendor failures to understand common gaps in governance, oversight, contracts, and risk monitoring
    - Case Study: Vendor Misused Customer Data
    - Case Study: Biased Hiring Algorithm
    - Case Study: Hallucinated Financial Analysis
    - Executive Scenario Challenge
    - Module Summary

Module 08: AI Security Architecture and Controls

- Understand the core principles of AI security architecture and how they ensure the protection and resilience of AI systems throughout their lifecycle
  - AI Security Architecture
  - Why Security Architecture Matters in AI
  - AI Security Architecture Principles
  - Traditional Security V/s AI Security Architecture
  - Components of AI Security Architecture
  - Governance Practices for AI Security Architecture
  - Secure Software Development Lifecycles (SDLC)
  - Threat Modeling for AI Systems
  - AI Threat Modeling Frameworks
  - Threat Modeling Use Cases
  - Zero Trust Security
  - Infrastructure Hardening
  - Model Training
  - Inference Controls
  - Continuous Testing
  - Monitoring, Detection and Response
  - Best Practices in AI Security Architecture
- Explore various frameworks used in AI security architecture, including their role in securing AI models, data, and infrastructure
  - AI Security Architecture Frameworks
  - Cloud Security Alliance (CSA) AI Security Framework
  - Artificial Intelligence Controls Matrix (AICM) Framework
  - OWASP AI Security Top Ten
- Learn the critical design considerations for building secure AI architectures that effectively address potential vulnerabilities and threats
  - Secure Design Patterns for AI
  - Designing Defense-in-Depth Strategies for AI

Designing Layered Approach for Secure AI Systems
    - Security by Design

- Identify and implement best practices in AI system development to ensure robust security measures from the design phase through deployment
    - Importance of Code Management
    - Code Management for Security in AI
    - Version Control
    - Version Control Best Practices
    - Repository Security and Access Controls
    - Secure Coding Best Practices
    - Secure Coding Standards
    - Code Review Processes

- Apply security best practices in AI model development to protect models from adversarial attacks, data poisoning, and other vulnerabilities
    - Model Security
    - Protecting Model Integrity
    - Tools for Protecting Model Integrity
    - Model Signing
    - Secure Model Serving

- Implement security controls and practices during the deployment phase of AI models to ensure safe operation and mitigate risks
    - Container Security
    - Container Security Controls
    - Memory and Resource Protection
    - Hardening AI Runtime Environments
    - Network Segmentation Controls
    - Rate Limiting and DDoS Protection
    - API Security for AI Systems
    - Best Practices for API Security in AI Systems

API Gateway Implementations

- Module Summary

Module 09: Building Privacy, Trust, and Safety in AI Systems

- o Building Privacy, Trust, and Safety in AI Systems
- Explain key privacy-enhancing techniques used to protect sensitive data in AI systems
  - Privacy by Design
  - Data Minimization
  - Differential Privacy
  - Decentralization
  - Data Protection: Encryption and Access Control
  - Data Anonymization and Pseudonymization
  - Data Retention and Deletion Policies
  - Secure Data Destruction Practices
  - Privacy-Preserving Analytics
- Assess AI-related privacy risks and apply appropriate mitigation methods
  - Evaluating Privacy Risks with Privacy Impact Assessments
  - Evaluate Privacy Risks with Risk Assessment Framework
  - Reducing Privacy Risk with De-Identification Techniques
- Implement transparency, trust-building, and safety controls to ensure reliable AI behavior
  - Incorporating Transparency with Consent Management
  - Ensuring Transparency with the Right to Explanation
  - Improving Transparency with Explainability Interfaces
  - Enhancing Transparency through Stakeholder Communication
  - Building Trust with User Feedback Loops
  - AI Trustworthiness and Safety Frameworks
  - Measuring and Scoring AI Trustworthiness
  - Maintaining Trust with Continuous Monitoring
  - Validating Trust with Verification Mechanisms
  - Assessing Trust with Third-Party Audits
  - Ensuring AI Safety with Testing and Red-Teaming
  - Defining Boundaries with AI Guardrails
  - Blocking Harmful Outputs with Content Filtering

Building Resilient AI Systems with Failure Handling

- Design user-centric AI interactions that improve usability, clarity, and trust
  - Principles of User-Centric AI Design
  - Empowering Users through Education and Awareness
  - Addressing User Concerns with Complaint Mechanisms
- Apply ethical guidelines and fairness practices to ensure safe and aligned AI development
  - Documenting AI Systems with Transparency Reports
  - Guiding Ethical AI Development with Decision Frameworks
  - Ensuring Fairness with Audits and Bias Assessment
- Evaluate and monitor AI systems to maintain trust, compliance, and consistent performance
  - Certifying Ethical AI with Certification and Attestation
  - Validating Compliance with Certification
  - Module Summary

Module 10: AI Incident Response and Business Continuity

- o AI Incident Response and Business Continuity
- Design structured, AI-focused incident response strategies and frameworks aligned with organizational and business impact needs
  - Understanding AI Incidents and Business Impact
  - AI-specific Incident Response
  - Limitations of Traditional IR in Managing AI Incidents
  - How AI Incident Response Supports Business Growth
  - Building an Effective AI-Specific IR Plan
  - Classifying AI Incidents for Effective Response
  - AI Incident Severity Levels
- Apply the AI incident response lifecycle to detect, contain, investigate, and recover from AI-related incidents effectively
  - Initial IR Actions
  - IR Lifecycle
  - Phase 1: Preparation
  - Phase 2: Detection
  - Phase 3: Analysis and Triage
  - Phase 4: Containment
  - Phase 5: Eradication
  - Phase 6: Recovery
  - AI-Specific IR Tools
  - AI-Specific IR Best Practices
- Evaluate and execute structured internal, external, regulatory, and customer communication strategies during AI incidents to maintain trust and compliance
  - Importance of Communication During an Incident
  - Internal Escalation Protocols
  - External Communication Protocols
  - Regulatory Notification Requirements for AI Incidents
  - Global Regulatory Notification Timelines

    - Effective Media and Public Communication for AI Incidents
    - Customer Notification Strategies for AI Incidents
- Assess AI incidents through post-incident reviews, metrics, and documentation to drive learning, accountability, and continuous improvement
    - Purpose of Post-Incident Review
    - Key Metrics for Post-Incident Review
    - Metrics to Measure IR Effectiveness
    - Post-Incident Documentation
    - AI Post-Incident Metrics and Analytics
    - Enhancing Training and Awareness After Incidents
    - Post-Incident Knowledge Base Update
    - Post-Incident Review Tools
- Develop AI-focused business continuity strategies by identifying critical AI functions, assessing business impact, and prioritizing recovery actions
    - AI Business Continuity
    - Key Components of an AI-Specific BC Strategy
    - Business Impact Analysis in AI-Specific BC
    - Identifying Critical Functions
    - Quantifying Impact
    - Recovery Prioritization
    - Recovery Tiers Matrix
    - Backup and Recovery Requirements
    - Backup and Recovery Best Practices
    - Redundancy and Failover Mechanisms
- Design AI-specific disaster recovery plans by defining recovery objectives, backup strategies, failover mechanisms, and supply chain dependencies
    - AI Disaster Recovery
    - DR Plan Dependencies
    - Defining Recovery Objectives for AI Systems

DR Site Options for AI Systems
    - Failover and Failback Procedures for AI Systems
    - Automation in AI-Specific DR
    - Backup Frequency and Retention in AI-Specific DR
    - Data Synchronization in AI Recovery
    - Ensuring AI Supply Chain Continuity
    - AI-Specific DR Tools
- Evaluate and enhance AI incident response and recovery readiness through testing, simulations, training, and continuous optimization activities
    - DR Testing for AI Systems
    - Key Testing Types in AI DR
    - Tabletop Exercises for AI-Specific DR Drills
    - Training in DR for AI Systems
    - Optimization in DR for AI Systems
    - Continuous Improvement During Recovery
    - Module Summary

Module 11: AI Assurance, Testing, and Auditing

- Establish AI assurance principles, mechanisms, and frameworks to support reliable, compliant, and accountable AI systems
  - AI Assurance
  - Key Components of AI Assurance
  - AI Assurance Mechanisms
  - Frameworks and Standards for AI Assurance
  - Case Studies: Successful AI Assurance Practices
- Apply structured AI testing strategies to evaluate data, models, system behavior, performance, robustness, and security across the AI lifecycle
  - Testing in AI
  - Why AI Testing is Different?
  - AI Test Planning
  - Objectives of AI Test Strategy
  - Key Components of AI Test Planning
  - Defining the Testing Scope
  - Testing Strategy
  - Risk-Based AI Testing Strategies
  - Functional Testing
  - Types of Functional Testing
  - Test Case Development
  - Testing Methodologies
  - Model Performance Testing
  - Model Stability and Consistency Testing
  - Edge Case Testing
  - Testing Overfitting and Underfitting Models
  - Testing Model Drift Over Time
  - Specialized Testing
  - User Acceptance Testing (UAT)
  - UAT Process
  - Challenges in AI UAT

    - Best Practices for AI UAT
    - Usability Testing
    - Accessibility Testing
    - User-Level Performance Testing
    - Scenario and Workflow Testing
    - Regression Testing
    - Security and Robustness Testing
    - Role of Red Teaming in AI Testing
    - Best Practices for Security Testing for AI Systems
    - Penetration Testing for AI Systems
    - Monitoring and Continuous Testing
    - AI Bug Bounty Programs
    - Tools and Technologies for Testing AI Models
- Conduct pre-deployment and post-deployment validation and verification of AI systems
    - Validation of AI Systems
    - Data Validation Strategy
    - Cross-Validation and Holdout Testing
    - Generalization and Transfer Learning Validation
    - Verification of AI Systems
    - Model Behavior Verification Techniques
    - Data Pipeline Verification Techniques
    - Integration Verification Techniques
    - Deployment and Operational Verification Techniques
    - Non-Functional Verification Techniques
    - Best Practices for AI System Verification
- Assess AI systems for vulnerabilities, bias, fairness, explainability, and transparency, and manage remediation
    - Vulnerability Management for AI Systems
    - Best Practices for Vulnerability Management for AI Systems
    - AI Security Patch Management

Best Practices for AI Security Patch Management
    - Bias and Fairness Assessment
    - Explainability and Transparency Assessment
- Perform structured AI audits using risk-based methodologies, evidence collection, and governance-aligned reporting practices
    - AI Auditing
    - Key Components of AI Auditing
    - AI Auditing Process
    - Audit Planning and Scope Definition
    - Audit Sampling and Evidence Collection

□□ Certification Path

Certified Responsible AI Governance & Ethics (CRAGE)

Exam: CRAGE

Frequently Asked Questions

Q: What delivery options are available for Certified Responsible AI Governance & Ethics (CRAGE)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Certified Responsible AI Governance & Ethics (CRAGE) course helps prepare you for the Certified Responsible AI Governance & Ethics (CRAGE) certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the CRAGE official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 3-day Certified Responsible AI Governance & Ethics (CRAGE) course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Certified Responsible AI Governance & Ethics (CRAGE) training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Certified Responsible AI Governance & Ethics (CRAGE)?

Yes, we provide corporate training, dedicated training, and closed classes for Certified Responsible AI Governance & Ethics (CRAGE). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: Why choose Nexus Human for Certified Responsible AI Governance & Ethics (CRAGE)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Certified Responsible AI Governance & Ethics (CRAGE) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 14/11/2026.