www.logicalimagination.com
800.657.1494

AI Foundations & Risk for IT Professionals

Course #: AI-200 **Duration:** 1 day

Prerequisites

General technical literacy and familiarity with IT systems and enterprise environments. No prior AI implementation experience is required.

Details

This course establishes a shared foundation for IT teams tasked with supporting or implementing artificial intelligence in enterprise environments. Participants learn how modern AI systems behave, where they fail in production, and what risks they introduce across security, privacy, compliance, and operations.

Rather than focusing on tools or coding, the course emphasizes system behavior, failure modes, and governance considerations, equipping IT professionals to make informed decisions about when and how AI should be introduced into organizational systems.

After attending this course, students should be able to:

Explain how modern AI and large language model–based systems operate at a systems level
Identify common technical, operational, and organizational risks associated with AI
Recognize AI failure modes that impact reliability, security, and trust
Evaluate where AI is appropriate—and inappropriate—in enterprise systems
Establish foundational governance and accountability principles for AI initiatives

This course is designed for IT professionals responsible for evaluating, supporting, securing, or governing AI-enabled systems, including those involved in architecture, security, compliance, and operations. This course is technical in orientation but does not require programming.

Software Needed

A laptop or desktop computer with a modern web browser and reliable internet access is recommended for accessing course materials and participating in discussions. No programming tools or AI software access is required.

Outline

AI Foundations & Risk for IT Professionals

- **Why AI Is an IT Concern**
  - How AI has shifted from experimentation to infrastructure
  - Differences between consumer AI tools and enterprise AI systems
  - Why AI adoption often bypasses IT governance
  - The evolving role of IT in AI-enabled organizations
- **How Modern AI Systems Behave**
  - Overview of machine learning and large language models

- Training vs inference in operational systems
  - Probabilistic outputs and non-deterministic behavior
  - Why AI systems behave differently than traditional software
- **Understanding AI Failure Modes**
  - Hallucinations and fabricated outputs
  - Inconsistent behavior across similar inputs
  - Overconfidence and false authority
  - Data leakage and context misuse
- **AI Risk Categories in Enterprise Environments**
  - Operational risk (reliability, supportability, maintenance)
  - Security risk (data exposure, prompt injection, misuse)
  - Compliance and regulatory risk
  - Reputational and trust risk
- **Security and Privacy Considerations**
  - What AI systems can "see" and access
  - Data boundaries, permissions, and exposure
  - Risks of external AI services
  - Managing sensitive, proprietary, and regulated data
- **Human Accountability and Governance**
  - Why AI does not eliminate responsibility
  - Decision authority vs decision support
  - Human-in-the-loop principles
  - Auditability and traceability
- **Evaluating AI Use Cases**
  - Identifying appropriate AI applications
  - Red flags for high-risk use cases
  - When AI adds value—and when it adds risk
  - Aligning AI use with organizational maturity
- **Preparing IT for AI Adoption**
  - Establishing shared language and expectations
  - Defining roles and responsibilities
  - Setting guardrails without blocking innovation
  - Coordinating across IT, security, legal, and business teams
- **Foundations for Responsible AI Systems**
  - Principles for safe and maintainable AI use
  - Early governance decisions that matter later
  - Preparing for workflow-based and agentic AI systems
  - Setting the stage for implementation and architecture training
- **Summary and Next Steps**
  - Key risk and behavior insights
  - Applying foundations in IT decision-making
  - Transitioning to AI workflow and architecture design
  - Preparing for hands-on implementation courses