Why should you take this course?

Practical considerations and instructor qualifications

Review:

Practical Considerations

- Get AIGP certified
- Pursue role in AI governance
- Round out resume
- Self-enrichment / professional development

Dr. David

- Pain points
  - Time
  - Money
  - Format
  - No prerequisites
- Uniquely qualified
  - Education
  - Experience

What is the AIGP?

Artificial Intelligence Governance Professional

Review (1):

What is the AIGP?

- Artificial Intelligence Governance Professional
- Certification provided by the IAPP

What do AIGP's do?

- Implement responsible AI practices
- Risk management
- Establish multi-stakeholder oversight body
- Monitor AI systems throughout life cycle
- Address issues such as bias, discrimination, privacy, misuse

Review (2):

Who should pursue the AIGP?

- AI compliance
- Risk management
- Legal and governance
- Data scientists
- AI project managers
- Model operations teams
- Social scientists
- Trust professionals

What does the AIGP cover?

- Foundations of AI governance
- How laws, standards, and frameworks apply to AI
- How to govern AI development
- How to govern AI deployment and use

Review (3):

How do I get certified?

- Prepare
- Register
- Pass
- Maintain

How is the exam structured?

- 100 questions
- Question format
- 3 hours, with optional 15-minute break
- Scored on scale from 100-500

What is the IAPP?

Privacy, AI governance, and digital responsibility

Review:

- IAPP
- KnowledgeNet Chapters

Why get AIGP certified?

Data from the last couple years supports need for AI governance professionals

Review (1):

Helen Toner

- Don't be intimidated by technology or the folks building it.
- Focus on adaptability, not certainty.

Dario Amodei

- AI will likely become the most powerful and strategic technology in history. By 2027, AI developed by frontier labs will likely be smarter than Nobel Prize winners across most fields of science and engineering.

Review (2):

Investment

- USD $175 billion globally awaiting investment in AI projects
- Microsoft to invest $80 billion in data centers in FY25
- GenAI companies: raised $56 billion (worldwide) in 2024
- Global data center spending predicted to reach $250 billion annually

Consumer protection

- 99% of Americans use at least one AI-enabled product, but 64% don't realize they're using AI
- 72% expect AI to negatively impact the spread of false information
- 64% believe AI will negatively affect social connections
- 60% think AI will negatively impact job opportunities

Review (3):

Business trends

- 98.4% of organizations are increasing AI and data investments

- 74.8% see value coming from productivity gains and customer service improvements

Impact on the workforce

- 80% of U.S. workers could have at least 10% of their work activities affected by LLMs

Review (4):

Career advancement

- Microsoft aims to train 2.5 million Americans in AI skills in 2025
- LinkedIn, "AI Consultant" 2nd fastest growing job in U.S.
- HBR, 84.3% have hired chief data/analytics officers, up from 12.0% in 2012
- HBR, 33.1% have chief AI officers

- Commitment to learning, self-improvement
- Demonstrates subject matter expertise
- Stand out from non-certificate holders

What is risk management?

The identification, assessment, and mitigation of risk

Review (1):

What is risk management?

- Identify, assess, mitigate harm
- Risk: potential harm
- Threat: delivers harm

Typical methodology

- Risk score = severity of harm * probability of occurrence

Review (2):

What is a control?

- Countermeasure or action designed to modify risk
- Three types
  - Administrative (e.g., training)
  - Technical (e.g., firewall)
  - Physical (e.g., locks, security guards)

Two examples

- Car accident
- Adversarial prompt

What is AI risk management?

Identification, assessment, and mitigation of AI risk

Review (1):

Alignment

- Organization's risk management strategies must be aligned

- May each have AI component, or

- Have separate AI strategy

AI RM strategy

- Identify, assess, mitigate risk

- Includes
  - Conduct risk assessment/analysis
  - Identify risks
  - Determine responsibility for mitigation/control implementation

Review (2):

Context

- Risk assessments are context-specific
  - E.g., FRT applications
- Consider
  - AI system owner, operator/deployer
  - Industry/sector
  - Use case
  - Social impacts
  - Timing
  - Jurisdiction(s)

Risk considerations

- Identify stakeholders
- AI's business purpose, planned usages
- Potential harms
- Training data (includes sensitive PII)
- Non-AI alternatives

Review (3):

Risk impact and response

- Typically identified as high, moderate, low
- High: avoid use system; modify system to prevent risk
- Moderate: mitigate risks
- Low: accept or mitigate as appropriate