COURSE OUTLINE

Module 1: Foundations of artificial intelligence

LESSON 1: CORE CONCEPTS OF AI - ***1.a.1/3 (10)***
LESSON 2 TYPES OF AL AND MACHINE LEARNING ***1.a.1, 4.a.2 (31)***
LESSON 3: THE AI TECHNOLOGY STACK *(48)*

Module 2: AI impacts on people and responsible AI principles

LESSON 1: AI HARMS AND RISKS ***1.a.2 (57)***
LESSON 2: PRINCIPLES AND APPLICATION OF TRUSTWORTHY AND RESPONSIBLE AI ***2.d.1, 1.a.4 (78)***

Module 3: Responsible AI governance and risk management

LESSON 1: ESTABLISHING AI STRATEGY ***1.b.4, 1.b.5, 1.c.1 (93)***
LESSON 2: ESTABLISHING AI GOVERNANCE ***1.b.1,2,3 (100)***
LESSON 3: AI RISK IDENTIFICATION AND MANAGEMENT ***2.d.2,3 (111)***

Module 4: Governing AI development

LESSON 1: GOVERNING THE PLANNING, DESIGNING AND BUILDING OF THE AI MODEL ***3.a.1-4 (126)***
LESSON 2: GOVERNING DATA COLLECTION AND USE IN AI DESIGN AND DEVELOPMENT ***3.b.1-2 (148)***

Module 5: Governing AI deployment

LESSON 1: KEY CONSIDERATIONS IN PLANNING FOR AI DEPLOYMENT
1.c.2, 4.a.3,3.a.2,3.a.3,4.b.4,1.c.3,4.b.3 (160-161)
LESSON 2: GOVERNING THE RELEASE, MONITORING AND MAINTENANCE OF THE AI MODEL
3.c.1,3.c.2, 3.c.3, 3.c.6, 4.c.5, 3.c.4, 4.c.7, 4.c.1, 3.c.5 (173-174)

Module 6: The EU AI Act

LESSON 1: INTRODUCTION TO THE EU AI ACT
LESSON 2: RISK CLASSIFICATION AND KEY REQUIREMENTS ***2.c.1, 2.c.2, 2.c.5, 2.c.3 (197)***
LESSON 3: ENFORCEMENT AND PENALTIES ***2.c.4 (216)***

Module 7: Other laws and standards related to AI

LESSON 1: AI-SPECIFIC LAWS, STANDARDS AND FRAMEWORKS ***2.d.4 (221)***
LESSON 2: HOW EXISTING DATA PRIVACY LAWS APPLY TO AI ***2.a (239)***
LESSON 3: OTHER TYPES OF EXISTING LAWS THAT APPLY TO AI ***2.b (252)***

THE AIGP BODY OF KNOWLEDGE

Domain I— Understanding the foundations of AI governance

Domain I — Understanding the foundations of AI governance focuses on what AI governance is, including the common principles and pillars to build an AI governance program. This domain cover best practices regardless of industry, sector or size.

I.A Understand what AI is and why it needs governance.

1. Know the generally accepted definitions and types of AI.
2. Identify the types of risks and harms posed by AI to individuals, groups, organizations and society (e.g., misalignment with objectives, ethics and bias risk, and complexity and scalability).
3. Identify the unique characteristics of AI that require a comprehensive approach to governance (e.g., complexity, opacity, autonomy, speed and scale, potential for harm or misuse, data dependency, and probabilistic versus deterministic outputs).
4. Identify and apply the common principles of responsible AI (e.g., fairness, safety and reliability, privacy and security, transparency and explainability, accountability and human-centricity).

I.B Establish and communicate organizational expectations for AI governance.

1. Define roles and responsibilities for AI governance stakeholders.
2. Establish cross-functional collaboration in the AI governance program (e.g., for efficacy and diversity of expertise and perspective).
3. Create and deliver a training and awareness program to all stakeholders on AI terminology, strategy and governance.
4. Differentiate approaches to AI governance based upon company size, maturity, industry, products and services, objectives and risk tolerance.
5. Identify differences among AI developers, deployers and users from a governance perspective (e.g., with respect to responsibilities, opportunities and needs).

I.C Establish policies and procedures to apply throughout the AI life cycle.

1. Create and implement policies to ensure oversight and accountability across all AI life cycle stages (e.g., use case assessment, risk management, ethics by design, data acquisition and use, model development, training and testing, deployment and monitoring, documentation and reporting and incident management).
2. Evaluate and update existing data privacy and security policies for AI.
3. Create and implement policies to manage third-party risk (e.g., procurement, supply chain and human resources).

Domain II — Understanding how laws, standards and frameworks apply to AI

Domain II — Understanding how laws, standards and frameworks apply to AI focuses on existing laws that apply to AI, as well as new AI-sp ecific laws, standards and frameworks.

II.A Understand how existing data privacy laws apply to AI.

1. Understand how notice, choice, consent, and purpose limitation requirements apply to AI.
2. Understand how data minimization and privacy by design requirements apply to AI.

3. Understand how obligations on data controllers apply to AI (e.g., regarding privacy impact assessments, use of third-party processors, cross-border data transfers, data subject rights, incident management, breach notification and record keeping).
4. Understand the requirements that apply to sensitive or special categories of data (e.g., biometrics).

II.B Understand how other types of existing laws apply to AI.

1. Understand how intellectual property laws apply to AI (e.g., prohibiting or limiting use of data for AI training).
2. Understand how non-discrimination laws apply to AI (e.g., in the employment, credit, lending, housing and insurance contexts).
3. Understand how consumer protection laws apply to AI (e.g., prohibiting unfair and deceptive acts or practices).
4. Understand how product liability laws apply to AI (e.g., prohibiting design or manufacturing defects).

II.C Understand the main elements ofthe EU AI Act.

1. Understand the risk classification framework for AI (i.e., prohibited AI, high-risk, limited-risk and minimal-risk) and what systems fall into each category.
2. Understand the key requirements for high-risk, limited-risk and minimal-risk AI including risk management, data governance, technical documentation, conformity assessment, record keeping, human oversight, transparency and notification, quality management (as applicable).
3. Understand the distinct requirements for general purpose AI models.
4. Understand the enforcement framework and penalties for non-compliance.
5. Understand the differences in requirements based on organizational context (e.g., providers, deployers, importers, and distributors).

II.D Understand the main industry standards and tools that apply to AI.

1. Understand the OECD principles, framework, policies and recommended practices for trustworthy AI.
2. Understand the NIST AI Risk Management Framework and Playbook (e.g., the core functions, categories and subcategories).
3. Understand the NIST ARIA program for methodologies, tools, metrics and measurements on AI safety.
4. Understand the core ISO AI standards (i.e., 22989 and 42001).

Domain III — Understanding how to govern AI development

Domain III — Understanding how to govern AI development focuses on the responsibilities of AI governance professionals with respect to designing, building, training, testing and maintaining AI models.

III.A Govern the designing and building of the AI model.

1. Define the business context and use case of the AI model.
2. Perform or review an impact assessment on the AI model.
3. Identify laws that apply to the AI model.
4. Apply the policies, procedures, best practices and ethical considerations to designing and building the AI model (e.g., purpose of AI, requirements gathering, architecture and model

selection, human oversight, data analysis, metric and threshold evaluation, stakeholder engagement and feedback and operational controls).
5. Identify and manage the internal and external risks and contributing factors related to designing and building the AI model (e.g., using probability/severity harms matrix, using a risk mitigation hierarchy, stakeholder mapping, use case evaluation, benchmarking, pre-deployment pilots and testing).
6. Document the designing and building process (e.g., to establish compliance and manage risks).

III.B Govern the collection and use of data in training and testing the AI model.

1. Establish and follow the requirements for data governance (e.g., assess and document lawful rights to collect and use data, and to assess data quality, quantity, integrity and fit-for-purpose).
2. Establish and document data lineage and provenance.
3. Plan and perform training and testing of the AI model (e.g., unit, integration, validation, performance, security, bias and interpretability).
4. Identify and manage issues and risks during training and testing of an the AI model.
5. Document the training and testing process (e.g., to validate results, establish compliance and manage risks).

III.C Govern the release, monitoring and maintenance of the AI model.

1. Assess readiness and prepare for release into production (e.g., creating the model card and satisfying conformity requirements).
2. Conduct continuous monitoring of the AI model and establish a regular schedule for maintenance, updates and retraining.
3. Conduct periodic activities to assess the AI model's performance, reliability and safety (e.g., audits, red teaming, threat modeling and security testing).
4. Manage and document incidents, issues and risks.
5. Collaborate with cross-functional stakeholders to understand why incidents arise from AI models (e.g., brittleness, lack of robustness, lack of quality data, insufficient testing, and model or data drift).
6. Make public disclosures with to meet transparency obligations (e.g., technical documentation, instructions for use to deployers, and post-market monitoring plans).

Domain IV — Understanding how to govern AI deployment and use

Domain IV: Understanding how to govern AI deployment and use focuses on the responsibilities of AI governance professionals with respect to selecting an AI model, then deploying and using it responsibly through on-going monitoring, maintenance, and other key obligations. This domain applies to any model typ e, such as a company deploying its own proprietary model or one from a third party.

IV.A Evaluate key factors and risks relevant to the decision to deploy the AI model.

1. Understand the context of the AI use case (e.g., business objectives, performance requirements, data availability, ethical considerations and workforce readiness).
2. Understand the differences in AI model types (e.g., classic vs generative, proprietary vs open source, small vs large, and language vs multimodal capabilities).
3. Understand the differences in AI deployment options (e.g., cloud vs on-premise vs edge, and using the AI model as-is or with fine-tuning, retrieval augmented generation, or other techniques to improve performance and fit).

IV.B Perform key activities to assess the AI model.

1. Perform or review an impact assessment on the selected AI model.
2. Identify laws that apply to the AI model.
3. Identify and evaluate key terms and risks in the vendor or open source agreement.
4. Identify and understand issues that are unique to a company deploying its own proprietary AI model (e.g., increased obligations and higher potential liability).

IV.C Govern the deployment and use of the AI model.

1. Apply the policies, procedures, best practices and ethical considerations to the deployment of an AI model (e.g., data governance, risk management, issue management, user training).
2. Conduct continuous monitoring of the AI model and establish a regular schedule for maintenance, updates and retraining.
3. Conduct periodic activities to assess the AI model's performance, reliability and safety (e.g., audits, red teaming, threat modeling and security testing).
4. Document incidents, issues, risks and post-market monitoring plans.
5. Forecast and reduce risks of secondary or unintended uses and downstream harms.
6. Establish external communication plans.
7. Create and implement a policy and controls to deactivate or localize an AI model as necessary (e.g., due to regulatory requirements or performance issues).