TAISE Curriculum

Module 1: Introduction to AI

- Module 1 Overview
- Module Vocabulary
- Definitions and Concepts of Artificial Intelligence
- How is Machine Learning Related to AI?
- What is "AI"?
- History of AI Development
- Traditional and Generative AI
- Overview of Generative AI Modalities
- Cloud Service Models

Module 2: Generative AI Architecture and Design

- Module 2 Overview
- Module Vocabulary
- Mathematical Foundations for Machine Learning
- Understanding AI Architecture Paradigms
- The Transformer Architecture
- Attention Mechanisms Deep Dive
- Pre-training Architecture and Objectives
- How Generative AI Models Learn
- Architecture of Diffusion Models **(Optional)**
- Diffusion Models and Denoising **(Optional)**
- Data Ingestion and Storage Strategies
- Retrieval-Augmented Generation (RAG) Deep Dive
- Knowledge-Augmented Generation (KAG)
- Cloud Service Models for Generative AI
- Deployment Strategies and Hybrid Environments
- Security and Interoperability

Module 3: AI Use Cases: GenAI, Multimodal, and AI Agents

- Module 3 Overview
- Module Vocabulary
- Everyday Applications of Generative AI
- Image Generation Example: Deepfakes
- Risks and Challenges of AI
- Bias in Data and Algorithms
- Examples in Industry
- The Responsible AI Life Cycle
- Case Study #1—Personalized Medicine Through Multimodal AI
- Case Study #2—AI Chatbots in Mental Health
- Case Study #3—Charlotte AI: Cybersecurity's First Generative AI Analyst

Module 4: Fairness, Accountability, and Explainability in AI

- Module 4 Overview
- Module Vocabulary
- Ethics in the AI Model Development Life Cycle
- Responsible AI in the AI Development Cycle
- Model Understanding
- Interpretability and Explainability Techniques
- Algorithmic Fairness
- Transparency Through Model and Data Documentation
- Communicating with Stakeholders

Module 5: AI Model Lifecycle and Threat Taxonomy

- Module 5 Overview
- Module Vocabulary
- Phases of AI Model Development
- Case Study: AI Model Development Life Cycle
- Understanding Threats
- Introduction to Threat Modeling
- Periodic Risk Reviews and Scenario-Based Risk Analysis
- Risk for AI Models

- Risk Management Using NIST AI RMF
- ISO/IEC Standards for AI Risk Management
- MITRE ATLAS: Adversarial Threat Landscape for AI Systems

Module 6: Model Governance, Risk Management, and Compliance

- Module 6 Overview
- Module Vocabulary
- Foundations and Current Regulatory Landscape
- Current US Regulatory Landscape
- European Union AI Act—Global Impact and Requirements
- AI Risk Management Frameworks and Standards
- STAR for AI, CCM, and AICM
- Framework Selection and Integration Strategy
- Organizational Structures and Accountability
- RACI Models for AI Systems
- AI Governance Committees and Decision-Making
- Accountability Frameworks and Escalation Procedures
- Documentation, Compliance, and Implementation
- AI Policy Development and Implementation
- Audit Trails and Continuous Monitoring
- Cross-Border Challenges in Global AI Development
- Implementation Roadmap for Organizations

Module 7: Introduction to AI Safety and Security

- Module 7 Overview
- Module Vocabulary
- An Analytical Framework for Safety and Security
- Distinguishing AI Safety and Security
- Key Security Challenges in AI Systems
- AI-Augmented Cybersecurity Testing and Red Teaming
- AI Tools for Zero Trust Implementation
- Challenges in Securing Generative and Agentic AI Systems
- Case Study #1: LLMs for Automated Phishing Scams
- Case Study #2: Secure Data Flow in Multinational Operations

Module 8: Cloud and AI Security

- Module 8 Overview
- Module Vocabulary
- Introduction to Cloud Security for AI Systems
- Secure Deployment and Management of AI Models on Cloud Platforms
- Continuous Monitoring and MLOps Pipeline Security
- Incident Response and Disaster Recovery for AI in the Cloud
- Zero Trust Architecture for AI Workloads and Cloud Deployments

Module 9: Data Security & Privacy in AI Systems

- Module 9 Overview
- Module Vocabulary
- Privacy and Security for Machine Learning
- Data Authenticity, Anonymization, and Minimization Techniques
- Data Quality Management and Preprocessing Strategies
- Data Lineage and Metadata Management
- Leveraging Synthetic Data

Module 10: Continuous Learning and Adaptation

- Module 10 Overview
- Module Vocabulary
- The Evolution Beyond Static Models
- Setting Up Monitoring and Data Drift Detection
- Online Learning and Model Update Strategies
- MLOps Integration and LLMOps
- Incorporating User Feedback and Incident Integration
- Educating Stakeholders on AI Risks and Limitations
- Operationalizing Continuous Learning