

AI Enabled Coordinated Assurance Certificate Program

Course Duration: 8 Hours

TOC

Module 1: Introduction to Coordinated Assurance

- 1.1 Foundations and Importance of Coordinated Assurance
- 1.2 Roles of Assurance Providers and Stakeholders in Coordinated Assurance
- 1.3 Standard 9.5 and Governance Expectations

Module 2: The Role of AI in Enhancing Collaboration

- 2.1 AI's Impact on Data Integration and Communication
- 2.2 Overview of Key AI Technologies for Assurance
- 2.3 Collaboration Use Cases Enabled by AI
- 2.4 Risk in AI Utilization

Module 3: Using AI for Assurance Mapping and Reliance

- 3.1 Identifying Overlaps and Gaps with AI
- 3.2 Introduction to Integrated Assurance Mapping
- 3.3 Reliance Strategies and AI

Module 4: Enforcement & Model Integrity

- 4.1 Securing AI Systems Post-Deployment
- 4.2 Model Integrity and Auditing
- 4.3 Cryptographic Integrity Protections (Hash Validation & Signature Rotation)
- 4.4 Side-Channel Attack Scenarios on Model Checkpoints, Quantized Models, and GPU Memory
- 4.5 Guardrail Testing Patterns for Automated Prompt Sanitization
- 4.6 Separation of Duties & Dual Control for High-Risk AI Models
- 4.7 Evaluation Guidance for Model Behavior Consistency
- 4.8 RSAIF Mapping, GRC Interpretation, and Evidence Requirements
- 4.9 Introducing Dual Lab Paths and a Tools Capability Matrix
- 4.10 Hands-On: Implementing RBAC for Secure AI APIs (Dual Lab Path)

4.11 Knowledge Check

Module 5: Case Study – Implementing AI in Coordinated Assurance

5.1 Case Study – Implementing AI in Coordinated Assurance

5.2 Introduction to Ethical Considerations in the Case Study

5.3 Overview of Case Outcomes

Module 6: Toolkits & Automation

6.1 Introduction to AI Security Tools

6.2 Automating AI Security and Compliance

6.3 Hallucination Monitoring and Scoring Mechanisms

6.4 Architecture of Automated Compliance Pipeline

6.5 Automated Rollback Workflows, Drift Alerts, and Scheduled Red Teaming

6.6 Cross-Model Validation for Multi-Model AI Systems

6.7 GPU Runtime Observability and Isolation Requirements

6.8 Introduction: AI Security Automation Stack

6.9 Expanding AI Security Tool Categories

6.10 Tool Selection Criteria and Capability Matrix

6.11 Real Automation Workflow & Evidence Generation

6.12 Hands-On Lab

Module 7: Conclusion – Building Trust and Governance Across Functions

7.1 AI Governance Frameworks and Controls (in Coordinated Assurance)

7.2 Trust, Transparency, and Ethics in AI-Enabled Assurance

7.3 Measuring Assurance Effectiveness (Metrics, KRIs, KPIs, and Continuous Improvement)

7.4 Conclusion and Next Steps