

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27091 — Privacy in AI Systems

ISO Certification Programme



LAPT — London Academy of Professional Training

Address 85 Great Portland Street, W1W 7LT, London, United Kingdom

Email info@lapt.org

Telephone +44 7513 283044

Web lapt.org

Reference IIT-AII-27091 • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	IIT-AII-27091
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1

Audit and Compliance Processes

5 chapters · 30 classes 65 marks

• 1 Understanding ISO 27091 and Its Importance in AI Privacy — 6 classes

› 1.1 Define ISO 27091 and Its Relevance to AI Privacy

› 1.2 Identify Key Principles of ISO 27091 in AI Systems

› 1.3 Explain the Role of Leadership in Implementing ISO 27091

› 1.4 Analyze Common Compliance Challenges with ISO 27091 in AI

› 1.5 Evaluate Case Studies: Successful ISO 27091 Implementation in AI

› 1.6 Develop an Action Plan for ISO 27091 Compliance in Your Organization

• 2 Key Audit Principles and Frameworks for AI Systems — 6 classes

› 2.1 Identify Key Audit Principles of AI Systems

› 2.2 Analyze ISO 27091 Compliance Requirements

› 2.3 Explore Frameworks for Auditing AI Systems

› 2.4 Develop Audit Objectives for AI Implementations

› 2.5 Assess Risks and Controls in AI Audit Processes

› 2.6 Implement Effective Audit Strategies for AI Privacy

• 3 Risk Assessment Methodologies for AI Privacy Compliance — 6 classes

› 3.1 Identify Key Risks in AI Privacy Management

› 3.2 Analyze Existing Compliance Frameworks for AI Systems

› 3.3 Evaluate Risk Assessment Tools for AI Privacy

› 3.4 Develop a Privacy Risk Assessment Matrix for AI Projects

› 3.5 Formulate Risk Mitigation Strategies for Identified AI Privacy Risks

› 3.6 Implement a Continuous Monitoring Plan for AI Privacy Compliance

• 4 Conducting Compliance Audits in AI Environments — 6 classes

› 4.1 Identify Key Compliance Requirements for AI Systems

› 4.2 Develop an Audit Framework Tailored for AI Environments

› 4.3 Plan and Schedule AI Compliance Audits Effectively

› 4.4 Implement Data Privacy Measures During Audits

› 4.5 Analyze Audit Findings in the Context of AI Data Usage

› 4.6 Create Actionable Recommendations to Enhance Compliance

• 5 Reporting and Continuous Improvement in AI Privacy Audits — 6 classes

› 5.1 Analyze Current Reporting Standards for AI Privacy Audits

› 5.2 Identify Key Metrics for Continuous Improvement in AI Privacy

› 5.3 Develop Effective Reporting Templates for AI Privacy Findings

› 5.4 Implement a Feedback Loop for AI Privacy Audit Findings

› 5.5 Create an Action Plan for Addressing Compliance Gaps

› 5.6 Evaluate the Impact of Improvements on AI Privacy Management

• 1 Understanding ISO 27091: Framework and Principles — 6 classes

- › 1.1 Define ISO 27091 and Its Importance in AI Privacy
- › 1.2 Explore Key Principles of ISO 27091 Compliance
- › 1.3 Identify Stakeholders in ISO 27091 Implementation
- › 1.4 Analyze the Framework of ISO 27091 Compliance
- › 1.5 Assess Risks and Challenges in Implementing ISO 27091
- › 1.6 Develop a Plan for Achieving ISO 27091 Compliance

• 2 Identifying Privacy Risks in AI Implementations — 6 classes

- › 2.1 Define Privacy Risks in AI Systems
- › 2.2 Identify Key Stakeholders in AI Privacy
- › 2.3 Assess AI Data Handling Practices
- › 2.4 Evaluate Legal and Regulatory Requirements
- › 2.5 Analyze Potential Impact of Privacy Risks
- › 2.6 Develop Mitigation Strategies for Privacy Risks

• 3 Establishing Compliance and Governance Structures — 6 classes

- › 3.1 Assess Current Governance Structures for Privacy Compliance
- › 3.2 Identify Key Stakeholders in ISO 27091 Implementation
- › 3.3 Develop a Privacy Governance Policy Framework
- › 3.4 Define Roles and Responsibilities for Compliance
- › 3.5 Establish Monitoring and Reporting Mechanisms
- › 3.6 Create an Action Plan for Continuous Improvement in Governance

• 4 Developing Privacy Policies and Procedures for AI — 6 classes

- › 4.1 Identify Key Components of Privacy Policies for AI Systems
- › 4.2 Analyze Regulatory Requirements for AI Privacy Compliance
- › 4.3 Develop Risk Assessment Procedures for AI Privacy
- › 4.4 Create Draft Privacy Policies Tailored for AI Applications
- › 4.5 Review and Revise Draft Policies Based on Stakeholder Feedback
- › 4.6 Implement Procedures for Ongoing Privacy Policy Evaluation

• 5 Auditing and Continuous Improvement in Compliance — 6 classes

- › 5.1 Identify Key Stakeholders for Auditing ISO 27091 Compliance
- › 5.2 Establish Audit Objectives and Scope for AI Systems
- › 5.3 Develop an Audit Plan and Timeline for Continuous Improvement
- › 5.4 Implement Effective Data Collection Techniques for Auditing
- › 5.5 Analyze Findings and Measure Compliance Against ISO 27091 Standards
- › 5.6 Create a Continuous Improvement Framework Post-Audit

• 1 Understanding Privacy Principles in AI Systems — 6 classes

- › 1.1 Define Key Privacy Principles in AI Context
- › 1.2 Identify Legal and Ethical Frameworks Impacting AI Privacy
- › 1.3 Analyze Case Studies of Privacy Failures in AI Systems
- › 1.4 Assess the Role of Data Minimization in AI Privacy
- › 1.5 Develop Strategies for Enhancing Transparency in AI Systems
- › 1.6 Create an Action Plan for Implementing Privacy Principles in AI

• 2 Risk Assessment Framework for AI Privacy**• 3 Governance Structures for AI Privacy Management****• 4 Implementing Privacy by Design in AI Development****• 5 Leading Ethical AI Practices and Compliance**

• 1 Understanding AI and Privacy: Key Concepts and Definitions — 6 classes

- › 1.1 Define Key AI Privacy Terms
- › 1.2 Explore the Concept of Data Minimization
- › 1.3 Identify Privacy Risks in AI Systems
- › 1.4 Analyze Legal Frameworks Governing AI and Privacy
- › 1.5 Evaluate the Role of Consent in AI Privacy
- › 1.6 Apply Privacy-by-Design Principles in AI Development

• 2 Regulatory Landscape: Global and UK-Specific Legal Frameworks for AI — 6 classes

- › 2.1 Explore the Evolution of AI Regulations Globally
- › 2.2 Analyze Key UK Legislation Impacting AI Development
- › 2.3 Identify Core Principles of Data Protection in AI Systems
- › 2.4 Evaluate Compliance Challenges in AI Regulation
- › 2.5 Compare International AI Regulatory Approaches
- › 2.6 Propose Best Practices for Navigating the AI Regulatory Landscape

• 3 Risk Management in AI: Identifying and Mitigating Privacy Risks — 6 classes

- › 3.1 Understand Key Privacy Risks in AI Systems
- › 3.2 Analyze Legal Frameworks Impacting AI Privacy
- › 3.3 Identify Stakeholder Responsibilities in Privacy Risk Management
- › 3.4 Assess Current Risk Management Practices in AI
- › 3.5 Develop Strategies for Mitigating Privacy Risks
- › 3.6 Implement a Risk Management Plan for AI Privacy

• 4 Ethics and Accountability in AI: Legal Obligations and Best Practices — 6 classes

- › 4.1 Define Key Ethical Principles in AI Systems
- › 4.2 Explore Legal Obligations for AI Developers
- › 4.3 Identify Best Practices for Accountability in AI
- › 4.4 Analyze Real-world Case Studies of AI Ethical Dilemmas
- › 4.5 Evaluate Impact of Non-compliance with AI Regulations
- › 4.6 Develop an Accountability Framework for AI Implementation

• 5 The Future of AI Legislation: Emerging Trends and Challenges — 6 classes

- › 5.1 Analyze Global Trends in AI Legislation
- › 5.2 Examine Key Privacy Standards Impacting AI Development
- › 5.3 Identify Emerging Regulatory Challenges in AI Implementation
- › 5.4 Discuss the Role of Stakeholders in Shaping AI Policies
- › 5.5 Evaluate Case Studies of AI Legislative Responses
- › 5.6 Propose Strategic Approaches to Comply with Future AI Laws

• 1 Understanding Privacy Fundamentals in AI Systems — 6 classes

- › 1.1 Define Privacy and Its Importance in AI Systems
- › 1.2 Identify Key Privacy Risks Associated with AI Technologies
- › 1.3 Explore Regulatory Frameworks Impacting AI Privacy
- › 1.4 Analyze Real-World Case Studies of Privacy Breaches in AI
- › 1.5 Assess Strategies for Mitigating Privacy Risks in AI Systems
- › 1.6 Implement Best Practices for Privacy Governance in AI Development

• 2 Identifying Privacy Risks in AI Development — 6 classes

- › 2.1 Define Key Privacy Concepts in AI
- › 2.2 Identify Common Privacy Risks in AI Development
- › 2.3 Analyze Real-World Examples of Privacy Failures in AI
- › 2.4 Assess Privacy Risks Using Risk Assessment Frameworks
- › 2.5 Recommend Best Practices for Mitigating Privacy Risks in AI
- › 2.6 Develop a Privacy Risk Management Plan for AI Projects

• 3 Assessing Impact of AI Algorithms on Privacy — 6 classes

- › 3.1 Identify Key Privacy Concerns in AI Algorithms
- › 3.2 Analyze Data Collection Methods of AI Systems
- › 3.3 Evaluate the Impact of Bias in AI on Privacy
- › 3.4 Assess Legal and Ethical Implications of AI Privacy
- › 3.5 Develop Strategies for Mitigating Privacy Risks in AI
- › 3.6 Create a Privacy Impact Assessment Framework for AI Projects

• 4 Mitigating Privacy Risks in AI Deployment — 6 classes

- › 4.1 Identify Key Privacy Risks in AI Systems
- › 4.2 Assess Impact of Privacy Risks on Stakeholders
- › 4.3 Explore Legal and Ethical Frameworks for Privacy in AI
- › 4.4 Develop Mitigation Strategies for Privacy Risks
- › 4.5 Implement Best Practices for Data Protection in AI
- › 4.6 Evaluate the Effectiveness of Privacy Risk Mitigation Measures

• 5 Establishing Governance and Compliance for AI Privacy — 6 classes

- › 5.1 Identify Key Privacy Regulations Affecting AI Governance
- › 5.2 Assess Privacy Risks Associated with AI Deployment
- › 5.3 Develop a Framework for AI Privacy Compliance
- › 5.4 Implement Data Protection Impact Assessments for AI Systems
- › 5.5 Establish Roles and Responsibilities for AI Privacy Governance
- › 5.6 Evaluate and Enhance AI Privacy Practices Through Continuous Monitoring

• 1 Understanding Stakeholder Dynamics in AI Privacy — 6 classes

- › 1.1 Identify Key Stakeholders in AI Privacy
- › 1.2 Analyze Stakeholder Needs and Concerns
- › 1.3 Map Stakeholder Influence on AI Privacy Dynamics
- › 1.4 Develop Communication Strategies for Stakeholder Engagement
- › 1.5 Facilitate Stakeholder Workshops on AI Privacy Issues
- › 1.6 Evaluate Stakeholder Feedback to Enhance AI Privacy Policies

• 2 Mapping Stakeholder Influence and Interest — 6 classes

- › 2.1 Identify Key Stakeholders in AI Privacy
- › 2.2 Analyze Stakeholder Influence on AI Privacy Decisions
- › 2.3 Assess Stakeholder Interest Levels in AI Privacy Policies
- › 2.4 Develop a Stakeholder Influence Matrix for AI Systems
- › 2.5 Prioritize Stakeholders Based on Influence and Interest
- › 2.6 Create a Strategic Engagement Plan for Key Stakeholders

• 3 Developing Stakeholder Engagement Strategies — 6 classes

- › 3.1 Identify Key Stakeholders for AI Privacy
- › 3.2 Analyze Stakeholder Interests and Concerns
- › 3.3 Develop a Stakeholder Engagement Matrix
- › 3.4 Create Effective Communication Strategies for Stakeholders
- › 3.5 Implement Feedback Mechanisms for Stakeholder Input
- › 3.6 Evaluate and Adjust Engagement Strategies Based on Feedback

• 4 Communicating Privacy Measures to Stakeholders — 6 classes

- › 4.1 Identify Key Stakeholders for Privacy Communication
- › 4.2 Analyze Stakeholder Concerns Regarding AI Privacy
- › 4.3 Develop Clear Messages on Privacy Measures in AI
- › 4.4 Utilize Effective Communication Channels for Stakeholder Engagement
- › 4.5 Address Stakeholder Feedback on Privacy Initiatives
- › 4.6 Evaluate the Impact of Communication Strategies on Stakeholder Trust

• 5 Evaluating and Adapting Stakeholder Engagement Approaches — 6 classes

- › 5.1 Identify Key Stakeholder Characteristics and Needs
- › 5.2 Assess Current Stakeholder Engagement Strategies
- › 5.3 Analyze the Impact of AI on Stakeholder Engagement
- › 5.4 Develop Adaptive Stakeholder Engagement Frameworks
- › 5.5 Implement Feedback Mechanisms for Stakeholder Involvement
- › 5.6 Evaluate and Refine Engagement Approaches Based on Outcomes