LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27090 — Cybersecurity AI Security

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-27090 • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	25	144	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**IIT-AII-27090**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 AI Threat Assessment and Risk Management

5 chapters · 30 classes · **85 marks**

• 1 Understanding AI Threat Landscape — 6 classes

- › 1.1 Identify Key AI Threats in Cybersecurity
- › 1.2 Analyze the Impact of AI Vulnerabilities on Systems
- › 1.3 Evaluate Real-World Case Studies of AI Threats
- › 1.4 Assess Risk Levels Associated with AI Technologies
- › 1.5 Develop Strategies for Mitigating AI-Related Risks
- › 1.6 Create an AI Threat Assessment Framework for Organizations

• 2 Identifying AI-Specific Risks — 6 classes

- › 2.1 Analyze the Unique Risks Associated with AI Technologies
- › 2.2 Evaluate Case Studies of AI Security Breaches
- › 2.3 Identify Vulnerabilities in AI Systems and Algorithms
- › 2.4 Assess the Impact of AI on Organizational Risk Profiles
- › 2.5 Develop Strategies to Mitigate AI-Specific Risks
- › 2.6 Create an AI Risk Assessment Framework for Implementation

• 3 Risk Assessment Frameworks for AI Systems — 6 classes

- › 3.1 Identify Key Components of Risk Assessment Frameworks for AI
- › 3.2 Analyze Different Risk Assessment Models Applied to AI Systems
- › 3.3 Evaluate Vulnerabilities Specific to AI Technologies
- › 3.4 Develop Risk Scenarios Relevant to AI Implementation
- › 3.5 Prioritize Risks Using a Risk Matrix for AI Systems
- › 3.6 Formulate Mitigation Strategies for Identified AI Risks

• 4 Mitigation Strategies for AI Threats — 6 classes

- › 4.1 Identify Common AI Threats in Cybersecurity
- › 4.2 Analyze Vulnerabilities of AI Systems
- › 4.3 Develop Risk Assessment Frameworks for AI
- › 4.4 Implement Mitigation Techniques for Identified Risks
- › 4.5 Monitor AI Systems for Emerging Threats
- › 4.6 Evaluate the Effectiveness of Mitigation Strategies

• 5 Implementing an AI Risk Management Program — 6 classes

- › 5.1 Identify Key Components of an AI Risk Management Program
- › 5.2 Conduct a Threat Assessment for AI Systems
- › 5.3 Develop Risk Assessment Methodologies for AI Applications
- › 5.4 Establish Metrics for Evaluating AI Risks
- › 5.5 Create an Action Plan for Mitigating AI Risks
- › 5.6 Communicate AI Risk Management Strategies to Stakeholders

2 Data Privacy and Compliance in AI Systems

5 chapters · 30 classes **45 marks**

- **1 Understanding Data Privacy Principles in AI Systems** — 6 classes
  - 1.1 Define Key Data Privacy Principles in AI Systems
  - 1.2 Explore the Importance of Consent in Data Handling
  - 1.3 Analyze Data Minimization Strategies for AI Applications
  - 1.4 Examine User Rights and AI: Access, Deletion, and Corrections
  - 1.5 Assess Compliance Risks and Accountability in AI Systems
  - 1.6 Implement Best Practices for Data Privacy in AI Development
- **2 Regulatory Frameworks Impacting AI Data Practices** — 6 classes
  - 2.1 Analyze Key Regulatory Frameworks Impacting AI Data Practices
  - 2.2 Identify Data Privacy Principles Under GDPR for AI Systems
  - 2.3 Examine Compliance Requirements for AI in Data Protection Legislation
  - 2.4 Evaluate the Role of National Data Protection Authorities in AI Governance
  - 2.5 Assess the Impact of Global Regulatory Trends on AI Deployment
  - 2.6 Develop a Compliance Checklist for AI Data Privacy Practices
- **3 Risk Assessment and Management for AI Data Compliance** — 6 classes
  - 3.1 Identify Key Risks in AI Data Processing
  - 3.2 Evaluate Compliance Requirements for AI Systems
  - 3.3 Develop a Risk Assessment Framework for AI
  - 3.4 Analyze Common Vulnerabilities in AI Data Security
  - 3.5 Implement Mitigation Strategies for Identified Risks
  - 3.6 Review and Update Risk Management Practices Regularly
- **4 Implementing Data Protection by Design in AI Development** — 6 classes
  - 4.1 Identify Key Principles of Data Protection by Design in AI
  - 4.2 Analyze Regulatory Requirements for AI Data Protection
  - 4.3 Evaluate Existing AI Systems for Data Privacy Compliance
  - 4.4 Design an Implementation Plan for Data Protection in AI Projects
  - 4.5 Develop Risk Assessment Strategies for AI Data Privacy
  - 4.6 Create a Data Protection Audit Checklist for AI Applications
- **5 Monitoring and Auditing AI Systems for Data Privacy Compliance** — 6 classes
  - 5.1 Identify Key Regulations Impacting AI Data Privacy
  - 5.2 Understand the Role of Monitoring in Compliance Frameworks
  - 5.3 Develop a Data Privacy Audit Checklist for AI Systems
  - 5.4 Implement Continuous Monitoring Techniques for AI Compliance
  - 5.5 Analyze Case Studies of AI Compliance Failures
  - 5.6 Create a Compliance Reporting Strategy for AI Systems

3 Evaluating Cybersecurity Strategies Effectiveness

0 chapters **65 marks**

4 Implementing ISO 27090 Standards

5 chapters · 30 classes **105 marks**

- **1 Understanding ISO 27090: Overview and Importance in Cybersecurity AI** — 6 classes
  - 1.1 Define ISO 27090 and its Role in Cybersecurity AI
  - 1.2 Identify Key Components and Principles of ISO 27090
  - 1.3 Analyze the Importance of ISO 27090 for AI Security
  - 1.4 Explore Case Studies: ISO 27090 Implementation in Organizations
  - 1.5 Evaluate the Benefits and Challenges of Adopting ISO 27090
  - 1.6 Develop a Strategy for Implementing ISO 27090 Standards in Your Organization
- **2 Key Principles and Frameworks of ISO 27090 Implementation** — 6 classes
  - 2.1 Understand Key Principles of ISO 27090 Standards
  - 2.2 Explore the Framework for ISO 27090 Implementation
  - 2.3 Identify Stakeholders in ISO 27090 Compliance
  - 2.4 Assess Current Cybersecurity Posture Against ISO 27090
  - 2.5 Develop an Action Plan for ISO 27090 Adoption
  - 2.6 Evaluate the Effectiveness of ISO 27090 Implementation
- **3 Risk Assessment and Management in Cybersecurity AI Under ISO 27090** — 6 classes
  - 3.1 Identify Key Risks in Cybersecurity AI Systems
  - 3.2 Analyze Vulnerabilities in AI Implementation
  - 3.3 Evaluate Threats Specific to Cybersecurity AI
  - 3.4 Develop a Risk Assessment Framework for AI
  - 3.5 Mitigate Risks Through Effective Management Strategies
  - 3.6 Implement Continuous Monitoring for AI Risk Management
- **4 Developing Policies and Procedures for ISO 27090 Compliance** — 6 classes
  - 4.1 Identify Core Components of ISO 27090 Policies
  - 4.2 Develop Risk Assessment Procedures for Compliance
  - 4.3 Establish Data Protection Guidelines under ISO 27090
  - 4.4 Create Incident Response Policies for AI Security
  - 4.5 Integrate Training and Awareness Programs for ISO Compliance
  - 4.6 Evaluate and Revise Policies for Continuous Improvement
- **5 Assessing and Maintaining ISO 27090 Compliance in Cybersecurity AI** — 6 classes
  - 5.1 Evaluate Current Cybersecurity AI Practices Against ISO 27090 Standards
  - 5.2 Identify Gaps in Compliance and Risk Management Strategies
  - 5.3 Develop a Compliance Assessment Framework for Cybersecurity AI
  - 5.4 Implement Continuous Monitoring Techniques for ISO 27090 Compliance
  - 5.5 Conduct Regular Audits to Ensure Ongoing ISO 27090 Compliance
  - 5.6 Create an Action Plan for Addressing Non-Compliance Issues in Cybersecurity AI

5 Incident Response Planning for AI

5 chapters · 30 classes **65 marks**

- **1 Understanding Incident Response in AI Contexts** — 6 classes
  - 1.1 Define Incident Response in AI Contexts
  - 1.2 Identify Key Components of an AI Incident Response Plan
  - 1.3 Assess Risks and Threats Unique to AI Systems
  - 1.4 Develop Response Strategies for AI Incidents
  - 1.5 Implement Communication Protocols During an AI Incident
  - 1.6 Evaluate and Improve Incident Response Plans for AI
- **2 Frameworks and Standards for AI Incident Response Planning** — 6 classes
  - 2.1 Analyze Existing AI Incident Response Frameworks
  - 2.2 Identify Key Standards for AI Security Compliance
  - 2.3 Evaluate the Role of Stakeholders in Incident Response
  - 2.4 Develop a Tailored Incident Response Plan for AI
  - 2.5 Practice Incident Response Scenarios in AI Contexts
  - 2.6 Assess and Improve Incident Response Plans Post-Incident
- **3 Risk Assessment and Threat Modeling for AI Systems** — 6 classes
  - 3.1 Identify Key AI Risks in Incident Response
  - 3.2 Analyze Threat Vectors Specific to AI Systems
  - 3.3 Evaluate Vulnerabilities in AI Model Architectures
  - 3.4 Assess Impact and Likelihood of AI Threats
  - 3.5 Create a Risk Mitigation Strategy for AI Incidents
  - 3.6 Implement Continuous Monitoring for AI Threats
- **4 Developing AI-Specific Incident Response Procedures** — 6 classes
  - 4.1 Understand the Unique Challenges of AI in Incident Response
  - 4.2 Identify Key Stakeholders for AI Incident Management
  - 4.3 Develop AI-Specific Incident Detection Techniques
  - 4.4 Create AI Incident Response Team Roles and Responsibilities
  - 4.5 Design an AI Incident Response Playbook
  - 4.6 Conduct a Tabletop Exercise for AI Incident Scenarios
- **5 Testing, Training, and Continuous Improvement for AI Incident Responses** — 6 classes
  - 5.1 Assess Current AI Incident Response Models
  - 5.2 Develop Simulation Scenarios for AI Incidents
  - 5.3 Conduct Tabletop Exercises for Team Preparedness
  - 5.4 Analyze Response Outcomes and Identify Gaps
  - 5.5 Implement Continuous Training Programs for Staff
  - 5.6 Review and Revise Incident Response Plans Regularly

6 Security Awareness and Culture Development

5 chapters · 24 classes **65 marks**

- **1 Understanding the Importance of Security Awareness in Cybersecurity** — 6 classes
  - 1.1 Identify Key Components of Security Awareness
  - 1.2 Assess the Current Security Culture in Your Organization
  - 1.3 Explore Common Cyber Threats and Their Impact
  - 1.4 Develop Strategies to Enhance Security Awareness
  - 1.5 Create Engaging Security Training Programs for Employees
  - 1.6 Evaluate the Effectiveness of Security Awareness Initiatives
- **2 Identifying Common Cybersecurity Threats and Vulnerabilities** — 6 classes
  - 2.1 Define Cybersecurity Threats and Vulnerabilities
  - 2.2 Identify Major Types of Cybersecurity Threats
  - 2.3 Analyze Common Vulnerabilities in Digital Systems
  - 2.4 Explore Real-World Examples of Cybersecurity Breaches
  - 2.5 Assess Organizational Risk Factors Related to Cyber Threats
  - 2.6 Develop Strategies for Mitigating Cybersecurity Risks
- **3 Building a Cybersecurity Awareness Program** — 6 classes
  - 3.1 Identify Key Components of a Cybersecurity Awareness Program
  - 3.2 Assess Current Organizational Security Culture
  - 3.3 Develop Engaging Training Materials for Cybersecurity Awareness
  - 3.4 Implement Effective Communication Strategies for Program Launch
  - 3.5 Measure the Impact of Cybersecurity Awareness Initiatives
  - 3.6 Foster Continuous Improvement in Cybersecurity Culture
- **4 Engaging Employees in Cybersecurity Practices** — 6 classes
  - 4.1 Foster a Cybersecurity Culture in the Workplace
  - 4.2 Identify Common Cyber Threats and Vulnerabilities
  - 4.3 Recognize Security Best Practices for Daily Operations
  - 4.4 Encourage Open Communication About Cybersecurity Concerns
  - 4.5 Develop Engaging Training Programs for Staff
  - 4.6 Implement Feedback Mechanisms to Improve Cyber Awareness
- **5 Evaluating and Sustaining Security Awareness Initiatives**