

# LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

## ISO 27001LOG — Information Security in Logistics IT Systems

*ISO Certification Programme*



---

### LAPT — London Academy of Professional Training

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

**Email** [info@lapt.org](mailto:info@lapt.org)

**Telephone** +44 7513 283044

**Web** [lapt.org](http://lapt.org)

**Reference** TR-LOG-27001LOG • ISO Transport

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

|               |                                                |
|---------------|------------------------------------------------|
| REFERENCE     | TR-LOG-27001LOG                                |
| AWARD         | Certificate                                    |
| ASSESSMENT    | 430 marks — 258 to pass (60%)                  |
| PREREQUISITES | None                                           |
| VALIDITY      | Lifetime                                       |
| AWARDING BODY | LAPT — London Academy of Professional Training |

CURRICULUM

1

Implementing Security Controls

0 chapters

45 marks

2

Incident Response Management

0 chapters

85 marks

3

Information Security Principles

5 chapters · 30 classes

85 marks

• 1 Understanding Information Security Concepts in Logistics — 6 classes

› 1.1 Define Key Information Security Concepts in Logistics

› 1.2 Identify Common Threats to Information Security in Logistics

› 1.3 Explore the Role of Data Protection in Logistics Operations

› 1.4 Assess Security Risks in Logistics IT Systems

› 1.5 Implement Basic Information Security Measures in Logistics

› 1.6 Evaluate the Importance of Ongoing Security Training for Logistics Staff

• 2 Identifying Information Security Risks in Logistics IT Systems — 6 classes

› 2.1 Define Key Information Security Terms in Logistics

› 2.2 Identify Common Types of Information Security Risks in Logistics IT

› 2.3 Analyze Real-World Case Studies of Security Breaches in Logistics

› 2.4 Assess Vulnerabilities in Current Logistics IT Systems

› 2.5 Evaluate the Impact of Information Security Risks on Logistics Operations

› 2.6 Develop a Risk Mitigation Plan for Logistics IT Systems

• 3 Implementing Information Security Controls in Logistics Operations — 6 classes

› 3.1 Assess Current Information Security Risks in Logistics Operations

› 3.2 Identify Key Information Security Controls for Logistics IT Systems

› 3.3 Develop a Security Policy Framework for Logistics Operations

› 3.4 Implement Technical Controls for Protecting Logistics Data

› 3.5 Establish Monitoring and Evaluation Mechanisms for Security Controls

› 3.6 Train Staff on Information Security Best Practices in Logistics

• 4 Compliance and Regulatory Frameworks Affecting Logistics IT Security — 6 classes

› 4.1 Identify Key Compliance Standards in Logistics IT Security

› 4.2 Analyze the Impact of GDPR on Logistics Operations

› 4.3 Evaluate the Role of ISO 27001 in Information Security Management

› 4.4 Examine Regulatory Requirements for Data Protection in Logistics

› 4.5 Develop an Internal Audit Process for Compliance Monitoring

› 4.6 Implement Best Practices for Maintaining Compliance in Logistics IT Systems

• 5 Developing a Culture of Security Awareness in Logistics Teams — 6 classes

› 5.1 Identify Key Security Threats in Logistics IT Systems

› 5.2 Develop an Understanding of Security Policies and Procedures

› 5.3 Promote Best Practices for Secure Data Handling

› 5.4 Implement Regular Security Training Sessions for Teams

› 5.5 Foster Open Communication About Security Concerns

› 5.6 Evaluate the Effectiveness of Security Awareness Initiatives

**• 1 Understanding ISO 27001: Principles and Structure** — 6 classes

- › 1.1 Identify Key Principles of ISO 27001
- › 1.2 Explore the Structure of ISO 27001 Documentation
- › 1.3 Analyze the Importance of Information Security Management
- › 1.4 Differentiate Between ISO 27001 and Other Standards
- › 1.5 Assess Compliance Requirements for Logistics IT Systems
- › 1.6 Develop a Basic Implementation Plan for ISO 27001

**• 2 Risk Assessment Methodologies in Logistics IT Systems** — 6 classes

- › 2.1 Identify Key Risks in Logistics IT Systems
- › 2.2 Analyze Vulnerabilities Affecting Information Security
- › 2.3 Evaluate Impact and Likelihood of Identified Risks
- › 2.4 Prioritize Risks Using Qualitative Assessment Techniques
- › 2.5 Develop Mitigation Strategies for High-Priority Risks
- › 2.6 Implement Continuous Risk Monitoring and Review Processes

**• 3 Implementing Security Controls for ISO 27001 Compliance** — 6 classes

- › 3.1 Identify and Assess Security Risks in Logistics IT Systems
- › 3.2 Define Security Objectives Aligned with ISO 27001 Requirements
- › 3.3 Develop and Implement Security Controls in Logistics Systems
- › 3.4 Monitor and Review Security Control Effectiveness
- › 3.5 Integrate Continuous Improvement into Security Practices
- › 3.6 Prepare for Internal Audits and Compliance Checks

**• 4 Continuous Monitoring and Improvement of ISMS** — 6 classes

- › 4.1 Understand the Importance of Continuous Monitoring in ISMS
- › 4.2 Identify Key Metrics for Evaluating ISMS Performance
- › 4.3 Develop a Monitoring Plan for ISMS Effectiveness
- › 4.4 Implement Tools and Techniques for Continuous Monitoring
- › 4.5 Analyze Data to Identify Improvement Opportunities in ISMS
- › 4.6 Create an ISMS Improvement Action Plan Based on Findings

**• 5 Leadership and Culture in Information Security Management** — 6 classes

- › 5.1 Define Leadership Roles in ISO 27001 Implementation
- › 5.2 Identify Key Cultural Elements for Information Security
- › 5.3 Develop Strategies to Foster a Security-Conscious Culture
- › 5.4 Evaluate the Impact of Leadership on Security Behaviour
- › 5.5 Implement Effective Communication Channels for Security Policies
- › 5.6 Assess Continuous Improvement Practices in Security Leadership