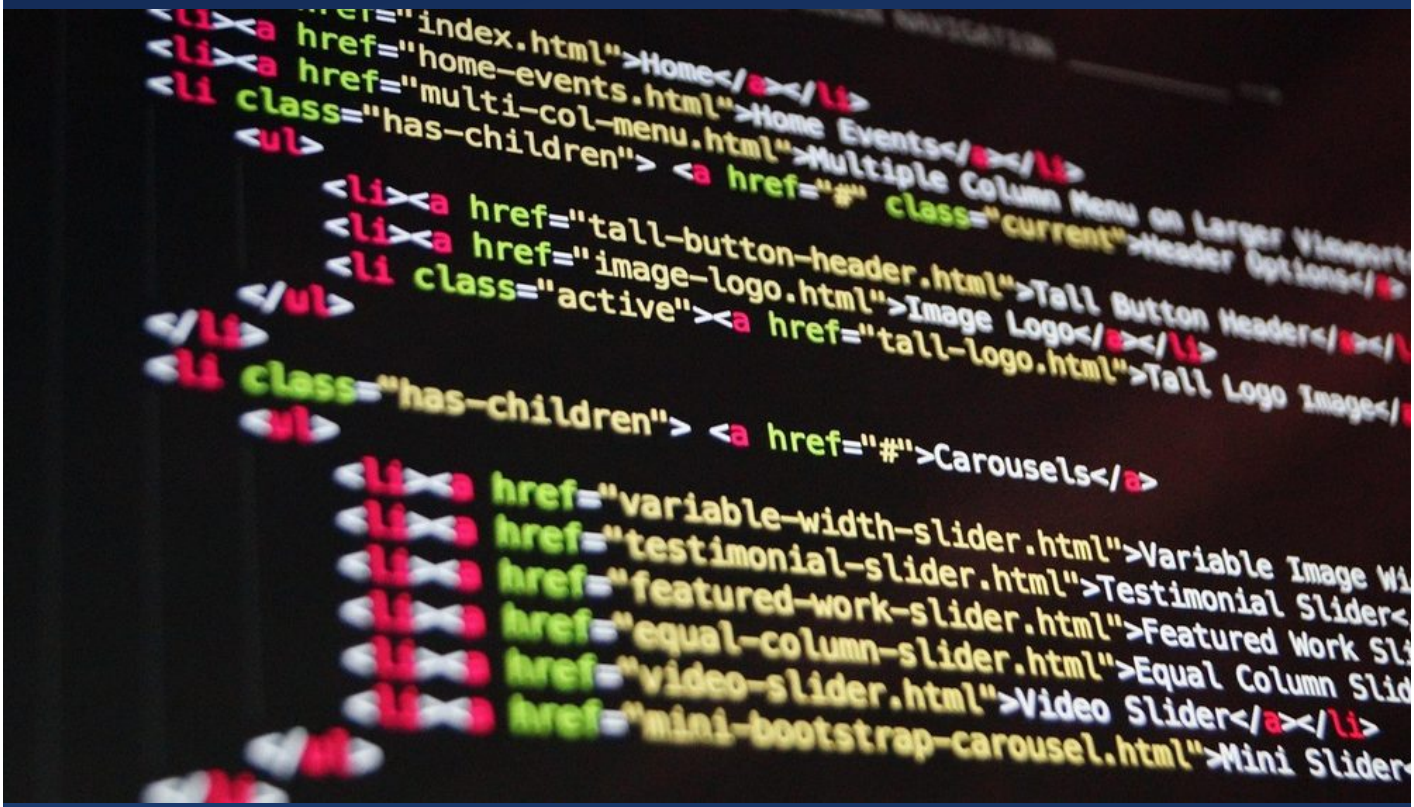
LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27002 — Code of Practice for Information Security Controls

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-INS-27002 • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	10	30	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**IIT-INS-27002**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Compliance and Legal Issues

0 chapters · **65 marks**

2 Continuous Improvement in Information Security

0 chapters · **65 marks**

3 Incident Management and Response

0 chapters · **65 marks**

4 Information Security Governance

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

• 1 Fundamentals of Information Security Governance — 6 classes

- 1.1 Define Information Security Governance Concepts
- 1.2 Identify Key Components of ISO 27002
- 1.3 Explain the Importance of Governance in Information Security
- 1.4 Assess the Role of Leadership in Information Security Governance
- 1.5 Analyze Risk Management Strategies in Governance Frameworks
- 1.6 Develop an Action Plan for Implementing Governance Controls

• 2 Frameworks and Standards for Information Security Management — 6 classes

- 2.1 Define Key Information Security Frameworks
- 2.2 Explore ISO 27002 Standards and Requirements
- 2.3 Analyze the Role of Governance in Information Security
- 2.4 Identify Best Practices for Implementing Security Controls
- 2.5 Evaluate Compliance with Information Security Standards
- 2.6 Develop a Continuous Improvement Plan for Security Management

• 3 Risk Management in Information Security Governance — 6 classes

- 3.1 Understand the Importance of Risk Management in Information Security Governance
- 3.2 Identify Key Risk Management Concepts and Terminology
- 3.3 Analyze Real-World Case Studies of Risk Management Failures
- 3.4 Evaluate Risk Assessment Methodologies in Information Security
- 3.5 Develop a Risk Management Plan for Information Security
- 3.6 Implement Continuous Monitoring and Review Processes in Risk Management

• 4 Roles and Responsibilities in Information Security Governance — 6 classes

- 4.1 Define Key Roles in Information Security Governance
- 4.2 Identify Responsibilities of Information Security Leaders
- 4.3 Explore the Role of Stakeholders in Information Security
- 4.4 Analyze Accountability Structures in Information Security
- 4.5 Develop Effective Communication Strategies for Security Roles
- 4.6 Implement Best Practices for Role-Based Security Governance

• 5 Measuring Effectiveness and Continuous Improvement in Governance — 6 classes

- 5.1 Define Key Performance Indicators for Information Security Governance
- 5.2 Identify Metrics for Measuring Effectiveness of Security Controls
- 5.3 Analyze Data Collection Methods for Governance Metrics
- 5.4 Evaluate the Impact of Governance on Organizational Security Posture
- 5.5 Develop a Continuous Improvement Plan for Information Security Governance
- 5.6 Implement Feedback Mechanisms to Enhance Governance Practices

5 Risk Management Strategies

5 chapters · 85 marks

- 1 Understanding Risk Management in Information Security
- 2 Identifying and Assessing Risks
- 3 Developing Risk Mitigation Strategies
- 4 Implementing Risk Management Frameworks
- 5 Monitoring and Reviewing Risk Management Practices

6 Security Control Implementation

0 chapters · 65 marks