LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27002ISC — 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 SSR-ISC-27002ISC • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	15	84	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

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

CURRICULUM

1 Information Security Principles

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

• 1 Understanding Information Security Fundamentals — 6 classes

- › 1.1 Define Key Information Security Concepts
- › 1.2 Identify Common Information Security Threats
- › 1.3 Explore the Importance of Confidentiality, Integrity, and Availability
- › 1.4 Recognize the Role of Policies and Procedures in Information Security
- › 1.5 Examine Risk Management Principles in Information Security
- › 1.6 Apply Information Security Best Practices to Case Studies

• 2 Risk Management and Assessment in Information Security — 6 classes

- › 2.1 Identify Key Concepts in Risk Management
- › 2.2 Analyze Common Threats to Information Security
- › 2.3 Evaluate Risk Assessment Methodologies
- › 2.4 Determine Risk Levels and Impacts
- › 2.5 Develop Risk Mitigation Strategies
- › 2.6 Implement Continuous Risk Monitoring Practices

• 3 Implementing Information Security Policies and Procedures — 6 classes

- › 3.1 Analyze Current Information Security Policies
- › 3.2 Identify Key Information Security Procedures
- › 3.3 Develop Tailored Information Security Policies
- › 3.4 Communicate Information Security Policies Effectively
- › 3.5 Implement Information Security Procedures in Practice
- › 3.6 Evaluate and Revise Information Security Policies Regularly

• 4 Information Security Controls and Best Practices — 6 classes

- › 4.1 Identify Key Information Security Controls
- › 4.2 Evaluate Best Practices for Risk Management
- › 4.3 Implement Access Control Mechanisms
- › 4.4 Assess Data Protection Strategies
- › 4.5 Monitor and Review Security Performance
- › 4.6 Develop a Response Plan for Security Incidents

• 5 Compliance and Monitoring in Information Security Management — 6 classes

- › 5.1 Recognize the Importance of Compliance in Information Security
- › 5.2 Identify Key Information Security Standards and Regulations
- › 5.3 Assess Current Compliance Levels Against ISO 27002ISC
- › 5.4 Implement Effective Monitoring Strategies for Information Security
- › 5.5 Evaluate Compliance Risks and Develop Mitigation Plans
- › 5.6 Report on Compliance Findings and Continuous Improvement in Security Practices

2 ISO 27002 Framework Application

5 chapters · 30 classes **85 marks**

• 1 Foundations of ISO 27002: Understanding Information Security Controls — 6 classes

- 1.1 Define Key Concepts in Information Security Controls
- 1.2 Explain the Importance of ISO 27002 in Information Security Management
- 1.3 Identify the Major Sections and Structure of ISO 27002
- 1.4 Assess the Role of Leadership in Implementing Information Security Controls
- 1.5 Analyze Real-World Applications of ISO 27002 Controls
- 1.6 Develop a Plan for Integrating ISO 27002 in Organizational Practices

• 2 Key Controls and Their Implementation: A Deep Dive into ISO 27002 — 6 classes

- 2.1 Understand the Structure of ISO 27002 Controls
- 2.2 Identify Key Information Security Controls in ISO 27002
- 2.3 Evaluate Control Objectives and Their Importance
- 2.4 Analyze Implementation Strategies for ISO 27002 Controls
- 2.5 Measure the Effectiveness of Information Security Controls
- 2.6 Develop a Continuous Improvement Plan for ISO 27002 Compliance

• 3 Risk Assessment and Management Within the ISO 27002 Framework — 6 classes

- 3.1 Define Key Concepts in Risk Assessment and Management
- 3.2 Identify Risks Relevant to the ISO 27002 Framework
- 3.3 Evaluate the Impact and Likelihood of Identified Risks
- 3.4 Develop Risk Treatment Plans Aligned with ISO 27002
- 3.5 Implement Risk Management Strategies in Practice
- 3.6 Review and Monitor Risk Management Outcomes

• 4 Monitoring and Reviewing Controls: Ensuring Compliance and Effectiveness — 6 classes

- 4.1 Identify Key Monitoring Metrics for Information Security Controls
- 4.2 Implement Effective Monitoring Techniques for ISO 27002 Compliance
- 4.3 Analyze Data from Monitoring to Evaluate Control Effectiveness
- 4.4 Develop a Review Schedule for Information Security Controls
- 4.5 Communicate Findings from Monitoring and Reviews to Stakeholders
- 4.6 Adjust and Optimize Controls Based on Monitoring Insights

• 5 Continuous Improvement and Future Trends in ISO 27002 Compliance — 6 classes

- 5.1 Identify Key Elements of Continuous Improvement in ISO 27002
- 5.2 Analyze Current Compliance Gaps Against ISO 27002 Standards
- 5.3 Develop Action Plans for Addressing Compliance Gaps
- 5.4 Implement Measurement and Monitoring Techniques for ISO 27002
- 5.5 Explore Emerging Trends Impacting ISO 27002 Compliance
- 5.6 Create a Roadmap for Sustaining Continuous Improvement in Information Security

3 Leadership in Information Security

0 chapters **85 marks**

4 Policy Development and Implementation

0 chapters **65 marks**

5 Risk Management Strategies

5 chapters · 24 classes **65 marks**

- **1 Fundamentals of Risk Management in Information Security** — 6 classes
  - 1.1 Define Key Concepts in Risk Management
  - 1.2 Identify Common Security Risks in Information Systems
  - 1.3 Evaluate the Impact of Risks on Information Security
  - 1.4 Analyze Risk Assessment Methodologies
  - 1.5 Develop a Risk Mitigation Plan
  - 1.6 Implement Continuous Risk Monitoring Strategies
- **2 Identifying and Assessing Information Security Risks** — 6 classes
  - 2.1 Define Information Security Risks in Your Organisation
  - 2.2 Identify Common Vulnerabilities and Threats
  - 2.3 Evaluate the Impact of Identified Risks
  - 2.4 Assess the Likelihood of Information Security Incidents
  - 2.5 Prioritise Risks Based on Impact and Likelihood
  - 2.6 Develop a Risk Assessment Report for Stakeholders
- **3 Developing Risk Mitigation Strategies** — 6 classes
  - 3.1 Identify Key Risks in Information Security
  - 3.2 Analyze the Impact of Risks on Business Operations
  - 3.3 Develop Risk Acceptance Criteria for Stakeholders
  - 3.4 Explore Preventive Measures for Identified Risks
  - 3.5 Formulate a Risk Mitigation Plan Based on Best Practices
  - 3.6 Evaluate and Adjust Mitigation Strategies Regularly
- **4 Monitoring and Reviewing Risk Management Practices** — 6 classes
  - 4.1 Identify Key Metrics for Risk Management Monitoring
  - 4.2 Establish Reporting Frameworks for Risk Assessment
  - 4.3 Analyze Historical Data to Improve Risk Strategies
  - 4.4 Conduct Regular Audits of Risk Management Practices
  - 4.5 Utilize Feedback Loops for Continuous Improvement
  - 4.6 Develop an Action Plan for Addressing Identified Risks
- **5 Integrating Risk Management with Business Processes**

6 Security Control Evaluation

0 chapters **45 marks**