LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001ISC — Information Security Management 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 SSR-ISC-27001ISC • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	30	180	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**SSR-ISC-27001ISC**
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

5 chapters · 30 classes · **65 marks**

- **1 Understanding Information Security Compliance Frameworks** — 6 classes
  - 1.1 Define Key Concepts in Information Security Compliance
  - 1.2 Identify the Main Information Security Compliance Frameworks
  - 1.3 Explore the Importance of ISO 27001 in Compliance
  - 1.4 Analyze Legal Regulations Impacting Information Security
  - 1.5 Discuss Best Practices for Implementing Compliance Frameworks
  - 1.6 Assess the Role of Leadership in Compliance Management
- **2 Legal Obligations and Responsibilities in Information Security** — 6 classes
  - 2.1 Identify Key Legal Frameworks Affecting Information Security
  - 2.2 Analyze Compliance Requirements for ISO 27001
  - 2.3 Evaluate the Role of Data Protection Legislation in Information Security
  - 2.4 Assess Organizational Responsibilities Under Information Security Laws
  - 2.5 Examine Consequences of Non-Compliance with Information Security Regulations
  - 2.6 Develop an Action Plan for Ensuring Legal Compliance in Information Security
- **3 Risk Management and Legal Compliance** — 6 classes
  - 3.1 Identify Key Risk Management Concepts in ISO 27001
  - 3.2 Analyze Legal and Regulatory Requirements for Compliance
  - 3.3 Assess Risk Assessment Methodologies in Information Security
  - 3.4 Develop a Risk Treatment Plan to Mitigate Identified Risks
  - 3.5 Create Procedures for Monitoring and Reviewing Legal Compliance
  - 3.6 Implement Practical Scenarios for Risk Management Compliance
- **4 Incident Response and Legal Requirements** — 6 classes
  - 4.1 Understand the Importance of Incident Response in ISO 27001
  - 4.2 Identify Key Legal Requirements for Incident Reporting
  - 4.3 Analyze the Role of Compliance in Incident Management
  - 4.4 Develop a Framework for Effective Incident Response
  - 4.5 Document and Communicate Incident Response Procedures
  - 4.6 Evaluate Real-World Case Studies of Incident Response Failures
- **5 Governance, Auditing, and Continuous Compliance** — 6 classes
  - 5.1 Define Governance in Information Security Management
  - 5.2 Explore the Role of Auditing in Compliance Practices
  - 5.3 Identify Key Components of an Effective Audit Framework
  - 5.4 Examine Continuous Compliance Strategies for ISO 27001
  - 5.5 Analyze Case Studies of Governance Failures in Information Security
  - 5.6 Implement a Continuous Improvement Plan for Compliance Maintenance

2 Information Security Governance

5 chapters · 30 classes **85 marks**

- **1 Fundamentals of Information Security Governance** — 6 classes
  - 1.1 Define and Explain the Concept of Information Security Governance
  - 1.2 Identify Key Components of an Information Security Governance Framework
  - 1.3 Analyze the Role of Leadership in Information Security Governance
  - 1.4 Assess Risks and Compliance Requirements in Information Security
  - 1.5 Develop an Effective Information Security Policy
  - 1.6 Implement Continuous Improvement Strategies in Information Security Governance
- **2 Information Security Policies and Frameworks** — 6 classes
  - 2.1 Define Information Security Policies and Their Importance
  - 2.2 Identify Key Components of an Effective Security Framework
  - 2.3 Analyze the Relationship Between Policies and Compliance Requirements
  - 2.4 Develop a Sample Information Security Policy Document
  - 2.5 Evaluate Existing Security Frameworks and Their Applicability
  - 2.6 Implement Best Practices for Policy Review and Updates
- **3 Risk Management in Information Security Governance** — 6 classes
  - 3.1 Identify Risk Factors in Information Security
  - 3.2 Assess and Prioritize Information Security Risks
  - 3.3 Develop Risk Mitigation Strategies
  - 3.4 Implement Risk Management Frameworks
  - 3.5 Monitor and Review Risk Management Processes
  - 3.6 Communicate Risk Management Findings to Stakeholders
- **4 Roles and Responsibilities in Information Security Governance** — 6 classes
  - 4.1 Define Key Roles in Information Security Governance
  - 4.2 Identify Responsibilities of Senior Management in Security Leadership
  - 4.3 Explore the Role of the Information Security Officer
  - 4.4 Assess Team Collaboration and Responsibilities in Governance
  - 4.5 Analyze Stakeholder Involvement in Information Security
  - 4.6 Develop a Framework for Accountability in Security Roles
- **5 Measuring and Improving Information Security Governance** — 6 classes
  - 5.1 Define Key Metrics for Information Security Governance
  - 5.2 Assess Current Information Security Governance Framework
  - 5.3 Analyze Gaps in Information Security Performance
  - 5.4 Implement Continuous Improvement Strategies for Governance
  - 5.5 Develop a Dashboard for Ongoing Security Metrics Monitoring
  - 5.6 Conduct a Review and Adapt Information Security Policies

3 ISMS Framework Development

5 chapters · 30 classes **105 marks**

- **1 Understanding ISO 27001 — Principles and Objectives** — 6 classes
  - 1.1 Define Key Principles of ISO 27001
  - 1.2 Explore the Objectives of an Information Security Management System
  - 1.3 Identify the Benefits of Implementing ISO 27001
  - 1.4 Examine the Structure of the ISO 27001 Standard
  - 1.5 Analyze Risk Management within the ISMS Framework
  - 1.6 Apply ISO 27001 Principles to Real-World Scenarios
- **2 Scope and Context of the ISMS** — 6 classes
  - 2.1 Define the Scope of the ISMS
  - 2.2 Identify Stakeholders and Their Requirements
  - 2.3 Analyze the Internal and External Context
  - 2.4 Determine Boundaries for the ISMS
  - 2.5 Assess Information Security Risks and Opportunities
  - 2.6 Document the Scope and Context of the ISMS
- **3 Risk Assessment and Treatment Process** — 6 classes
  - 3.1 Identify and Categorize Information Assets
  - 3.2 Analyze and Evaluate Risks to Information Assets
  - 3.3 Prioritize Risks Based on Impact and Likelihood
  - 3.4 Determine Risk Treatment Options and Strategies
  - 3.5 Develop and Implement Risk Treatment Plans
  - 3.6 Review and Monitor Risk Treatment Effectiveness
- **4 Developing ISMS Policies and Objectives** — 6 classes
  - 4.1 Assessing Current ISMS Policies and Gaps
  - 4.2 Identifying Key Information Security Objectives
  - 4.3 Aligning Policies with Organisational Goals
  - 4.4 Drafting Effective ISMS Policies
  - 4.5 Establishing Measurable Objectives for ISMS
  - 4.6 Communicating and Implementing ISMS Policies
- **5 Monitoring, Review, and Continuous Improvement of ISMS** — 6 classes
  - 5.1 Analyze Current ISMS Performance Metrics
  - 5.2 Identify Key Stakeholders for ISMS Review
  - 5.3 Conduct Effective ISMS Internal Audits
  - 5.4 Implement Corrective Actions for ISMS Nonconformities
  - 5.5 Develop a Continuous Improvement Plan for ISMS
  - 5.6 Evaluate and Report on ISMS Improvement Outcomes

4 Performance Evaluation and Improvement

5 chapters · 30 classes **45 marks**

- **1 Understanding Performance Evaluation in Information Security Management Systems** — 6 classes
  - 1.1 Define Key Concepts in Performance Evaluation
  - 1.2 Identify Metrics and KPIs for Information Security
  - 1.3 Analyze Current Performance Against Established Standards
  - 1.4 Evaluate Tools and Techniques for Assessment
  - 1.5 Develop an Action Plan for Performance Improvement
  - 1.6 Implement Continuous Improvement Strategies in Security Management
- **2 Key Performance Indicators (KPIs) for Information Security** — 6 classes
  - 2.1 Define Key Performance Indicators for Information Security
  - 2.2 Identify Relevant KPIs for Risk Management
  - 2.3 Analyze Current Performance Metrics in Information Security
  - 2.4 Establish Baselines for Information Security KPIs
  - 2.5 Develop Action Plans for KPI Improvement
  - 2.6 Review and Adjust KPIs for Continuous Improvement
- **3 Conducting Internal Audits for Performance Assessment** — 6 classes
  - 3.1 Define Internal Audits in the Context of ISO 27001
  - 3.2 Identify Key Performance Indicators for Security Audits
  - 3.3 Develop an Internal Audit Checklist for Information Security
  - 3.4 Conduct a Mock Internal Audit for Performance Assessment
  - 3.5 Analyze Audit Findings and Report on Performance Gaps
  - 3.6 Recommend Improvement Actions Based on Audit Results
- **4 Managing Nonconformities and Corrective Actions** — 6 classes
  - 4.1 Identify and Classify Nonconformities in ISMS
  - 4.2 Analyze Root Causes of Identified Nonconformities
  - 4.3 Develop Effective Corrective Action Plans
  - 4.4 Implement Corrective Actions and Monitor Progress
  - 4.5 Evaluate Effectiveness of Corrective Actions
  - 4.6 Document Nonconformities and Corrective Actions for Compliance
- **5 Continuous Improvement Strategies in Information Security Management** — 6 classes
  - 5.1 Analyze Current Information Security Practices
  - 5.2 Identify Key Performance Indicators for Improvement
  - 5.3 Develop a Continuous Improvement Plan for Security Measures
  - 5.4 Implement Feedback Mechanisms for Security Protocols
  - 5.5 Assess the Impact of Improvement Strategies on Security
  - 5.6 Foster a Culture of Continuous Improvement in Security Teams

5 Risk Assessment and Management

5 chapters · 30 classes **85 marks**

- **1 Understanding Risk Assessment Principles and Frameworks** — 6 classes
  - 1.1 Define Key Concepts in Risk Assessment
  - 1.2 Identify the Importance of Risk Assessment in Information Security
  - 1.3 Describe Common Risk Assessment Frameworks
  - 1.4 Analyze the Risk Assessment Process Steps
  - 1.5 Evaluate Risk Assessment Tools and Techniques
  - 1.6 Apply Risk Assessment Principles to Real-World Scenarios
- **2 Identifying and Analyzing Information Security Risks** — 6 classes
  - 2.1 Define Key Concepts in Information Security Risk
  - 2.2 Identify Assets and Their Value in Information Security
  - 2.3 Evaluate Threats and Vulnerabilities Impacting Security
  - 2.4 Analyze the Potential Impact of Information Security Risks
  - 2.5 Assess Current Controls and Their Effectiveness
  - 2.6 Develop a Risk Mitigation Strategy Based on Analysis
- **3 Risk Evaluation and Treatment Strategies** — 6 classes
  - 3.1 Identify Key Risk Evaluation Criteria
  - 3.2 Analyze Risk Impact and Likelihood
  - 3.3 Prioritize Risks Using Assessment Frameworks
  - 3.4 Develop Risk Treatment Options
  - 3.5 Implement Risk Treatment Plans Effectively
  - 3.6 Review and Monitor Risk Treatment Outcomes
- **4 Implementing Risk Management Controls and Measures** — 6 classes
  - 4.1 Identify and Classify Information Assets for Risk Management
  - 4.2 Assess Potential Threats and Vulnerabilities to Information Assets
  - 4.3 Determine Risk Tolerance Levels and Acceptable Risks
  - 4.4 Develop and Prioritize Risk Mitigation Strategies
  - 4.5 Implement Risk Management Controls and Measures Effectively
  - 4.6 Monitor and Review Risk Management Practices for Continuous Improvement
- **5 Risk Management Communication and Reporting** — 6 classes
  - 5.1 Identify Key Stakeholders in Risk Management Communication
  - 5.2 Develop Effective Risk Communication Strategies
  - 5.3 Utilize Visual Aids for Risk Reporting
  - 5.4 Craft Clear and Concise Risk Management Reports
  - 5.5 Facilitate Stakeholder Engagement through Effective Communication
  - 5.6 Evaluate the Impact of Risk Communication on Decision Making

6 Security Awareness and Culture

5 chapters · 30 classes **45 marks**

- **1 Understanding Information Security and Its Importance** — 6 classes
  - 1.1 Define Information Security and Its Key Components
  - 1.2 Explore the Importance of Information Security in Today's Digital World
  - 1.3 Identify Common Threats and Vulnerabilities in Information Systems
  - 1.4 Understand the Role of Organizational Culture in Promoting Security Awareness
  - 1.5 Assess Personal Responsibility in Upholding Information Security Practices
  - 1.6 Develop Practical Strategies for Enhancing Security Awareness Within Teams
- **2 Identifying Security Threats and Vulnerabilities** — 6 classes
  - 2.1 Define Common Security Threats in Information Systems
  - 2.2 Analyze Real-World Security Breaches and Their Impact
  - 2.3 Identify Vulnerabilities in Your Organization's Infrastructure
  - 2.4 Evaluate Human Factors Contributing to Security Risks
  - 2.5 Assess Potential Risks Using Threat Modeling Techniques
  - 2.6 Develop a Personal Action Plan to Mitigate Identified Threats
- **3 Building a Security-Conscious Culture** — 6 classes
  - 3.1 Identify Key Components of a Security-Conscious Culture
  - 3.2 Assess Current Organizational Security Awareness Levels
  - 3.3 Develop Effective Security Training Programs for Staff
  - 3.4 Foster Open Communication About Security Risks
  - 3.5 Implement Behavioral Incentives for Security Best Practices
  - 3.6 Evaluate the Impact of Security Culture on Business Outcomes
- **4 Implementing Effective Security Awareness Programs** — 6 classes
  - 4.1 Assess Current Security Awareness Levels in Your Organization
  - 4.2 Define Key Messages and Objectives for Security Awareness Programs
  - 4.3 Develop Engaging Training Materials and Resources
  - 4.4 Implement Interactive Security Awareness Workshops
  - 4.5 Evaluate the Effectiveness of Security Awareness Initiatives
  - 4.6 Foster a Continuous Security Culture Through Ongoing Engagement
- **5 Measuring and Sustaining Security Awareness Initiatives** — 6 classes
  - 5.1 Define Key Metrics for Security Awareness Success
  - 5.2 Implement Surveys to Assess Security Awareness Levels
  - 5.3 Analyze Data to Identify Gaps in Security Awareness
  - 5.4 Develop Tailored Training Programs Based on Assessment Findings
  - 5.5 Create a Feedback Loop to Refine Security Awareness Initiatives
  - 5.6 Sustain Engagement Through Continuous Improvement Strategies