LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001PCR — Information Security Management

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-PCR-27001PCR • 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-PCR-27001PCR**
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 Considerations

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

- **1 Understanding Legal Frameworks for Information Security** — 6 classes
  - 1.1 Explore Key Legal Principles for Information Security
  - 1.2 Identify Relevant Information Security Legislation
  - 1.3 Analyze the Role of Data Protection Regulations
  - 1.4 Discuss Implications of Non-Compliance in Information Security
  - 1.5 Evaluate Case Studies of Legal Framework Applications
  - 1.6 Implement Best Practices for Legal Compliance in ISMS
- **2 Analyzing ISO 27001 Requirements and Compliance** — 6 classes
  - 2.1 Identify Key Components of ISO 27001 Requirements
  - 2.2 Evaluate Risk Assessment Procedures in ISO 27001
  - 2.3 Analyze Compliance Obligations Under ISO 27001 Standards
  - 2.4 Examine the Role of Information Security Policies in ISO 27001
  - 2.5 Assess the Importance of Regular Audits for ISO 27001 Compliance
  - 2.6 Develop an Action Plan for Implementing ISO 27001 Requirements
- **3 Risk Management and Legal Considerations in ISO 27001** — 6 classes
  - 3.1 Identify Key Legal Obligations in Information Security Management
  - 3.2 Analyze Risks and Impacts Related to ISO 27001 Compliance
  - 3.3 Evaluate the Role of Risk Assessment in ISO 27001 Implementation
  - 3.4 Develop a Risk Treatment Plan in Compliance with Legal Standards
  - 3.5 Create an Incident Response Plan Addressing Legal and Compliance Issues
  - 3.6 Review and Update Risk Management Strategies for Ongoing Compliance
- **4 Developing Policies and Procedures for Compliance** — 6 classes
  - 4.1 Identify Key Compliance Requirements for ISO 27001PCR
  - 4.2 Analyze Existing Policies and Gaps in Compliance
  - 4.3 Develop Effective Information Security Policies
  - 4.4 Create Procedures for Policy Implementation and Monitoring
  - 4.5 Establish Roles and Responsibilities for Compliance Oversight
  - 4.6 Evaluate and Review Policies for Continuous Improvement
- **5 Auditing and Continuous Improvement in Compliance Processes** — 6 classes
  - 5.1 Identify Key Components of Compliance Auditing
  - 5.2 Analyze Regulatory Requirements Impacting Audits
  - 5.3 Develop Effective Audit Strategies for Compliance
  - 5.4 Implement Tools for Effective Audit Evidence Collection
  - 5.5 Evaluate Findings and Recommend Improvements
  - 5.6 Create a Continuous Improvement Plan for Compliance Processes

2 Continuous Improvement and Auditing

5 chapters · 30 classes **65 marks**

- **1 Understanding Continuous Improvement in Information Security Management** — 6 classes
  - 1.1 Define Continuous Improvement in Information Security Management
  - 1.2 Identify Key Principles of Continuous Improvement Frameworks
  - 1.3 Explore the Role of Auditing in Continuous Improvement
  - 1.4 Analyze Case Studies of Successful Continuous Improvement Initiatives
  - 1.5 Develop Continuous Improvement Action Plans for Information Security
  - 1.6 Assess the Impact of Continuous Improvement on Security Management Practices
- **2 Key Techniques for Auditing Information Security Processes** — 6 classes
  - 2.1 Identify Key Audit Objectives for Information Security
  - 2.2 Analyze Risks and Opportunities in Security Processes
  - 2.3 Develop Effective Audit Checklists and Questionnaires
  - 2.4 Implement Sampling Techniques for Audit Evidence Collection
  - 2.5 Evaluate Audit Findings and Develop Recommendations
  - 2.6 Create a Continuous Improvement Plan Based on Audit Results
- **3 Establishing Metrics and Performance Indicators for Security Improvement** — 6 classes
  - 3.1 Define Key Metrics for Information Security Performance
  - 3.2 Identify Relevant Performance Indicators for Continuous Improvement
  - 3.3 Develop a Framework for Measuring Security Effectiveness
  - 3.4 Analyze Data Collection Methods for Security Metrics
  - 3.5 Implement Monitoring Processes for Performance Indicators
  - 3.6 Evaluate and Adjust Metrics Based on Security Audits
- **4 Conducting Effective Internal Audits in ISO 27001 Framework** — 6 classes
  - 4.1 Identify the Purpose and Scope of Internal Audits in ISO 27001
  - 4.2 Develop an Internal Audit Plan Aligned with ISO 27001 Requirements
  - 4.3 Implement Effective Auditing Techniques for Information Security
  - 4.4 Engage Stakeholders to Enhance Internal Audit Participation
  - 4.5 Analyze Audit Findings and Identify Areas for Improvement
  - 4.6 Establish Follow-Up Processes to Ensure Continuous Improvement
- **5 Leveraging Audit Findings for Strategic Improvement** — 6 classes
  - 5.1 Analyze Audit Findings to Identify Improvement Opportunities
  - 5.2 Prioritize Audit Findings for Strategic Impact
  - 5.3 Develop Action Plans based on Audit Insights
  - 5.4 Implement Changes: Best Practices for Continuous Improvement
  - 5.5 Measure Success: Evaluating the Impact of Improvements
  - 5.6 Communicate Audit Outcomes to Stakeholders Effectively

3 Implementing an ISMS

5 chapters · 30 classes **105 marks**

- **1 Understanding the ISO 27001 Framework and ISMS Principles** — 6 classes
  - 1.1 Explore the ISO 27001 Framework Overview
  - 1.2 Identify Key Components of an Information Security Management System (ISMS)
  - 1.3 Analyze the Importance of Risk Assessment in ISO 27001
  - 1.4 Understand the Roles and Responsibilities in ISMS Implementation
  - 1.5 Apply the Principles of Continuous Improvement to ISMS
  - 1.6 Develop an Action Plan for ISO 27001 Compliance
- **2 Risk Assessment and Management in Information Security** — 6 classes
  - 2.1 Define Key Concepts in Risk Assessment for ISMS
  - 2.2 Identify Potential Risks in Information Security
  - 2.3 Evaluate the Impact and Likelihood of Identified Risks
  - 2.4 Develop Risk Mitigation Strategies in Information Security
  - 2.5 Implement a Risk Management Action Plan
  - 2.6 Monitor and Review Risks Effectively in an ISMS
- **3 Developing an Information Security Policy and Objectives** — 6 classes
  - 3.1 Identify Key Components of an Information Security Policy
  - 3.2 Assess Organizational Context for Security Objectives
  - 3.3 Develop Measurable Information Security Objectives
  - 3.4 Align Information Security Policy with Business Goals
  - 3.5 Communicate the Information Security Policy Effectively
  - 3.6 Evaluate and Revise Security Objectives Periodically
- **4 Implementing Controls and Security Measures** — 6 classes
  - 4.1 Identify Essential Security Controls for ISMS Implementation
  - 4.2 Assess Risks to Determine Appropriate Security Measures
  - 4.3 Develop Policies and Procedures for Security Control Implementation
  - 4.4 Train Staff on Security Controls and ISMS Procedures
  - 4.5 Monitor and Review the Effectiveness of Implemented Controls
  - 4.6 Adjust Security Measures Based on Monitoring Outcomes and Feedback
- **5 Monitoring, Reviewing, and Continuous Improvement of the ISMS** — 6 classes
  - 5.1 Define Key Performance Indicators for ISMS Monitoring
  - 5.2 Conduct Internal Audits of the ISMS
  - 5.3 Analyze Audit Results to Identify Improvement Areas
  - 5.4 Implement Corrective Actions for ISMS Deficiencies
  - 5.5 Review and Update ISMS Policies Based on Findings
  - 5.6 Foster a Culture of Continuous Improvement in Information Security

4 ISO 27001 Principles and Standards

5 chapters · 30 classes **85 marks**

• 1 Understanding ISO 27001: The Framework of Information Security Management — 6 classes

- 1.1 Define Key Concepts in Information Security Management
- 1.2 Explore the Structure of ISO 27001 Standards
- 1.3 Identify the Benefits of Implementing ISO 27001
- 1.4 Analyze the Requirements for Information Security Policies
- 1.5 Examine the Role of Risk Assessment in ISO 27001
- 1.6 Develop an Action Plan for ISO 27001 Implementation

• 2 Core Principles of Information Security: Confidentiality, Integrity, and Availability (CIA) — 6 classes

- 2.1 Define and Explore the Concept of Confidentiality in Information Security
- 2.2 Investigate Techniques to Maintain Data Integrity
- 2.3 Analyze the Importance of Availability in Information Systems
- 2.4 Discuss the Interrelationship Between Confidentiality, Integrity, and Availability
- 2.5 Implement Best Practices for Enhancing Information Security Using the CIA Triad
- 2.6 Evaluate Real-world Scenarios to Apply the CIA Principles Effectively

• 3 Risk Management in ISO 27001: Identifying and Evaluating Risks — 6 classes

- 3.1 Understand the Importance of Risk Management in ISO 27001
- 3.2 Identify Common Types of Information Security Risks
- 3.3 Conduct a Risk Assessment: Tools and Techniques
- 3.4 Evaluate the Impact and Likelihood of Identified Risks
- 3.5 Develop Risk Treatment Options for Managing Risks
- 3.6 Communicate and Monitor Risks in an ISO 27001 Framework

• 4 Implementing Controls: The Annex A Structure and Beyond — 6 classes

- 4.1 Understand the Structure of Annex A Controls
- 4.2 Identify Key Control Categories in ISO 27001
- 4.3 Assess Organizational Risks for Control Selection
- 4.4 Implement Essential Security Controls Effectively
- 4.5 Evaluate Control Performance and Effectiveness
- 4.6 Develop a Continuous Improvement Plan for Controls

• 5 Continuous Improvement and Audit of the ISMS: Ensuring Compliance and Effectiveness — 6 classes

- 5.1 Identify Key Components of Continuous Improvement in ISMS
- 5.2 Analyze the ISO 27001 Audit Process for Compliance
- 5.3 Evaluate Effectiveness of Current ISMS Practices
- 5.4 Develop an Action Plan for ISMS Enhancement
- 5.5 Implement Audit Findings for Continuous Improvement
- 5.6 Review and Reflect on ISMS Adaptations and Successes

5 Leadership in Information Security

5 chapters · 30 classes **45 marks**

• 1 Understanding Leadership Roles in Information Security Management — 6 classes

- 1.1 Define Key Leadership Roles in Information Security Management
- 1.2 Analyze Leadership Styles and Their Impact on Security Governance
- 1.3 Explore the Responsibilities of Information Security Leaders
- 1.4 Identify Best Practices for Building a Security-Centric Culture
- 1.5 Develop Communication Strategies for Engaging Stakeholders
- 1.6 Apply Leadership Principles to Real-World Security Scenarios

• 2 Establishing a Security Culture and Governance Framework — 6 classes

- 2.1 Define Security Culture and Its Importance in Organizations
- 2.2 Identify Key Elements of an Effective Governance Framework
- 2.3 Assess the Current Security Culture within Your Organization
- 2.4 Develop Strategies to Enhance Security Awareness Among Employees
- 2.5 Implement Governance Structures to Support Information Security
- 2.6 Measure and Evaluate the Effectiveness of Security Governance Initiatives

• 3 Risk Assessment and Management Strategies for Leaders — 6 classes

- 3.1 Understand the Fundamentals of Risk in Information Security
- 3.2 Identify and Evaluate Security Risks Within Your Organization
- 3.3 Develop Effective Risk Management Frameworks for Leadership
- 3.4 Prioritize Risks Based on Impact and Likelihood
- 3.5 Implement Risk Mitigation Strategies to Enhance Security
- 3.6 Monitor and Review Risk Management Strategies for Continuous Improvement

• 4 Developing Effective Communication and Training Programs — 6 classes

- 4.1 Assess Communication Needs for Information Security
- 4.2 Design Engaging Training Modules for Security Awareness
- 4.3 Implement Feedback Mechanisms to Improve Communication
- 4.4 Utilize Digital Tools to Enhance Information Security Training
- 4.5 Evaluate Training Program Effectiveness and Outcomes
- 4.6 Cultivate a Culture of Continuous Learning in Security Practices

• 5 Monitoring, Auditing, and Continuous Improvement in Information Security — 6 classes

- 5.1 Identify Key Components of Monitoring in Information Security
- 5.2 Explore Effective Auditing Techniques for Security Compliance
- 5.3 Analyze the Role of Leadership in Security Monitoring Practices
- 5.4 Develop a Continuous Improvement Plan for Information Security
- 5.5 Implement Metrics for Measuring Security Audit Effectiveness
- 5.6 Create an Action Plan for Regular Review and Adaptation of Security Policies

6 Risk Management Strategies

5 chapters · 30 classes **65 marks**

- **1 Understanding Risk Management Fundamentals** — 6 classes
  - 1.1 Define Key Concepts in Risk Management
  - 1.2 Identify Types of Risks in Information Security
  - 1.3 Analyze the Risk Management Process and Its Phases
  - 1.4 Evaluate Risk Assessment Techniques for Information Security
  - 1.5 Develop Risk Mitigation Strategies for Identified Risks
  - 1.6 Implement a Risk Monitoring and Review Plan
- **2 Identifying and Assessing Risks in Information Security** — 6 classes
  - 2.1 Define Information Security Risks and Their Implications
  - 2.2 Identify Common Threats to Information Security
  - 2.3 Assess the Impact of Information Security Risks
  - 2.4 Evaluate Likelihood and Vulnerability in Risk Scenarios
  - 2.5 Conduct a Risk Assessment Workshop
  - 2.6 Develop a Risk Mitigation Plan Based on Assessment Findings
- **3 Developing Effective Risk Mitigation Strategies** — 6 classes
  - 3.1 Identify Key Risks in Information Security Management
  - 3.2 Analyze Risk Impact and Likelihood for Effective Assessment
  - 3.3 Develop Tailored Risk Mitigation Strategies for Vulnerabilities
  - 3.4 Implement Risk Control Measures and Best Practices
  - 3.5 Monitor and Review Risk Mitigation Strategies for Continuous Improvement
  - 3.6 Communicate Risk Management Plans to Stakeholders Effectively
- **4 Monitoring and Reviewing Risk Management Processes** — 6 classes
  - 4.1 Define Key Metrics for Monitoring Risk Management Effectiveness
  - 4.2 Establish a Framework for Regular Risk Assessment Reviews
  - 4.3 Analyze Data Sources for Comprehensive Risk Monitoring
  - 4.4 Implement Tools and Technologies for Risk Management Tracking
  - 4.5 Develop Action Plans Based on Review Findings
  - 4.6 Communicate Risk Management Insights to Stakeholders Effectively
- **5 Integrating Risk Management into Leadership Practices** — 6 classes
  - 5.1 Identify Key Components of Risk Management in Leadership
  - 5.2 Assess the Impact of Risk on Organizational Goals
  - 5.3 Develop Risk Assessment Frameworks for Decision Making
  - 5.4 Integrate Risk Management into Strategic Planning Processes
  - 5.5 Communicate Risk Management Strategies Effectively to Stakeholders
  - 5.6 Evaluate the Effectiveness of Risk Management Practices in Leadership