LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001 — 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 MGT-MGS-27001 • ISO Management & Services

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	**MGT-MGS-27001**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Continuous Improvement Practices

5 chapters · 30 classes · **45 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 Practices
  - 1.3 Analyze the Role of Leadership in Continuous Improvement
  - 1.4 Evaluate Common Continuous Improvement Methodologies
  - 1.5 Implement Continuous Improvement Strategies in Information Security
  - 1.6 Measure and Review the Impact of Continuous Improvement Efforts
- **2 Key Principles and Methodologies for Continuous Improvement** — 6 classes
  - 2.1 Identify Key Principles of Continuous Improvement
  - 2.2 Explore Common Methodologies for Continuous Improvement
  - 2.3 Analyze the Role of Leadership in Continuous Improvement
  - 2.4 Apply the PDCA Cycle in Continuous Improvement Initiatives
  - 2.5 Evaluate the Impact of Continuous Improvement on Information Security
  - 2.6 Develop an Action Plan for Implementing Continuous Improvement Practices
- **3 Establishing Metrics and KPIs for Continuous Improvement** — 6 classes
  - 3.1 Define Key Concepts of Continuous Improvement
  - 3.2 Identify Essential Metrics for Information Security
  - 3.3 Set SMART KPIs for Continuous Improvement
  - 3.4 Collect and Analyze Data for Continuous Improvement
  - 3.5 Utilize Dashboards to Monitor Performance Metrics
  - 3.6 Review and Adjust KPIs for Ongoing Improvement
- **4 Conducting Effective Audits and Reviews for Improvement** — 6 classes
  - 4.1 Identify Key Objectives for Audits and Reviews
  - 4.2 Develop Effective Audit Checklists and Tools
  - 4.3 Conducting Thorough Data Collection for Audits
  - 4.4 Analyze Audit Findings to Identify Areas for Improvement
  - 4.5 Implement Action Plans Based on Audit Results
  - 4.6 Review and Refine Audit Processes for Continuous Improvement
- **5 Integrating Feedback Loops for Sustained Improvement** — 6 classes
  - 5.1 Establishing the Foundation for Feedback Loops
  - 5.2 Identifying Key Metrics for Continuous Improvement
  - 5.3 Collecting Feedback Effectively: Tools and Techniques
  - 5.4 Analyzing Feedback for Actionable Insights
  - 5.5 Implementing Changes Based on Feedback Analysis
  - 5.6 Evaluating the Effectiveness of Feedback Loops

2 Implementation Strategies

5 chapters · 30 classes **85 marks**

- **1 Understanding ISO 27001: Key Principles and Framework** — 6 classes
  - 1.1 Define ISO 27001 and Its Importance in Information Security
  - 1.2 Identify Key Principles of Information Security Management
  - 1.3 Explore the ISO 27001 Framework and Structure
  - 1.4 Analyze the Risk Management Process in ISO 27001
  - 1.5 Examine Roles and Responsibilities in Implementing ISO 27001
  - 1.6 Develop an Action Plan for ISO 27001 Implementation
- **2 Risk Assessment Methodologies for ISO 27001 Implementation** — 6 classes
  - 2.1 Identify Key Risk Assessment Terminology for ISO 27001
  - 2.2 Analyze Different Risk Assessment Methodologies for Implementation
  - 2.3 Evaluate the Role of Threats and Vulnerabilities in Risk Assessment
  - 2.4 Develop Risk Scenarios Relevant to ISO 27001 Framework
  - 2.5 Create a Risk Assessment Matrix for Prioritization of Risks
  - 2.6 Formulate a Risk Mitigation Strategy Based on Assessment Results
- **3 Defining and Documenting ISMS Policies and Procedures** — 6 classes
  - 3.1 Identify Key Components of ISMS Policies
  - 3.2 Analyze Regulatory and Compliance Requirements for ISMS
  - 3.3 Develop Effective ISMS Objectives and Goals
  - 3.4 Draft Comprehensive ISMS Documentation Framework
  - 3.5 Implement Review Processes for ISMS Policies and Procedures
  - 3.6 Communicate and Train Stakeholders on ISMS Policies
- **4 Developing a Security Awareness and Training Program** — 6 classes
  - 4.1 Identify Key Security Awareness Objectives
  - 4.2 Assess Current Security Knowledge Levels
  - 4.3 Develop Engaging Training Content
  - 4.4 Implement Training Delivery Methods
  - 4.5 Evaluate the Effectiveness of the Training Program
  - 4.6 Reinforce Learning Through Ongoing Awareness Campaigns
- **5 Monitoring, Review, and Continual Improvement of the ISMS** — 6 classes
  - 5.1 Identify Key Metrics for ISMS Monitoring
  - 5.2 Establish Review Processes for ISMS Effectiveness
  - 5.3 Conduct Internal Audits of the ISMS Framework
  - 5.4 Analyze Audit Findings and Identify Improvement Areas
  - 5.5 Implement Action Plans for Continual Improvement
  - 5.6 Communicate ISMS Performance and Changes to Stakeholders

3 Introduction to ISO 27001

5 chapters · 30 classes **85 marks**

- **1 Understanding the Basics of ISO 27001** — 6 classes
  - 1.1 Define ISO 27001 and Its Importance in Information Security
  - 1.2 Identify Key Components and Structure of ISO 27001
  - 1.3 Explore Risks and Threats Addressed by ISO 27001
  - 1.4 Explain the Role of Leadership in Implementing ISO 27001
  - 1.5 Discuss Common Challenges in Achieving ISO 27001 Certification
  - 1.6 Apply ISO 27001 Principles to Develop a Simple Information Security Plan
- **2 Key Terms and Definitions in ISO 27001** — 6 classes
  - 2.1 Understand the Importance of Information Security Management
  - 2.2 Define Key Terms Related to ISO 27001
  - 2.3 Explore the Structure of ISO 27001 Terminology
  - 2.4 Identify Roles and Responsibilities in Information Security
  - 2.5 Examine the Concept of Risk Assessment in ISO 27001
  - 2.6 Apply Key Definitions to Real-World Scenarios
- **3 The Structure of ISO 27001: An Overview** — 6 classes
  - 3.1 Identify the Key Components of ISO 27001
  - 3.2 Explain the Purpose and Importance of ISO 27001
  - 3.3 Explore the Structure of the ISO 27001 Standard
  - 3.4 Compare ISO 27001 with Other Information Security Standards
  - 3.5 Discuss the Role of Leadership in ISO 27001 Implementation
  - 3.6 Apply the Principles of ISO 27001 to Real-World Scenarios
- **4 Implementing an Information Security Management System** — 6 classes
  - 4.1 Define the Key Components of an Information Security Management System
  - 4.2 Assess Organizational Security Needs and Requirements
  - 4.3 Develop Information Security Policies and Procedures
  - 4.4 Identify and Evaluate Information Security Risks
  - 4.5 Implement Controls and Mitigation Strategies for Security Risks
  - 4.6 Monitor and Improve the Information Security Management System
- **5 Preparing for ISO 27001 Certification** — 6 classes
  - 5.1 Understand the Importance of ISO 27001 Certification
  - 5.2 Identify Key Elements of Information Security Management
  - 5.3 Assess Your Organization's Readiness for ISO 27001
  - 5.4 Develop a Roadmap for Achieving Certification
  - 5.5 Engage Stakeholders in the Certification Process
  - 5.6 Implement Initial Steps Towards ISO 27001 Compliance

4 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 the Importance of Organizational Culture in Security Leadership
- 1.3 Identify Stakeholder Expectations and Communication Strategies
- 1.4 Assess Leadership Styles and Their Impact on Information Security
- 1.5 Develop a Leadership Action Plan for Information Security Initiatives
- 1.6 Evaluate Real-World Case Studies of Leadership in Security Management

• 2 Developing a Security Culture within an Organization — 6 classes

- 2.1 Define the Elements of a Security Culture
- 2.2 Identify Key Stakeholders in Information Security
- 2.3 Assess Current Organizational Security Practices
- 2.4 Develop Training Programs for Security Awareness
- 2.5 Foster Open Communication About Security Issues
- 2.6 Measure and Evaluate the Effectiveness of the Security Culture

• 3 Risk Management and Strategic Decision-Making in Information Security — 6 classes

- 3.1 Analyze Key Risk Factors in Information Security
- 3.2 Develop a Risk Assessment Framework for Organizations
- 3.3 Evaluate Information Security Threats and Vulnerabilities
- 3.4 Prioritize Risks Based on Strategic Objectives
- 3.5 Formulate Strategic Decisions to Mitigate Risks
- 3.6 Implement a Risk Management Plan and Monitor Effectiveness

• 4 Engaging Stakeholders and Communicating Security Objectives — 6 classes

- 4.1 Identify Key Stakeholders in Information Security
- 4.2 Analyze Stakeholder Needs and Expectations
- 4.3 Develop Clear Security Objectives Aligned to Stakeholders
- 4.4 Create a Communication Plan for Security Initiatives
- 4.5 Implement Strategies for Engaging Stakeholders
- 4.6 Evaluate the Effectiveness of Communication on Security Understanding

• 5 Assessing and Improving Leadership Effectiveness in Information Security — 6 classes

- 5.1 Define Leadership Effectiveness in Information Security
- 5.2 Identify Key Leadership Competencies for Information Security
- 5.3 Assess Current Leadership Practices in Information Security
- 5.4 Analyze Challenges to Leadership Effectiveness in Information Security
- 5.5 Develop Strategies for Enhancing Leadership Skills in Information Security
- 5.6 Implement and Monitor Leadership Improvement Plans in Information Security

5 Monitoring and Measurement

5 chapters · 30 classes **65 marks**

• 1 Understanding Monitoring and Measurement in ISO 27001 — 6 classes

- 1.1 Define the Role of Monitoring in ISO 27001
- 1.2 Identify Key Metrics for Information Security
- 1.3 Differentiate Between Qualitative and Quantitative Measurements
- 1.4 Establish Effective Monitoring Strategies
- 1.5 Analyze Data Collection Methods for ISO 27001
- 1.6 Implement Continuous Improvement through Measurement Feedback

• 2 Establishing Key Performance Indicators (KPIs) for Information Security — 6 classes

- 2.1 Define Information Security Objectives and Goals
- 2.2 Identify Key Performance Indicators (KPIs) for Security Assessment
- 2.3 Establish Baseline Metrics for Information Security Effectiveness
- 2.4 Align KPIs with Business Objectives and Risk Management
- 2.5 Develop a KPI Monitoring and Reporting Framework
- 2.6 Analyze KPI Results and Drive Continuous Improvement in Security

• 3 Data Collection Techniques for Monitoring Security Performance — 6 classes

- 3.1 Identify Key Performance Indicators for Information Security
- 3.2 Explore Qualitative Data Collection Methods for Security Metrics
- 3.3 Implement Quantitative Data Collection Techniques for Performance Tracking
- 3.4 Assess the Role of Automated Tools in Data Collection
- 3.5 Analyze Data Trends to Measure Security Performance Over Time
- 3.6 Develop a Data Collection Strategy for Continuous Improvement

• 4 Analyzing and Interpreting Monitoring Data — 6 classes

- 4.1 Understand the Purpose of Monitoring Data in ISO 27001
- 4.2 Identify Key Metrics for Effective Information Security Management
- 4.3 Collect and Organize Monitoring Data for Analysis
- 4.4 Analyze Monitoring Data to Identify Trends and Patterns
- 4.5 Interpret Analysis Results to Inform Security Decisions
- 4.6 Communicate Findings and Recommendations to Stakeholders

• 5 Reporting and Communicating Monitoring Results to Stakeholders — 6 classes

- 5.1 Identify Key Stakeholders for Monitoring Results
- 5.2 Define Metrics for Effective Reporting
- 5.3 Develop a Template for Monitoring Reports
- 5.4 Tailor Communication Strategies for Different Stakeholders
- 5.5 Present Monitoring Results Clearly and Effectively
- 5.6 Solicit Feedback to Improve Future Reporting Processes

6 Risk Management Framework

5 chapters · 30 classes **105 marks**

- **1 Foundations of Risk Management in ISO 27001** — 6 classes
  - 1.1 Define Key Concepts in Risk Management Framework for ISO 27001
  - 1.2 Identify and Analyze Information Security Risks
  - 1.3 Evaluate the Importance of Risk Assessment in ISO 27001
  - 1.4 Develop Risk Treatment Options for Information Security
  - 1.5 Implement Risk Control Measures in Line with ISO 27001
  - 1.6 Review and Improve Risk Management Practices in ISO 27001
- **2 Risk Assessment Methodologies and Techniques** — 6 classes
  - 2.1 Identify Risk Assessment Methodologies in ISO 27001
  - 2.2 Compare Qualitative and Quantitative Risk Assessment Techniques
  - 2.3 Analyze the Role of Context in Risk Assessment
  - 2.4 Evaluate Risk Assessment Tools and Their Applications
  - 2.5 Develop a Risk Assessment Matrix for ISO 27001 Compliance
  - 2.6 Apply Risk Assessment Techniques in Real-World Scenarios
- **3 Risk Treatment Options and Decision Making** — 6 classes
  - 3.1 Identify Risk Treatment Options Effectively
  - 3.2 Assess the Feasibility of Risk Treatment Strategies
  - 3.3 Evaluate Cost-Benefit Analysis in Risk Decisions
  - 3.4 Prioritize Risk Treatment Options Strategically
  - 3.5 Develop a Risk Treatment Plan with Clear Objectives
  - 3.6 Implement and Monitor Risk Treatment Decisions
- **4 Monitoring and Reviewing Risks within the ISMS** — 6 classes
  - 4.1 Define Key Concepts in Risk Monitoring for ISMS
  - 4.2 Identify Tools and Techniques for Risk Assessment Review
  - 4.3 Establish Criteria for Evaluating Risk Effectiveness
  - 4.4 Develop a Risk Monitoring Schedule for Continuous Improvement
  - 4.5 Analyze Case Studies of Successful Risk Monitoring in ISMS
  - 4.6 Create an Action Plan for Implementing Risk Reviews
- **5 Developing a Risk Management Framework for ISO 27001** — 6 classes
  - 5.1 Identify Key Components of a Risk Management Framework
  - 5.2 Assess Organizational Context and Risk Appetite
  - 5.3 Conduct a Comprehensive Risk Assessment Process
  - 5.4 Develop Risk Treatment Plans Aligned with ISO 27001
  - 5.5 Implement Risk Monitoring and Review Procedures
  - 5.6 Create a Communication Strategy for Risk Management Findings