LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001CSRM — Information Security for Patient Data Protection

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

CURRICULUM

1 Data Protection Regulations

5 chapters · 30 classes · **45 marks**

- **1 Fundamentals of Data Protection Regulations** — 6 classes
  - 1.1 Understand Key Data Protection Terminology
  - 1.2 Identify Key Data Protection Regulations in the UK
  - 1.3 Explain the Principles of Data Protection
  - 1.4 Recognize the Roles and Responsibilities Under Data Protection Laws
  - 1.5 Assess Risks to Patient Data and Compliance Gaps
  - 1.6 Implement Best Practices for Patient Data Protection
- **2 Overview of UK Data Protection Legislation** — 6 classes
  - 2.1 Identify Key Components of UK Data Protection Legislation
  - 2.2 Examine the Principles of Data Protection Compliance
  - 2.3 Analyze the Rights of Individuals Under Data Protection Laws
  - 2.4 Differentiate Between GDPR and the Data Protection Act 2018
  - 2.5 Evaluate the Role of the Information Commissioner's Office
  - 2.6 Develop Strategies for Ensuring Compliance in Patient Data Management
- **3 Principles of Data Handling and Patient Consent** — 6 classes
  - 3.1 Understand the Foundations of Data Protection Regulations
  - 3.2 Identify the Key Principles of Data Handling
  - 3.3 Explore the Importance of Patient Consent
  - 3.4 Analyze Case Studies on Data Breaches and Patient Trust
  - 3.5 Implement Best Practices for Data Handling in Healthcare
  - 3.6 Evaluate Strategies for Ensuring Informed Patient Consent
- **4 Data Breach Management and Reporting Requirements** — 6 classes
  - 4.1 Identify and Define Data Breaches in Healthcare
  - 4.2 Understand Legal and Regulatory Frameworks for Reporting Data Breaches
  - 4.3 Assess the Impact of a Data Breach on Patient Privacy and Trust
  - 4.4 Develop a Data Breach Response Plan for Healthcare Providers
  - 4.5 Implement Effective Communication Strategies Post-Breach
  - 4.6 Review and Enhance Data Protection Measures After a Breach
- **5 Compliance Strategies for Health Care Organizations** — 6 classes
  - 5.1 Assess Current Compliance: Evaluate Existing Data Protection Practices
  - 5.2 Identify Key Regulations: Understand Relevant Data Protection Laws
  - 5.3 Develop Policies: Create Effective Data Protection Guidelines
  - 5.4 Implement Training: Educate Staff on Compliance Responsibilities
  - 5.5 Monitor Compliance: Establish Ongoing Audit and Review Processes
  - 5.6 Respond to Breaches: Create a Robust Incident Response Plan

2 Information Security Principles

5 chapters · 30 classes **85 marks**

- **1 Understanding Information Security Fundamentals in Healthcare** — 6 classes
  - 1.1 Define Key Terms in Information Security
  - 1.2 Identify Types of Patient Data and Their Sensitivity
  - 1.3 Explore the Importance of Information Security in Healthcare
  - 1.4 Analyze Common Threats to Patient Data Security
  - 1.5 Review Key Components of an Information Security Policy
  - 1.6 Implement Best Practices for Protecting Patient Data
- **2 Regulatory Frameworks and Compliance in Patient Data Protection** — 6 classes
  - 2.1 Examine Key Regulatory Frameworks Impacting Patient Data
  - 2.2 Identify Legal Obligations for Patient Data Protection
  - 2.3 Differentiate Between Compliance Standards in Healthcare
  - 2.4 Analyze the Role of Data Protection Authorities
  - 2.5 Evaluate Risks and Challenges in Compliance Implementation
  - 2.6 Develop an Action Plan for Ensuring Compliance
- **3 Risk Management for Patient Data Security** — 6 classes
  - 3.1 Identify Key Risks in Patient Data Security
  - 3.2 Assess the Impact of Identified Risks on Patient Data
  - 3.3 Evaluate Current Security Measures Against Risks
  - 3.4 Develop Mitigation Strategies for High-Risk Scenarios
  - 3.5 Implement Monitoring Procedures for Risk Management
  - 3.6 Communicate Risk Management Findings to Stakeholders
- **4 Implementing Security Controls and Best Practices** — 6 classes
  - 4.1 Assess Current Security Posture for Patient Data
  - 4.2 Identify and Prioritize Security Controls
  - 4.3 Develop and Implement Access Control Policies
  - 4.4 Establish Procedures for Data Encryption and Protection
  - 4.5 Monitor and Evaluate Security Control Effectiveness
  - 4.6 Train Staff on Best Practices for Information Security
- **5 Leadership Strategies for Sustaining Information Security** — 6 classes
  - 5.1 Establish Clear Information Security Objectives
  - 5.2 Foster a Culture of Security Awareness Among Staff
  - 5.3 Implement Effective Communication Strategies for Security Leadership
  - 5.4 Engage Stakeholders in Information Security Initiatives
  - 5.5 Develop Policies for Sustaining Information Security Efforts
  - 5.6 Measure and Report on Information Security Performance Metrics

3 ISO 27001 Standards Compliance

5 chapters · 30 classes **85 marks**

- **1 Understanding ISO 27001 Standards in Healthcare** — 6 classes
  - 1.1 Explain the Purpose of ISO 27001 in Healthcare
  - 1.2 Identify Key Components of ISO 27001 Standards
  - 1.3 Assess the Importance of Risk Assessment in Patient Data Protection
  - 1.4 Analyze the Role of Leadership in ISO 27001 Compliance
  - 1.5 Develop Strategies for Implementing ISO 27001 in Healthcare Settings
  - 1.6 Evaluate Case Studies of ISO 27001 Implementation in Healthcare
- **2 Key Components of an Information Security Management System (ISMS)** — 6 classes
  - 2.1 Define Key Components of an ISMS
  - 2.2 Identify Roles and Responsibilities in Information Security
  - 2.3 Assess Risks to Patient Data within the ISMS Framework
  - 2.4 Develop Policies for Information Security Management
  - 2.5 Implement Monitoring and Review Mechanisms for ISMS
  - 2.6 Create an Action Plan for Continuous Improvement of ISMS
- **3 Risk Management Strategies for Patient Data Protection** — 6 classes
  - 3.1 Identify Key Risks to Patient Data Security
  - 3.2 Assess the Impact of Data Breaches on Patient Privacy
  - 3.3 Develop Risk Mitigation Strategies for Patient Data
  - 3.4 Implement Access Controls to Safeguard Patient Information
  - 3.5 Monitor and Review Risk Management Effectiveness
  - 3.6 Communicate Risk Management Policies to Staff
- **4 Implementing Security Controls and Compliance Measures** — 6 classes
  - 4.1 Identify Key Security Controls for Patient Data Protection
  - 4.2 Assess Risks and Vulnerabilities in Current Systems
  - 4.3 Design Security Measures Aligned with ISO 27001 Standards
  - 4.4 Implement Effective Access Controls and Authentication Mechanisms
  - 4.5 Monitor and Evaluate Security Control Effectiveness
  - 4.6 Develop a Compliance Audit Plan for Continuous Improvement
- **5 Monitoring, Auditing, and Continual Improvement of ISMS** — 6 classes
  - 5.1 Identify Key Metrics for Monitoring ISMS Performance
  - 5.2 Develop an Effective Auditing Process for ISMS
  - 5.3 Implement Tools for Continuous Monitoring of Patient Data Security
  - 5.4 Analyze Audit Results to Identify Areas for Improvement
  - 5.5 Create an Action Plan for ISMS Enhancement Based on Findings
  - 5.6 Foster a Culture of Continuous Improvement in Information Security Practices

4 Measuring Security Effectiveness

5 chapters · 30 classes **45 marks**

- **1 Foundations of Information Security Measurements** — 6 classes
  - 1.1 Define Key Concepts in Information Security Measurements
  - 1.2 Identify Types of Security Metrics Relevant to Patient Data
  - 1.3 Analyze the Importance of Baselines in Security Measurements
  - 1.4 Explore Tools and Techniques for Measuring Security Effectiveness
  - 1.5 Develop a Framework for Evaluating Security Metrics
  - 1.6 Apply Measurement Techniques to Case Studies in Patient Data Protection
- **2 Key Performance Indicators (KPIs) for Security Programs** — 6 classes
  - 2.1 Identify Key Performance Indicators for Security Programs
  - 2.2 Evaluate the Relevance of KPIs in Measuring Security Effectiveness
  - 2.3 Analyze Data Collection Methods for KPI Measurement
  - 2.4 Develop a Framework for Monitoring Security KPI Performance
  - 2.5 Implement Corrective Actions Based on KPI Insights
  - 2.6 Communicate KPI Results to Stakeholders Effectively
- **3 Quantitative vs. Qualitative Assessment Techniques** — 6 classes
  - 3.1 Differentiate Between Quantitative and Qualitative Assessment Techniques
  - 3.2 Identify Key Metrics for Quantitative Security Assessment
  - 3.3 Explore Tools for Quantitative Assessment of Security Effectiveness
  - 3.4 Analyze Qualitative Assessment Methods in Patient Data Protection
  - 3.5 Compare the Benefits and Limitations of Each Assessment Technique
  - 3.6 Develop a Mixed-Methods Approach for Measuring Security Effectiveness
- **4 Implementing Audits and Security Assessments** — 6 classes
  - 4.1 Define the Objectives of Security Audits
  - 4.2 Identify Key Components of a Security Assessment
  - 4.3 Develop an Effective Audit Plan for Patient Data Security
  - 4.4 Implement Data Collection Techniques During Audits
  - 4.5 Analyze Audit Findings and Identify Security Gaps
  - 4.6 Create an Action Plan for Continuous Security Improvement
- **5 Continuous Improvement and Compliance Monitoring** — 6 classes
  - 5.1 Assess Current Security Measures for Patient Data
  - 5.2 Identify Key Performance Indicators for Security Effectiveness
  - 5.3 Implement a Continuous Improvement Framework
  - 5.4 Develop a Compliance Monitoring Checklist
  - 5.5 Evaluate Incident Response and Recovery Protocols
  - 5.6 Conduct a Security Audit and Report Findings

5 Risk Assessment and Management

5 chapters · 30 classes **85 marks**

- **1 Fundamentals of Risk Assessment in Healthcare** — 6 classes
  - 1.1 Define Key Concepts of Risk Assessment in Healthcare
  - 1.2 Identify Types of Risks Affecting Patient Data
  - 1.3 Evaluate the Impact of Data Breaches on Patient Care
  - 1.4 Explore Legal and Ethical Considerations in Risk Management
  - 1.5 Develop Risk Assessment Strategies for Healthcare Settings
  - 1.6 Implement Continuous Monitoring and Improvement of Risk Practices
- **2 Identifying and Analyzing Risks to Patient Data** — 6 classes
  - 2.1 Define Patient Data and Its Security Importance
  - 2.2 Identify Common Risks to Patient Data in Healthcare Settings
  - 2.3 Analyze the Impact of Data Breaches on Patient Care
  - 2.4 Evaluate Current Threats and Vulnerabilities to Patient Data
  - 2.5 Conduct a Risk Assessment for Patient Data Scenarios
  - 2.6 Develop Mitigation Strategies for Identified Risks
- **3 Risk Evaluation and Prioritization Strategies** — 6 classes
  - 3.1 Identify Key Risk Indicators for Patient Data Security
  - 3.2 Assess Vulnerabilities in Patient Data Management Systems
  - 3.3 Evaluate Potential Impact of Data Breaches on Patient Privacy
  - 3.4 Prioritize Risks Based on Likelihood and Impact Assessment
  - 3.5 Develop Mitigation Strategies for High-Priority Risks
  - 3.6 Implement a Risk Monitoring Framework for Continuous Improvement
- **4 Implementing Risk Treatment Plans** — 6 classes
  - 4.1 Identify Key Risks in Patient Data Management
  - 4.2 Evaluate the Impact of Identified Risks on Patient Confidentiality
  - 4.3 Develop Mitigation Strategies for High-Risk Scenarios
  - 4.4 Formulate a Risk Treatment Plan Template
  - 4.5 Gather Stakeholder Input on Proposed Risk Treatment Plans
  - 4.6 Implement and Monitor the Effectiveness of Risk Treatment Plans
- **5 Monitoring and Reviewing Risk Management Processes** — 6 classes
  - 5.1 Evaluate Existing Risk Management Frameworks
  - 5.2 Identify Key Performance Indicators for Monitoring Risks
  - 5.3 Conduct Regular Risk Assessments to Ensure Compliance
  - 5.4 Implement Continuous Monitoring Techniques for Patient Data
  - 5.5 Review and Analyze Incident Reports for Risk Insights
  - 5.6 Communicate Risk Management Findings to Stakeholders

6 Strategic Security Leadership

5 chapters · 30 classes **85 marks**

• 1 Understanding the Importance of Information Security in Patient Data Protection — 6 classes

- › 1.1 Define Information Security and Its Relevance to Patient Data
- › 1.2 Identify Key Threats to Patient Data Security
- › 1.3 Explore Legal and Ethical Considerations in Patient Data Protection
- › 1.4 Assess the Impact of Data Breaches on Healthcare Organizations
- › 1.5 Develop Strategies for Effective Patient Data Security Management
- › 1.6 Implement Best Practices for Maintaining Information Security Standards

• 2 ISO 27001: Framework and Requirements for Effective Security Management — 6 classes

- › 2.1 Define the ISO 27001 Framework for Information Security Management
- › 2.2 Identify Key Requirements for Implementing ISO 27001 Standards
- › 2.3 Analyze the Importance of Risk Assessment in Patient Data Protection
- › 2.4 Develop Policies and Procedures for Compliance with ISO 27001
- › 2.5 Evaluate the Role of Leadership in Sustaining Information Security Practices
- › 2.6 Create an Action Plan for Implementing ISO 27001 in Healthcare Settings

• 3 Risk Assessment and Management in Healthcare Settings — 6 classes

- › 3.1 Identify Key Risks to Patient Data in Healthcare
- › 3.2 Assess Vulnerabilities in Current Healthcare Security Practices
- › 3.3 Analyze Potential Impact of Data Breaches on Patient Care
- › 3.4 Develop a Risk Matrix for Healthcare Data Management
- › 3.5 Create a Risk Mitigation Strategy for Patient Data Protection
- › 3.6 Implement Continuous Monitoring and Improvement of Security Measures

• 4 Operationalizing Security Policies: Best Practices for Implementation — 6 classes

- › 4.1 Define Security Policies: Establishing Clear Guidelines for Patient Data Protection
- › 4.2 Assess Risk: Identifying Vulnerabilities in Information Security Practices
- › 4.3 Engage Stakeholders: Building a Collaborative Approach to Policy Implementation
- › 4.4 Develop Training Modules: Educating Staff on Security Policies and Best Practices
- › 4.5 Implement Monitoring Mechanisms: Ensuring Ongoing Compliance and Policy Adherence
- › 4.6 Evaluate and Revise Policies: Continuous Improvement in Data Protection Strategies

• 5 Leadership and Governance in Health Information Security — 6 classes

- › 5.1 Understand the Role of Leadership in Health Information Security
- › 5.2 Define Governance Frameworks for Patient Data Protection
- › 5.3 Identify Key Stakeholders in Health Information Security Initiatives
- › 5.4 Assess Risk Management Strategies for Health Information Systems
- › 5.5 Develop Effective Communication Plans for Security Governance
- › 5.6 Implement Continuous Improvement Practices in Data Protection Leadership