LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27040 — Storage Security

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 IIT-DTC-27040 • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	15	66	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**IIT-DTC-27040**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Designing Security Strategies

0 chapters · 45 marks

2 Evaluating Security Measures

0 chapters · 45 marks

3 ISO 27040 Standards Application

5 chapters · 30 classes · 105 marks

- **1 Understanding ISO 27040: Key Concepts and Principles** — 6 classes
  - 1.1 Define ISO 27040: Overview of Storage Security Principles
  - 1.2 Identify Key Concepts within ISO 27040 Framework
  - 1.3 Examine the Importance of Data Integrity and Availability in Storage
  - 1.4 Analyze Risk Management Approaches in Storage Security
  - 1.5 Explore Compliance Requirements and Best Practices for ISO 27040
  - 1.6 Apply ISO 27040 Principles to Develop a Security Strategy
- **2 Risk Management Framework in Storage Security** — 6 classes
  - 2.1 Define Risk Management Concepts in Storage Security
  - 2.2 Identify Key Risks in Storage Environments
  - 2.3 Assess Vulnerabilities in Storage Systems
  - 2.4 Implement Risk Mitigation Strategies for Storage Security
  - 2.5 Monitor and Review Risk Management Practices in Storage
  - 2.6 Develop a Risk Management Plan for ISO 27040 Compliance
- **3 Implementing Storage Security Controls** — 6 classes
  - 3.1 Identify Key Components of Storage Security Controls
  - 3.2 Evaluate Risks Associated with Storage Systems
  - 3.3 Design Effective Access Control Policies for Storage
  - 3.4 Implement Data Encryption Techniques for Storage Security
  - 3.5 Monitor and Audit Storage Systems for Compliance
  - 3.6 Develop a Response Plan for Storage Security Incidents
- **4 Monitoring and Auditing Storage Solutions** — 6 classes
  - 4.1 Identify Key Metrics for Monitoring Storage Solutions
  - 4.2 Implement Effective Monitoring Tools and Techniques
  - 4.3 Analyze Data for Storage Security Insights
  - 4.4 Conduct Internal Audits for Compliance with ISO 27040
  - 4.5 Develop Audit Reporting and Action Plans
  - 4.6 Review and Enhance Storage Monitoring Practices
- **5 Developing a Storage Security Management Plan** — 6 classes
  - 5.1 Identify Key Components of a Storage Security Management Plan
  - 5.2 Assess Current Storage Security Risks and Vulnerabilities
  - 5.3 Develop Security Controls Aligned with ISO 27040 Standards
  - 5.4 Establish Roles and Responsibilities for Storage Security
  - 5.5 Create Incident Response Procedures for Storage Security Breaches
  - 5.6 Implement and Monitor the Storage Security Management Plan

4 Leading Security Initiatives

0 chapters · 45 marks

5 Risk Management and Analysis

5 chapters · 6 classes **105 marks**

- **1 Understanding Risk Management Principles in Storage Security** — 6 classes
  - 1.1 Define Key Principles of Risk Management in Storage Security
  - 1.2 Identify Common Risks Associated with Data Storage
  - 1.3 Analyze Risk Assessment Techniques for Storage Security
  - 1.4 Evaluate the Impact of Vulnerabilities on Storage Systems
  - 1.5 Develop Mitigation Strategies for Identified Risks
  - 1.6 Create a Risk Management Plan for Storage Security Implementation
- **2 Risk Assessment Methodologies and Tools**
- **3 Identifying and Evaluating Threats to Storage Systems**
- **4 Developing and Implementing Risk Mitigation Strategies**
- **5 Monitoring and Reviewing Risk Management Processes**

6 Storage Security Fundamentals

5 chapters · 30 classes **85 marks**

- **1 Understanding Storage Security Concepts** — 6 classes
  - 1.1 Define Key Storage Security Concepts
  - 1.2 Identify Common Storage Security Risks
  - 1.3 Explore Storage Security Frameworks and Standards
  - 1.4 Analyze Data Protection Techniques for Storage
  - 1.5 Evaluate Access Control Mechanisms in Storage Security
  - 1.6 Implement Best Practices for Secure Storage Solutions
- **2 Identifying Storage Security Risks and Threats** — 6 classes
  - 2.1 Analyze Common Storage Security Threats
  - 2.2 Recognize Vulnerabilities in Storage Systems
  - 2.3 Assess Impact of Data Breaches on Storage
  - 2.4 Identify Regulatory Compliance Risks in Storage Security
  - 2.5 Evaluate Mitigation Strategies for Storage Risks
  - 2.6 Develop a Risk Management Plan for Storage Security
- **3 Implementing Access Controls in Storage Systems** — 6 classes
  - 3.1 Identify Key Access Control Concepts in Storage Security
  - 3.2 Explore Types of Access Controls for Storage Systems
  - 3.3 Assess the Role of Authentication Mechanisms in Storage Access
  - 3.4 Analyze the Importance of Authorization Protocols in Storage Systems
  - 3.5 Evaluate Access Control Policies and Their Implementation
  - 3.6 Design a Practical Access Control Strategy for a Storage Environment
- **4 Data Encryption and Protection Techniques** — 6 classes
  - 4.1 Understand the Basics of Data Encryption
  - 4.2 Identify Different Encryption Algorithms and Their Uses
  - 4.3 Explore Symmetric vs. Asymmetric Encryption Techniques
  - 4.4 Analyze Key Management Best Practices for Secure Storage
  - 4.5 Implement Data Protection Techniques for Storage Solutions
  - 4.6 Evaluate the Effectiveness of Encryption in Data Security
- **5 Monitoring and Auditing Storage Security Compliance** — 6 classes
  - 5.1 Understand the Importance of Monitoring Storage Security
  - 5.2 Identify Key Compliance Standards for Storage Security
  - 5.3 Explore Tools and Technologies for Monitoring Compliance
  - 5.4 Evaluate Effective Auditing Practices for Storage Security
  - 5.5 Analyze Case Studies on Storage Security Breaches
  - 5.6 Develop an Action Plan for Implementing Monitoring and Auditing