LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001DTC — Information Security in Data Centres

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-27001DTC • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	15	72	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**IIT-DTC-27001DTC**
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 Regulatory Frameworks

5 chapters · 12 classes · **65 marks**

- **1 Understanding Compliance in Data Centres** — 6 classes
  - 1.1 Identify Key Compliance Standards for Data Centres
  - 1.2 Explain the Importance of Regulatory Frameworks
  - 1.3 Analyze the Impact of Non-Compliance Risks
  - 1.4 Describe the Role of Leadership in Compliance Culture
  - 1.5 Develop a Compliance Checklist for Data Centre Operations
  - 1.6 Implement Best Practices for Ongoing Compliance Maintenance
- **2 Key Regulatory Frameworks for Data Centres** — 6 classes
  - 2.1 Understand Key Regulatory Frameworks Affecting Data Centres
  - 2.2 Identify ISO Standards Relevant to Data Centre Operations
  - 2.3 Explore the GDPR and Its Implications for Data Storage
  - 2.4 Analyze the Role of PCI DSS in Data Centre Security
  - 2.5 Assess Compliance Strategies for Regulatory Frameworks
  - 2.6 Develop an Implementation Plan for Adhering to Regulations
- **3 Risk Management and Compliance in Data Centres**
- **4 Auditing and Reporting for Compliance**
- **5 Maintaining Continuous Compliance in Data Centres**

2 Incident Response and Management

0 chapters · **65 marks**

3 Information Security Principles

5 chapters · 30 classes **105 marks**

1 Fundamentals of Information Security in Data Centres — 6 classes

- 1.1 Define Key Concepts of Information Security in Data Centres
- 1.2 Identify Common Threats to Data Centre Security
- 1.3 Analyze the Importance of Data Encryption in Security Protocols
- 1.4 Explore Access Control Mechanisms for Data Centres
- 1.5 Evaluate Best Practices for Incident Response in Data Centres
- 1.6 Develop a Basic Security Policy Framework for a Data Centre

2 Risk Management and Security Frameworks — 6 classes

- 2.1 Identify Key Concepts in Risk Management
- 2.2 Analyze Security Frameworks Relevant to Data Centres
- 2.3 Assess Organizational Risks and Threats
- 2.4 Develop Risk Mitigation Strategies
- 2.5 Implement Security Controls within a Framework
- 2.6 Evaluate the Effectiveness of Security Measures

3 Access Control and User Management Strategies — 6 classes

- 3.1 Identify Key Principles of Access Control in Data Centres
- 3.2 Evaluate Different Types of Access Control Models
- 3.3 Assess User Roles and Privileges for Effective Management
- 3.4 Implement Authentication Mechanisms in User Management
- 3.5 Develop a Strategy for Monitoring and Auditing Access
- 3.6 Create a Framework for Continuous Improvement in Access Control

4 Incident Response and Security Monitoring — 6 classes

- 4.1 Identify Key Components of Incident Response Plans
- 4.2 Analyze Common Types of Security Incidents in Data Centres
- 4.3 Explore Roles and Responsibilities in Incident Response Teams
- 4.4 Implement Effective Security Monitoring Techniques
- 4.5 Develop a Communication Strategy for Incident Management
- 4.6 Evaluate Incident Response Performance through Post-Incident Reviews

5 Compliance and Regulatory Considerations in Data Centres — 6 classes

- 5.1 Identify Key Compliance Frameworks for Data Centres
- 5.2 Analyze Regulatory Requirements Impacting Data Security
- 5.3 Assess Risks Associated with Non-Compliance in Data Centres
- 5.4 Implement Best Practices for Meeting Compliance Standards
- 5.5 Evaluate the Role of Audits in Ensuring Compliance
- 5.6 Develop a Compliance Action Plan for Data Centre Security

4 Risk Management Strategies

5 chapters · 30 classes **85 marks**

1 Introduction to Risk Management in Data Centres — 6 classes

- 1.1 Define Risk Management Principles in a Data Centre Context
- 1.2 Identify Common Risks Faced by Data Centres
- 1.3 Assess the Impact of Risks on Data Centre Operations
- 1.4 Evaluate Existing Risk Management Frameworks
- 1.5 Develop Strategies for Risk Mitigation in Data Centres
- 1.6 Implement a Risk Management Plan in a Data Centre Environment

2 Identifying Risks in Data Centre Operations — 6 classes

- 2.1 Analyze Common Risks in Data Centre Operations
- 2.2 Assess the Impact of Environmental Factors on Data Security
- 2.3 Identify Human-Related Risks in Data Centre Management
- 2.4 Evaluate Technological Vulnerabilities in System Infrastructure
- 2.5 Develop a Risk Assessment Framework Specifically for Data Centres
- 2.6 Implement Mitigation Strategies for Identified Risks

3 Risk Assessment Techniques for Data Centres — 6 classes

- 3.1 Identify Key Risks in Data Centre Operations
- 3.2 Evaluate the Impact of Risks on Data Centre Performance
- 3.3 Apply Qualitative Risk Assessment Techniques
- 3.4 Implement Quantitative Risk Analysis Methods
- 3.5 Develop Risk Mitigation Strategies for Identified Threats
- 3.6 Communicate Risk Assessment Findings to Stakeholders

4 Developing and Implementing Risk Mitigation Strategies — 6 classes

- 4.1 Identify Key Risks in Data Centre Operations
- 4.2 Evaluate the Impact of Identified Risks
- 4.3 Select Appropriate Risk Mitigation Techniques
- 4.4 Develop a Risk Mitigation Action Plan
- 4.5 Implement Risk Mitigation Strategies Effectively
- 4.6 Monitor and Review the Effectiveness of Mitigation Strategies

5 Monitoring and Reviewing Risk Management Processes — 6 classes

- 5.1 Identify Key Risk Indicators for Effective Monitoring
- 5.2 Establish a Framework for Reviewing Risk Management Processes
- 5.3 Utilize Data Analytics in Risk Assessment and Monitoring
- 5.4 Implement Continuous Improvement Strategies for Risk Management
- 5.5 Develop Training Programs for Risk Management Awareness
- 5.6 Conduct Regular Audits to Assess Risk Management Effectiveness

5 Security Architecture and Design

0 chapters **65 marks**

6 Team Leadership in Security Management

0 chapters **45 marks**