

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 22301DTC — Business Continuity for Data Centre Operations

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-22301DTC • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	IIT-DTC-22301DTC
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1 Business Continuity Fundamentals 5 chapters · 30 classes 65 marks • 1 Understanding Business Continuity Concepts in Data Centres — 6 classes › 1.1 Define Key Business Continuity Concepts in Data Centres › 1.2 Identify Critical Data Centre Services and Operations › 1.3 Assess Risks and Threats to Data Centre Continuity › 1.4 Develop Business Impact Analyses for Data Centre Scenarios › 1.5 Create a Business Continuity Plan for Data Centre Operations › 1.6 Implement and Test Data Centre Business Continuity Strategies • 2 Risk Assessment and Impact Analysis for Data Centres — 6 classes › 2.1 Identify Key Risks in Data Centre Operations › 2.2 Evaluate Vulnerabilities in Data Centre Systems › 2.3 Conduct a Comprehensive Impact Analysis › 2.4 Quantify the Consequences of Data Centre Disruptions › 2.5 Prioritize Risks Based on Impact Assessment › 2.6 Develop Risk Mitigation Strategies for Data Centres • 3 Developing and Implementing Business Continuity Plans — 6 classes › 3.1 Identify and Assess Business Continuity Risks › 3.2 Define Essential Functions and Recovery Time Objectives › 3.3 Develop Comprehensive Business Continuity Strategies › 3.4 Create and Document Business Continuity Plans › 3.5 Implement Training and Awareness Programs for Staff › 3.6 Evaluate and Test Business Continuity Plans for Effectiveness • 4 Testing, Maintenance, and Improvement of Business Continuity Plans — 6 classes › 4.1 Identify Key Components of Business Continuity Plans › 4.2 Develop Testing Strategies for Continuity Plans › 4.3 Implement Effective Maintenance Procedures › 4.4 Conduct Simulated Tests of Business Continuity Plans › 4.5 Analyze Test Results for Continuous Improvement › 4.6 Create an Improvement Action Plan Based on Testing Insights • 5 Leadership and Compliance in Business Continuity for Data Centres — 6 classes › 5.1 Define Business Continuity Principles for Data Centres › 5.2 Identify Key Leadership Roles in Business Continuity Management › 5.3 Examine Compliance Standards Relevant to Data Centre Operations › 5.4 Develop a Business Continuity Policy Framework › 5.5 Create Effective Communication Strategies for Crisis Situations › 5.6 Implement a Continuous Improvement Plan for Business Continuity Practices

3

Business Impact Analysis

5 chapters · 6 classes

65 marks

• 1 Understanding Business Impact Analysis Frameworks — 6 classes

- › 1.1 Define Key Concepts in Business Impact Analysis
- › 1.2 Identify Business Functions and Their Importance
- › 1.3 Assess Risks and Vulnerabilities in Data Centre Operations
- › 1.4 Determine Impact Categories for Business Continuity
- › 1.5 Develop a Business Impact Analysis Framework
- › 1.6 Apply Business Impact Analysis Results to Operational Strategies

• 2 Identifying Critical Business Functions and Resources

• 3 Assessing Risks and Vulnerabilities in Data Centre Operations

• 4 Quantifying Impact: Metrics and Measurement Techniques

• 5 Developing a Business Impact Analysis Report and Action Plan

4

Continuous Improvement in Business Continuity

0 chapters

65 marks

5

Risk Assessment and Management

5 chapters · 30 classes

85 marks

• 1 Understanding Risk Assessment Frameworks in Data Centres — 6 classes

- › 1.1 Define Key Concepts of Risk Assessment in Data Centres
- › 1.2 Identify Types of Risks Facing Data Centre Operations
- › 1.3 Explore Risk Assessment Frameworks Relevant to Data Centres
- › 1.4 Analyze the Components of a Risk Assessment Framework
- › 1.5 Conduct a Sample Risk Assessment for a Data Centre
- › 1.6 Develop a Risk Management Plan Based on Assessment Findings

• 2 Identifying Threats and Vulnerabilities in Data Centre Context — 6 classes

- › 2.1 Identify Critical Assets in Data Centre Operations
- › 2.2 Analyze Common Threats to Data Centre Integrity
- › 2.3 Assess Vulnerabilities in Physical Infrastructure
- › 2.4 Evaluate Cybersecurity Risks in Data Management
- › 2.5 Prioritize Threats Based on Impact and Likelihood
- › 2.6 Develop a Comprehensive Threat Mitigation Strategy

• 3 Analyzing Risk Impact and Likelihood in Data Centre Operations

— 6 classes

- › 3.1 Identify Key Risks in Data Centre Operations
- › 3.2 Assess the Likelihood of Risk Occurrences
- › 3.3 Evaluate the Impact of Risks on Business Functions
- › 3.4 Prioritize Risks Based on Impact and Likelihood
- › 3.5 Develop Mitigation Strategies for High-priority Risks
- › 3.6 Create a Risk Assessment Report for Data Centre Stakeholders

• 4 Developing Risk Mitigation Strategies for Data Centres — 6 classes

- › 4.1 Identify Key Risks in Data Centre Operations
- › 4.2 Analyze the Impact of Identified Risks
- › 4.3 Develop Risk Mitigation Strategies for Critical Infrastructure
- › 4.4 Implement Preventative Measures for Risk Reduction
- › 4.5 Monitor and Review Risk Mitigation Strategies
- › 4.6 Create a Risk Management Communication Plan

• 5 Monitoring and Reviewing Risk Management Practices — 6 classes

- › 5.1 Identify Key Risk Indicators for Monitoring
- › 5.2 Develop a Risk Management Review Framework
- › 5.3 Conduct Stakeholder Feedback Sessions on Risk Management
- › 5.4 Analyze Historical Data to Assess Risk Trends
- › 5.5 Implement Continuous Improvement Strategies for Risk Practices
- › 5.6 Prepare a Review Report on Risk Management Effectiveness

6

Testing and Exercising Plans

0 chapters

65 marks