

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27017 — Cloud Services Security Controls

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-INS-27017 • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	IIT-INS-27017
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1 Audit and Continuous Improvement 0 chapters45 marks	
2 Cloud Security Fundamentals 5 chapters · 30 classes105 marks	• 1 Understanding Cloud Security Basics — 6 classes › 1.1 Define Key Cloud Security Terminology › 1.2 Explain the Importance of Cloud Security Controls › 1.3 Identify Common Threats to Cloud Security › 1.4 Describe the ISO 27017 Standard for Cloud Security › 1.5 Analyze Cloud Security Roles and Responsibilities › 1.6 Implement Basic Cloud Security Best Practices • 2 ISO 27017 Framework Introduction — 6 classes › 2.1 Explore the Basics of ISO 27017 and Cloud Security › 2.2 Identify Key Concepts and Terminology in ISO 27017 › 2.3 Understand the Structure and Components of the ISO 27017 Framework › 2.4 Analyze the Benefits of Implementing ISO 27017 for Cloud Services › 2.5 Discuss the Role of Leadership in Adopting ISO 27017 Standards › 2.6 Apply ISO 27017 Principles to Real-World Cloud Security Scenarios • 3 Cloud Security Risks and Threats — 6 classes › 3.1 Identify Common Cloud Security Risks › 3.2 Analyze Vulnerabilities in Cloud Services › 3.3 Assess Threats to Cloud Data Integrity › 3.4 Evaluate Security Controls for Cloud Environments › 3.5 Develop a Risk Management Strategy for Cloud Security › 3.6 Implement Best Practices for Mitigating Cloud Security Threats • 4 Implementing Security Controls in the Cloud — 6 classes › 4.1 Identify Key Security Controls for Cloud Environments › 4.2 Assess Cloud Security Risks and Vulnerabilities › 4.3 Implement Access Control Measures in the Cloud › 4.4 Configure Data Encryption Techniques for Cloud Storage › 4.5 Establish Incident Response Protocols for Cloud Security Breaches › 4.6 Evaluate and Test Security Control Effectiveness in the Cloud • 5 Compliance and Audit Strategies for Cloud Security — 6 classes › 5.1 Identify Key Compliance Standards for Cloud Services › 5.2 Assess Risk Management Frameworks in Cloud Security › 5.3 Develop an Effective Cloud Governance Model › 5.4 Implement Audit Strategies for Cloud Environments › 5.5 Evaluate Continuous Compliance Monitoring Techniques › 5.6 Create a Cloud Security Compliance Checklist
3 Implementing Security Controls 0 chapters85 marks	
4 Policy Development and Compliance 0 chapters65 marks	

• 1 Understanding Cloud Security Risks — 6 classes

- › 1.1 Identify Key Cloud Security Risks
- › 1.2 Analyze Impact of Cloud Security Threats
- › 1.3 Assess Vulnerabilities in Cloud Environments
- › 1.4 Evaluate Risk Management Frameworks for Cloud
- › 1.5 Develop Strategies for Mitigating Cloud Risks
- › 1.6 Implement Continuous Monitoring for Cloud Security

• 2 Risk Assessment Frameworks for Cloud Services — 6 classes

- › 2.1 Identify Key Risk Assessment Frameworks for Cloud Services
- › 2.2 Analyze the Components of Risk Assessment Frameworks
- › 2.3 Evaluate the Importance of Standards Compliance in Risk Management
- › 2.4 Develop a Risk Assessment Approach Tailored for Cloud Environments
- › 2.5 Implement Risk Mitigation Strategies in Cloud Services
- › 2.6 Review and Monitor the Effectiveness of Risk Management Practices

• 3 Identifying and Evaluating Risks in Cloud Environments**• 4 Implementing Risk Mitigation Strategies****• 5 Monitoring and Continuous Improvement of Risk Management**