LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

Certificate in Information Security Fundamentals

Foundation Level

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 IT-CSI-F • IT Centres

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	24	120	445	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**IT-CSI-F**
AWARD	**Certificate**
ASSESSMENT	**445 marks — 267 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Data Protection Techniques

4 chapters · 20 classes **115 marks**

- **1 Understanding Data Protection Principles** — 5 classes
  - 1.1 Exploring Data Protection Basics
  - 1.2 Identifying Personal Data Types
  - 1.3 Analyzing Data Processing Principles
  - 1.4 Understanding Data Subject Rights
  - 1.5 Implementing Data Security Measures
- **2 Data Encryption Techniques and Implementation** — 5 classes
  - 2.1 Understanding Basic Encryption Concepts
  - 2.2 Exploring Symmetric Encryption Methods
  - 2.3 Delving into Asymmetric Encryption Techniques
  - 2.4 Implementing Encryption in Real-World Scenarios
  - 2.5 Evaluating Encryption Protocols and Best Practices
- **3 Access Control and Authentication Mechanisms** — 5 classes
  - 3.1 Understanding Access Control Concepts
  - 3.2 Exploring Authentication Mechanisms
  - 3.3 Implementing Role-Based Access Control
  - 3.4 Analyzing Multi-Factor Authentication Techniques
  - 3.5 Evaluating Effective Access Control Strategies
- **4 Data Loss Prevention and Recovery Strategies** — 5 classes
  - 4.1 Understanding Data Loss: Types and Causes
  - 4.2 Exploring Data Protection Technologies
  - 4.3 Implementing Data Loss Prevention Strategies
  - 4.4 Mastering Data Backup and Recovery Processes
  - 4.5 Evaluating and Enhancing Recovery Strategies

2 Introduction to Cybersecurity

4 chapters · 20 classes **65 marks**

- **1 Understanding Cybersecurity Fundamentals** — 5 classes
  - 1.1 Recognizing Key Cybersecurity Concepts
  - 1.2 Identifying Common Cyber Threats and Vulnerabilities
  - 1.3 Exploring the Importance of Data Security
  - 1.4 Understanding the Role of Firewalls and Antivirus
  - 1.5 Implementing Basic Cyber Hygiene Practices
- **2 Cyber Threats and Vulnerabilities** — 5 classes
  - 2.1 Identify Common Cyber Threats
  - 2.2 Understand the Impact of Cyber Threats
  - 2.3 Recognize Vulnerabilities in Information Systems
  - 2.4 Explore Techniques Used by Cyber Criminals
  - 2.5 Apply Strategies to Mitigate Cyber Risks
- **3 Cyber Defense Strategies and Technologies** — 5 classes
  - 3.1 Understanding Cyber Threats and Vulnerabilities
  - 3.2 Exploring Cyber Defense Technologies
  - 3.3 Implementing Data Protection Measures
  - 3.4 Analyzing Network Security Protocols
  - 3.5 Developing an Incident Response Plan
- **4 Regulatory and Ethical Considerations in Cybersecurity** — 5 classes
  - 4.1 Understanding Cybersecurity Regulations and Standards
  - 4.2 Exploring Key Ethical Principles in Cybersecurity
  - 4.3 Analyzing the Role of Data Protection Laws
  - 4.4 Evaluating Case Studies on Ethical Breaches
  - 4.5 Applying Best Practices for Legal and Ethical Compliance

3 Legal and Regulatory Compliance

4 chapters · 20 classes **45 marks**

- **1 Understanding Legal Frameworks in Cybersecurity** — 5 classes
  - 1.1 Exploring the Basics of Legal Frameworks in Cybersecurity
  - 1.2 Identifying Key Cybersecurity Laws and Regulations
  - 1.3 Analyzing Data Protection and Privacy Legislation
  - 1.4 Understanding Cybersecurity Compliance Requirements
  - 1.5 Applying Legal Concepts to Real-World Cybersecurity Scenarios
- **2 Data Protection and Privacy Laws** — 5 classes
  - 2.1 Understanding the Basics of Data Protection
  - 2.2 Exploring the Principles of GDPR
  - 2.3 Identifying Key Privacy Rights and Obligations
  - 2.4 Analyzing the Role of Data Protection Authorities
  - 2.5 Applying Data Protection Laws in Practice
- **3 Compliance Standards and Best Practices** — 5 classes
  - 3.1 Understand Key Compliance Standards in Information Security
  - 3.2 Explore the Impact of Regulatory Requirements on Businesses
  - 3.3 Identify Best Practices in Implementing Security Compliance
  - 3.4 Analyze Case Studies of Compliance Failures and Successes
  - 3.5 Develop Strategies for Maintaining Ongoing Compliance
- **4 Legal Implications of Security Breaches** — 5 classes
  - 4.1 Understanding Legal Definitions in Data Breaches
  - 4.2 Exploring Key Legislation Impacting Information Security
  - 4.3 Analyzing the Consequences of Security Breaches
  - 4.4 Identifying Responsibilities Under UK Data Protection Laws
  - 4.5 Applying Legal Knowledge to Security Breach Scenarios

4 Risk Management

4 chapters · 20 classes **65 marks**

- **1 Understanding Risk in Information Security** — 5 classes
  - 1.1 Defining Information Security Risk
  - 1.2 Identifying Potential Threats and Vulnerabilities
  - 1.3 Analyzing Impact and Likelihood
  - 1.4 Assessing and Prioritizing Risks
  - 1.5 Implementing Risk Mitigation Strategies
- **2 Risk Assessment Methodologies** — 5 classes
  - 2.1 Understanding Risk in Information Security
  - 2.2 Exploring Different Risk Assessment Methods
  - 2.3 Identifying and Analyzing Potential Threats
  - 2.4 Evaluating Vulnerability Impact and Likelihood
  - 2.5 Applying Risk Assessment in Real-World Scenarios
- **3 Risk Management Strategies and Controls** — 5 classes
  - 3.1 Understanding Risk Management Frameworks
  - 3.2 Identifying and Assessing Risks
  - 3.3 Implementing Risk Mitigation Strategies
  - 3.4 Evaluating Risk Controls and Their Effectiveness
  - 3.5 Adapting Risk Management to Emerging Threats
- **4 Monitoring and Reviewing Risk Management Plans** — 5 classes
  - 4.1 Understanding the Importance of Monitoring Risk Management Plans
  - 4.2 Identifying Key Metrics for Effective Risk Monitoring
  - 4.3 Techniques for Analyzing Risk Management Effectiveness
  - 4.4 Implementing Feedback Loops for Continuous Improvement
  - 4.5 Evaluating and Updating Risk Management Strategies

5 Security Policies and Procedures

4 chapters · 20 classes **90 marks**

- **1 Understanding Security Policies: Purpose and Scope** — 5 classes
  - 1.1 Defining Security Policies and Their Importance
  - 1.2 Identifying Key Components of Security Policies
  - 1.3 Exploring the Scope of Security Policies
  - 1.4 Examining Types of Security Policies
  - 1.5 Applying Security Policies to Organizational Contexts
- **2 Developing and Implementing Security Procedures** — 5 classes
  - 2.1 Understanding the Role of Security Policies
  - 2.2 Identifying Key Components of Security Procedures
  - 2.3 Designing Effective Security Procedures
  - 2.4 Implementing Security Procedures Across the Organization
  - 2.5 Evaluating and Improving Security Procedures
- **3 Compliance and Regulatory Requirements** — 5 classes
  - 3.1 Understanding the Importance of Compliance in Information Security
  - 3.2 Exploring Key Regulatory Frameworks
  - 3.3 Analyzing How to Implement Security Policies
  - 3.4 Identifying Common Compliance Challenges
  - 3.5 Evaluating Strategies for Maintaining Compliance
- **4 Monitoring and Reviewing Security Policies and Procedures** — 5 classes
  - 4.1 Understanding the Importance of Monitoring Security Policies
  - 4.2 Identifying Key Metrics for Security Policy Effectiveness
  - 4.3 Implementing Tools and Techniques for Security Monitoring
  - 4.4 Analyzing Security Policy Data for Continuous Improvement
  - 4.5 Conducting Regular Reviews and Updates of Security Procedures

6 Threats and Vulnerabilities

4 chapters · 20 classes **65 marks**

- **1 Understanding Cyber Threats** — 5 classes
  - 1.1 Defining Cyber Threats and Their Impact
  - 1.2 Identifying Common Types of Cyber Threats
  - 1.3 Exploring Threat Actors and Their Motivations
  - 1.4 Analyzing Vulnerabilities in Information Systems
  - 1.5 Implementing Basic Threat Mitigation Strategies
- **2 Identifying System Vulnerabilities** — 5 classes
  - 2.1 Understanding System Vulnerabilities
  - 2.2 Exploring Common Vulnerability Types
  - 2.3 Analyzing Real-World Vulnerability Examples
  - 2.4 Identifying Vulnerabilities in Software and Hardware
  - 2.5 Applying Tools for Vulnerability Assessment
- **3 Techniques of Exploit and Attack** — 5 classes
  - 3.1 Understanding Common Exploit Techniques
  - 3.2 Identifying System Vulnerabilities
  - 3.3 Analyzing Social Engineering Tactics
  - 3.4 Exploring Malware Delivery Methods
  - 3.5 Applying Defensive Strategies Against Exploits
- **4 Assessing and Mitigating Risks** — 5 classes
  - 4.1 Understanding Risk Assessment Fundamentals
  - 4.2 Identifying Information Security Threats
  - 4.3 Analyzing Vulnerabilities in Information Systems
  - 4.4 Developing Risk Mitigation Strategies
  - 4.5 Implementing and Evaluating Risk Controls