LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

Certificate in Cyber Security

C

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 ITC-C06 • IT Centres

UKPRN 10067351 • Registered in England and Wales, company 4984798

4	125	716	400	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**ITC-C06**
AWARD	**Certificate**
ASSESSMENT	**400 marks — 240 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1

Cyber Security Fundamentals and Threats

25 chapters · 120 classes **100 marks**

- **1 Understanding Cyber Threats and Vulnerabilities** — 4 classes
  - 1.1 Identifying Common Cyber Threats
  - 1.2 Exploring Vulnerabilities in Digital Systems
  - 1.3 Recognizing Phishing Attempts
  - 1.4 Applying Strategies to Mitigate Cyber Threats
- **2 Implementing Personal Security Practices** — 4 classes
  - 2.1 Understanding Basic Personal Security Concepts
  - 2.2 Identifying and Mitigating Common Digital Threats
  - 2.3 Creating Strong, Secure Passwords
  - 2.4 Safe Practices for Online Communication
- **3 Recognizing and Responding to Phishing Attacks** — 4 classes
  - 3.1 Understanding Phishing: Common Tactics and Techniques
  - 3.2 Identifying Phishing Emails: Key Signs and Red Flags
  - 3.3 Analyzing Real-Life Phishing Scenarios: What Went Wrong?
  - 3.4 Responding to Phishing Attempts: Best Practices and Tools
- **1 Identifying Common Digital Threats and Vulnerabilities** — 4 classes
  - 1.1 Recognizing Common Digital Threats
  - 1.2 Identifying Vulnerabilities in Digital Systems
  - 1.3 Understanding Phishing Techniques
  - 1.4 Analyzing Real-life Threat Scenarios
- **2 Techniques and Tools Used by Cybercriminals** — 4 classes
  - 2.1 Unmasking Phishing: Recognize Deceptive Emails and Websites
  - 2.2 Decoding Malware: Identify Malicious Software Threats
  - 2.3 Protecting Your Data: Understand the Methods of Data Breach
  - 2.4 Counteracting Cyber Threats: Employ Tools for Digital Protection
- **3 Strategies for Mitigating Digital Threats** — 4 classes
  - 3.1 Identifying Common Digital Threats
  - 3.2 Evaluating Risks in Digital Environments
  - 3.3 Implementing Security Measures Against Threats
  - 3.4 Practicing Safe Digital Behaviors
- **1 Understanding Phishing: Types and Techniques** — 4 classes
  - 1.1 Exploring the Basics: What is Phishing?
  - 1.2 Identifying Common Phishing Techniques
  - 1.3 Analyzing Real-World Phishing Examples
  - 1.4 Practicing Prevention: How to Protect Yourself
- **2 Recognizing Phishing Attempts: Indicators and Red Flags** — 4 classes
  - 2.1 Identifying Common Phishing Techniques
  - 2.2 Analyzing Email Content for Red Flags
  - 2.3 Exploring Websites for Phishing Indicators
  - 2.4 Applying Knowledge to Prevent Phishing Breaches
- **3 Preventive Measures and Response Strategies** — 4 classes
  - 3.1 Understanding Phishing Threats and Their Impact
  - 3.2 Identifying Common Phishing Techniques
  - 3.3 Implementing Preventive Measures Against Phishing
  - 3.4 Responding Effectively to Phishing Incidents
- **1 Understanding the Basics of Personal Digital Security** — 4 classes
  - 1.1 Recognizing Personal Digital Security Threats
  - 1.2 Exploring Common Phishing Tactics
  - 1.3 Implementing Basic Security Tools and Practices
  - 1.4 Developing a Personal Digital Security Plan
- **2 Identifying and Mitigating Common Phishing Attacks** — 4 classes
  - 2.1 Understanding Phishing: Recognizing Common Tactics
  - 2.2 Analyzing Phishing Emails: Spotting Red Flags
  - 2.3 Practicing Safe Responses: Steps to Take When Threatened
  - 2.4 Implementing Protective Measures: Strengthening Your Personal Security
- **3 Implementing Advanced Security Measures for Enhanced Protection** — 4 classes
  - 3.1 Understanding Multi-Factor Authentication for Enhanced Login Security
  - 3.2 Implementing Strong Password Practices and Management Tools
  - 3.3 Recognizing and Mitigating Advanced Phishing Tactics
  - 3.4 Updating Software and Systems for Optimal Cyber Security
- **2 Analyzing Successful Phishing Attacks and Defense Strategies** — 4 classes
  - 2.1 Understanding the Mechanics of Phishing Attacks
  - 2.2 Identifying Common Phishing Tactics and Techniques
  - 2.3 Exploring Case Studies of Real-World Phishing Incidents
  - 2.4 Developing Effective Defense Strategies Against Phishing
- **3 Evaluating Response and Recovery Post-Cyber Attack** — 4 classes
  - 3.1 Analyzing Cyber Attack Aftermaths: Key Indicators and Impacts
  - 3.2 Formulating Strategic Response Plans: Best Practices and Frameworks
  - 3.3 Implementing Recovery Tactics: Tools and Techniques
  - 3.4 Evaluating Recovery Success: Metrics and Continuous Improvement
- **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
- **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
- **24 Malware, Ransomware and Endpoint Protection** — 10 classes
  - 24.1 Types of Malicious Software
  - 24.2 How Malware Spreads
  - 24.3 Ransomware Attack Stages

2 **Network Security and Security Policies** 31 chapters · 167 classes **100 marks**

- **1 Understanding Personal Digital Security Threats** — 4 classes
  - 1.1 Identifying Common Digital Security Threats
  - 1.2 Recognizing Characteristics of Phishing Attacks
  - 1.3 Evaluating Risk Levels of Digital Interactions
  - 1.4 Implementing Basic Personal Security Measures
- **2 Identifying and Mitigating Phishing Attacks** — 4 classes
  - 2.1 Understanding the Anatomy of a Phishing Attack
  - 2.2 Recognizing Common Phishing Tactics
  - 2.3 Analyzing Real-World Phishing Examples
  - 2.4 Applying Techniques to Safeguard Personal Information
- **3 Applying Practical Security Tools and Best Practices** — 4 classes
  - 3.1 Understanding Digital Security Essentials
  - 3.2 Identifying and Avoiding Phishing Attacks
  - 3.3 Implementing Password Protection Strategies
  - 3.4 Utilizing Security Tools in Everyday Situations
- **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
- **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
- **1 Understanding Security Protocols and Architectures** — 6 classes
  - 1.1 Exploring the Basics of Security Protocols
  - 1.2 Analyzing Cryptographic Principles in Network Security
  - 1.3 Understanding Authentication and Authorization Processes
  - 1.4 Examining Secure Socket Layer (SSL) and Transport Layer Security (TLS)
  - 1.5 Investigating Virtual Private Network (VPN) Architectures
  - 1.6 Applying Security Protocols in Real-world Scenarios
- **2 Implementing Firewalls and Intrusion Detection Systems** — 6 classes
  - 2.1 Exploring Firewall Fundamentals
  - 2.2 Configuring Basic Firewall Rules
  - 2.3 Analyzing Network Traffic Using Firewalls
  - 2.4 Understanding Intrusion Detection System Types
  - 2.5 Setting Up a Basic Intrusion Detection System
  - 2.6 Integrating Firewalls with Intrusion Detection Systems
- **3 Conducting Vulnerability Assessments and Penetration Testing** — 6 classes
  - 3.1 Understanding Vulnerability Assessments
  - 3.2 Identifying Network Vulnerabilities
  - 3.3 Utilizing Tools for Vulnerability Scanning
  - 3.4 Analyzing Vulnerability Scan Results
  - 3.5 Conducting Penetration Testing Techniques
  - 3.6 Reporting and Remediating Security Vulnerabilities
- **4 Cryptography and Secure Data Transmission** — 6 classes
  - 4.1 Understanding Cryptography Fundamentals
  - 4.2 Exploring Symmetric and Asymmetric Encryption Techniques
  - 4.3 Implementing Public Key Infrastructure (PKI)
  - 4.4 Securing Data Transmission with SSL/TLS Protocols
  - 4.5 Analyzing Cryptographic Algorithms and Their Applications
  - 4.6 Applying Cryptography in Practical Scenarios
- **5 Ethical Hacking Frameworks and Legal Considerations** — 6 classes
  - 5.1 Understanding Ethical Hacking Frameworks
  - 5.2 Exploring Legal Implications of Hacking
  - 5.3 Identifying Key Components of Ethical Hacking
  - 5.4 Analyzing Case Studies on Legal and Ethical Boundaries
  - 5.5 Applying Ethical Hacking Techniques within Legal Constraints
  - 5.6 Evaluating Ethical Hacking Tools and Technologies
- **1 Understanding Network Security Basics** — 5 classes
  - 1.1 Identifying Key Network Security Threats
  - 1.2 Understanding Basic Network Security Measures
  - 1.3 Recognizing Secure Network Protocols
  - 1.4 Analyzing Encryption and Authentication Methods
  - 1.5 Applying Fundamental Network Defense Strategies
- **2 Identifying and Mitigating Network Threats** — 5 classes
  - 2.1 Understanding Network Threats: Types and Characteristics
  - 2.2 Identifying Common Network Vulnerabilities
  - 2.3 Recognising Signs of Network Threats
  - 2.4 Implementing Basic Mitigation Strategies
  - 2.5 Evaluating the Effectiveness of Network Security Measures
- **3 Implementing Access Control and Authentication** — 5 classes
  - 3.1 Understanding Access Control Models
  - 3.2 Differentiating Between Authentication Methods
  - 3.3 Implementing Role-Based Access Control
  - 3.4 Configuring Authentication Protocols
  - 3.5 Evaluating Security Risks in Access Control Systems
- **4 Network Security Tools and Best Practices** — 5 classes
  - 4.1 Understanding Network Security Tools
  - 4.2 Identifying Common Network Vulnerabilities
  - 4.3 Implementing Firewalls for Network Protection
  - 4.4 Configuring Intrusion Detection Systems
  - 4.5 Applying Best Practices for Network Security
- **5 Integrating 5G with IoT** — 5 classes
  - 5.1 Introduction to 5G Technology
  - 5.2 Understanding IoT Architecture

3 **Ethical Hacking and Penetration Testing** 16 chapters · 120 classes **100 marks**

- **1 Understanding Ethical Hacking Frameworks and Legal Considerations** — 6 classes
  - 1.1 Defining Ethical Hacking and Its Purpose
  - 1.2 Exploring Key Ethical Hacking Frameworks
  - 1.3 Comparing Ethical Hacking and Malicious Hacking
  - 1.4 Examining Legal Considerations in Hacking
  - 1.5 Understanding Privacy Laws and Regulations
  - 1.6 Applying Ethical Principles in Hacking Scenarios
- **2 Reconnaissance Techniques and Information Gathering** — 6 classes
  - 2.1 Understanding Reconnaissance in Ethical Hacking
  - 2.2 Exploring Passive Information Gathering Techniques
  - 2.3 Leveraging Active Reconnaissance Tactics
  - 2.4 Utilizing Open Source Intelligence (OSINT) Tools
  - 2.5 Applying Network Scanning and Enumeration
  - 2.6 Analyzing and Documenting Gathered Information
- **3 Network Scanning and Vulnerability Identification** — 6 classes
  - 3.1 Understanding Network Scanning Fundamentals
  - 3.2 Exploring Common Network Scanning Tools
  - 3.3 Identifying Open Ports and Services
  - 3.4 Detecting Vulnerabilities Using Automated Scanners
  - 3.5 Analyzing Vulnerability Assessment Reports
  - 3.6 Implementing Network Security Improvements
- **4 Exploitation Techniques and Gaining Access** — 6 classes
  - 4.1 Understanding Vulnerabilities and Exploits
  - 4.2 Analyzing Common Exploitation Techniques
  - 4.3 Crafting and Deploying Exploit Code
  - 4.4 Gaining Access Through Password Cracking
  - 4.5 Performing Privilege Escalation Tactics
  - 4.6 Securing Systems Against Exploitation
- **5 Post-Exploitation, Maintaining Access, and Covering Tracks** — 6 classes
  - 5.1 Understanding Post-Exploitation Activities
  - 5.2 Utilizing Persistence Mechanisms for Maintaining Access
  - 5.3 Implementing Backdoor Techniques for Ongoing Access
  - 5.4 Strategies for Covering Tracks and Avoiding Detection
  - 5.5 Analyzing Log Files for Trace Removal
  - 5.6 Applying Best Practices for Ethical Hacking Operations
- **1 Cryptography Essentials in Network Security** — 6 classes
  - 1.1 Understanding the Fundamentals of Cryptography
  - 1.2 Exploring Symmetric Encryption Algorithms
  - 1.3 Analyzing Asymmetric Encryption Processes
  - 1.4 Implementing Hash Functions for Data Integrity
  - 1.5 Applying Cryptographic Protocols in Network Security
  - 1.6 Evaluating the Role of Cryptography in Ethical Hacking
- **2 Advanced Authentication Protocols** — 6 classes
  - 2.1 Understanding Advanced Authentication Protocols
  - 2.2 Exploring Multi-Factor Authentication Techniques
  - 2.3 Analyzing Biometric Authentication Methods
  - 2.4 Implementing Secure Kerberos Protocol
  - 2.5 Comparing Token-Based Authentication Systems
  - 2.6 Evaluating Real-World Authentication Protocol Scenarios
- **3 Secure Transport Layer Protocols** — 6 classes
  - 3.1 Understand the Basics of Secure Transport Layer Protocols
  - 3.2 Explore the Functionality of SSL/TLS Protocols
  - 3.3 Analyze the Handshake Process in TLS
  - 3.4 Evaluate the Role of Certificates in Secure Connections
  - 3.5 Implement Secure Channel Establishment Practices
  - 3.6 Troubleshoot Common Issues in Transport Layer Security
- **4 Next-Generation Firewall and Intrusion Detection Systems** — 6 classes
  - 4.1 Introduction to Next-Generation Firewalls
  - 4.2 Analyzing Firewall Capabilities and Features
  - 4.3 Understanding Intrusion Detection Systems
  - 4.4 Comparing Intrusion Detection and Prevention Systems
  - 4.5 Configuring Next-Generation Firewall Policies
  - 4.6 Implementing Intrusion Detection Strategies
- **5 Incident Response and Secure Cyber Operations** — 6 classes
  - 5.1 Understanding Incident Response Frameworks
  - 5.2 Identifying and Classifying Security Incidents
  - 5.3 Implementing Incident Detection Techniques
  - 5.4 Coordinating Incident Response Teams Effectively
  - 5.5 Applying Secure Cyber Operations in Real-Time Scenarios
  - 5.6 Evaluating Post-Incident Recovery and Reporting
- **11 Planning and Scoping a Penetration Test** — 10 classes
  - 11.1 Types of Penetration Tests
  - 11.2 Defining Goals and Scope
  - 11.3 Rules of Engagement
  - 11.4 Written Authorisation and Legal Cover
  - 11.5 Client Kick-Off Meetings
  - 11.6 Choosing Methodology and Tools
  - 11.7 Building a Safe Test Lab
  - 11.8 Scheduling and Risk of Disruption
  - 11.9 Handling Sensitive Data During Testing
  - 11.10 Preparing the Test Plan Document
- **12 Web Application Penetration Testing** — 10 classes
  - 12.1 How Web Applications Are Attacked
  - 12.2 Mapping an Application
  - 12.3 Testing Input Handling
  - 12.4 Injection Flaws
  - 12.5 Broken Authentication and Sessions
  - 12.6 Access Control Weaknesses
  - 12.7 Cross-Site Scripting Testing
  - 12.8 Misconfiguration and Exposed Data
  - 12.9 Using an Intercepting Proxy
  - 12.10 Testing a Practice Web Application
- **13 Wireless and Infrastructure Attack Assessment** — 10 classes
  - 13.1 Wireless Network Security Basics
  - 13.2 Surveying Wireless Environments
  - 13.3 Testing Wireless Encryption Weaknesses
  - 13.4 Rogue Access Points
  - 13.5 Testing Network Services
  - 13.6 Testing Default and Weak Configurations
  - 13.7 Segmentation and Pivoting Concepts
  - 13.8 Testing Remote Access Services
  - 13.9 Safe Handling of Systems Found Vulnerable
  - 13.10 Practice Assessment of a Lab Network
- **14 Password Attacks and Social Engineering Assessment** — 10 classes
  - 14.1 How Passwords Are Stored and Cracked
  - 14.2 Online and Offline Password Attacks
  - 14.3 Using Wordlists and Rules
  - 14.4 Password Policy Assessment
  - 14.5 Multi-Factor Authentication Bypass Risks
  - 14.6 Social Engineering Techniques
  - 14.7 Planning Phishing Simulations
  - 14.8 Physical Security Testing Basics
  - 14.9 Awareness Findings and Metrics
  - 14.10 Reporting Human Risk Constructively
- **15 Threat Intelligence and Threat Hunting** — 10 classes
  - 15.1 What Threat Intelligence Is
  - 15.2 Sources of Threat Information
  - 15.3 Indicators of Compromise
  - 15.4 Attacker Tactics and Techniques
  - 15.5 Building Intelligence Summaries
  - 15.6 Sharing Intelligence Safely

4 **Risk, Governance, Compliance and Legislation** 53 chapters · 309 classes **100 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
- **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
- **5 Legal Compliance and Data Protection** — 5 classes
  - 5.1 Introduction to Cyber Threat Hunting
  - 5.2 Understanding Legal Compliance Frameworks
  - 5.3 Data Protection Regulations Overview
  - 5.4 Techniques for Effective Threat Hunting
  - 5.5 Reporting and Documentation Standards
- **1 Understanding Risk in Cyber Security Contexts** — 6 classes
  - 1.1 Defining Risk in Cyber Security
  - 1.2 Identifying Cyber Threats and Vulnerabilities
  - 1.3 Analyzing Impact and Likelihood of Cyber Risks
  - 1.4 Exploring Risk Assessment Frameworks
  - 1.5 Developing Cyber Risk Mitigation Strategies
  - 1.6 Evaluating and Monitoring Risk Management Effectiveness
- **2 Risk Assessment Methodologies and Tools** — 6 classes
  - 2.1 Understanding Risk Assessment Fundamentals
  - 2.2 Identifying and Categorizing Network Risks
- **5 Evaluating and Improving Compliance Posture** — 6 classes
  - 5.1 Understanding Compliance Posture: Foundations and Importance
  - 5.2 Identifying Key Compliance Gaps: Tools and Methodologies
  - 5.3 Analyzing Current Policies: Strengths and Weaknesses
  - 5.4 Implementing Changes: Strategies for Policy Improvement
  - 5.5 Monitoring Compliance: Techniques for Continuous Evaluation
  - 5.6 Enhancing Compliance Posture: Developing a Roadmap
- **1 Introduction to Strategic Information Risk Management** — 6 classes
  - 1.1 Understanding the Fundamentals of Information Risk
  - 1.2 Identifying Key Information Assets in an Organization
  - 1.3 Analyzing Potential Information Threats and Vulnerabilities
  - 1.4 Evaluating the Impact of Information Risks on Business Objectives
  - 1.5 Developing Strategic Information Risk Management Frameworks
  - 1.6 Implementing Information Risk Mitigation Strategies
- **2 Identifying and Assessing Information Risks** — 6 classes
  - 2.1 Understanding Information Risk Concepts
  - 2.2 Analyzing Information Risk Sources
  - 2.3 Categorizing Information Assets and Their Values
  - 2.4 Evaluating Potential Threats and Vulnerabilities
  - 2.5 Assessing Likelihood and Impact of Information Risks
  - 2.6 Prioritizing Information Risks Based on Assessments
- **3 Developing Risk Mitigation and Management Strategies** — 6 classes
  - 3.1 Understanding Information Risk Fundamentals
  - 3.2 Identifying Organizational Risk Factors
  - 3.3 Evaluating Risk Assessment Techniques
  - 3.4 Developing Effective Risk Mitigation Plans
  - 3.5 Implementing Risk Management Frameworks
  - 3.6 Monitoring and Adapting Risk Strategies
- **4 Implementing Information Risk Management Frameworks** — 6 classes
  - 4.1 Understanding Information Risk Management Frameworks
  - 4.2 Assessing Organisational Context and Risk Appetite
  - 4.3 Identifying and Evaluating Information Assets
  - 4.4 Developing Risk Assessment Processes
  - 4.5 Integrating Risk Management into Business Processes
  - 4.6 Monitoring and Reviewing Risk Management Frameworks
- **5 Evaluating and Improving Risk Management Processes** — 6 classes
  - 1.1 Understanding Risk Management Frameworks
  - 1.2 Identifying Key Risk Indicators
  - 1.3 Analyzing Risk Assessment Techniques
  - 1.4 Evaluating Risk Mitigation Strategies
  - 1.5 Implementing Continuous Risk Monitoring
  - 1.6 Enhancing Risk Management with Feedback Loops
- **1 Understanding Regulatory Bodies and Frameworks** — 6 classes
  - 1.1 Exploring Key Regulatory Bodies in Information Security
  - 1.2 Understanding Global Compliance Frameworks
  - 1.3 Analyzing Regional Legal Requirements for Cybersecurity
  - 1.4 Comparing International Information Security Standards
  - 1.5 Integrating Regulatory Requirements into Security Strategy
  - 1.6 Evaluating the Impact of Legislation on Information Security Practices
- **2 GDPR and Global Data Protection Laws** — 6 classes
  - 2.1 Understanding the Core Principles of GDPR
  - 2.2 Analyzing Key Definitions: Controllers, Processors, and Data Subjects
  - 2.3 Exploring Global Data Protection Laws: A Comparative Overview
  - 2.4 Identifying GDPR Compliance Requirements for Organizations
  - 2.5 Evaluating the Role of Data Protection Officers
  - 2.6 Implementing Data Breach Response Strategies
- **3 Assessing and Implementing Security Standards** — 6 classes
  - 3.1 Understanding Security Standards Frameworks
  - 3.2 Distinguishing Between Major Security Standards
  - 3.3 Evaluating Compliance Requirements
  - 3.4 Mapping Standards to Organizational Needs
  - 3.5 Implementing Security Standards Strategically

LAPT — 85 Great Portland Street, W1W 7LT, London, United Kingdom
info@lapt.org • +44 7513 283044 • lapt.org

UKPRN 10067351 • Company 4984798
Curriculum current at the date of issue.