

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

Adv Diploma in Information Security Strategy (CISO Track)

Executive 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-E • IT Centres

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	IT-CSI-E
AWARD	Certificate
ASSESSMENT	425 marks — 255 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1

Business Alignment and Communication

5 chapters · 30 classes60 marks

• 1 Understanding Business Drivers for Cybersecurity — 6 classes

› 1.1 Identifying Core Business Objectives

› 1.2 Analyzing the Role of Business Drivers in Cybersecurity

› 1.3 Exploring the Impact of Cyber Threats on Business Success

› 1.4 Mapping Cybersecurity Goals to Business Strategies

› 1.5 Evaluating Stakeholder Needs in Cybersecurity Investments

› 1.6 Developing Business-Aligned Cybersecurity Policies

• 2 Frameworks and Models for Aligning Cybersecurity with Business Strategy — 6 classes

› 2.1 Understanding the Importance of Business-Cybersecurity Alignment

› 2.2 Exploring Key Cybersecurity Frameworks

› 2.3 Evaluating Models for Integrating Cybersecurity into Business Strategy

› 2.4 Analyzing Case Studies of Effective Cybersecurity Alignment

› 2.5 Developing Business-Aligned Cybersecurity Strategies

› 2.6 Communicating Cybersecurity Strategies to Business Stakeholders

• 3 Developing a Cybersecurity Strategy Tailored to Business Needs — 6 classes

› 3.1 Understanding Business Objectives in Cybersecurity

› 3.2 Identifying Cybersecurity Needs Based on Business Goals

› 3.3 Analyzing Risks and Threats to Business Assets

› 3.4 Crafting a Cybersecurity Strategy Aligned with Business Priorities

› 3.5 Communicating Cybersecurity Plans to Business Stakeholders

› 3.6 Evaluating and Adjusting Cybersecurity Strategies for Business Impact

• 4 Effective Communication of Cybersecurity Strategies to Stakeholders — 6 classes

› 4.1 Understanding Stakeholder Perspectives in Cybersecurity

› 4.2 Crafting Clear and Concise Cybersecurity Messages

› 4.3 Building Rapport and Trust with Stakeholders

› 4.4 Utilizing Visuals and Data to Communicate Strategies

› 4.5 Tailoring Communication to Different Stakeholder Needs

› 4.6 Gaining Stakeholder Buy-In for Cybersecurity Initiatives

• 5 Measuring and Reporting Cybersecurity Performance to Business Leaders — 6 classes

› 5.1 Understanding Cybersecurity Metrics and Their Importance

› 5.2 Identifying Business-relevant Security Performance Indicators

› 5.3 Analyzing Data to Measure Cybersecurity Effectiveness

› 5.4 Developing a Cybersecurity Performance Reporting Framework

› 5.5 Communicating Cybersecurity Insights to Business Leaders

› 5.6 Translating Cybersecurity Performance into Business Value

• 1 Understanding the Landscape of Emerging Cyber Threats — 6

classes

- › 1.1 Identifying Emerging Cyber Threats
- › 1.2 Analyzing Threat Vectors and Attack Patterns
- › 1.3 Exploring Advanced Persistent Threats (APTs)
- › 1.4 Evaluating AI and Machine Learning in Cyber Attacks
- › 1.5 Understanding IoT Vulnerabilities and Risks
- › 1.6 Assessing Impacts of Quantum Computing on Cybersecurity

• 2 Advanced Threat Detection and Analysis Techniques — 6 classes

- › 2.1 Understanding Advanced Persistent Threats (APTs)
- › 2.2 Identifying Indicators of Compromise (IoCs)
- › 2.3 Leveraging Machine Learning for Threat Detection
- › 2.4 Analyzing Malware Behavior and Patterns
- › 2.5 Implementing Threat Intelligence Platforms
- › 2.6 Evaluating the Effectiveness of Detection Techniques

• 3 Harnessing AI and Machine Learning for Threat Prevention — 6

classes

- › 3.1 Understanding AI and Machine Learning in Threat Prevention
- › 3.2 Identifying Key AI Technologies for Cybersecurity
- › 3.3 Exploring Machine Learning Models in Threat Detection
- › 3.4 Implementing AI-Based Solutions for Threat Prevention
- › 3.5 Evaluating the Effectiveness of AI in Cybersecurity
- › 3.6 Addressing Challenges and Ethical Considerations

• 4 Assessing Risks Associated with Internet of Things (IoT) Security

— 6 classes

- › 4.1 Introduction to IoT Security Risks
- › 4.2 Identifying Vulnerabilities in IoT Devices
- › 4.3 Evaluating Network Security for IoT Systems
- › 4.4 Analyzing Data Privacy Concerns in IoT
- › 4.5 Mitigating Risks in IoT Environments
- › 4.6 Case Studies: Real-world IoT Security Breaches

• 5 Integrating Blockchain and Quantum Computing in Cybersecurity Strategies — 6 classes

- › 5.1 Understanding the Basics of Blockchain and Quantum Computing
- › 5.2 Exploring Blockchain's Role in Enhancing Cybersecurity
- › 5.3 Assessing Quantum Computing's Impact on Digital Security
- › 5.4 Analyzing Integrative Strategies for Blockchain and Quantum Tech
- › 5.5 Evaluating Use Cases of Blockchain and Quantum in Cyber Defense
- › 5.6 Designing Cybersecurity Strategies Using Emerging Technologies

• 1 Fundamentals of Enterprise Security Architecture — 6 classes

- › 1.1 Understanding Enterprise Security Architecture
- › 1.2 Identifying Key Components of Security Architecture
- › 1.3 Exploring the Role of Security Frameworks and Standards
- › 1.4 Analyzing Security Architecture Models
- › 1.5 Assessing Enterprise Security Risks and Threats
- › 1.6 Implementing Security Architecture in Practice

• 2 Integrating Security with Enterprise Architecture Frameworks — 6

classes

- › 2.1 Understanding Enterprise Architecture Frameworks
- › 2.2 Identifying Key Security Challenges in Architecture
- › 2.3 Mapping Security Requirements to Architectural Layers
- › 2.4 Analyzing Security Components in TOGAF Framework
- › 2.5 Integrating Security into SABSA Framework
- › 2.6 Evaluating Security Impact on Business Processes

• 3 Developing and Implementing Security Policies and Standards — 6

classes

- › 3.1 Understanding Security Policies and Their Importance
- › 3.2 Analyzing Key Components of Security Standards
- › 3.3 Assessing Organizational Needs for Security Policies
- › 3.4 Designing Comprehensive Security Policies
- › 3.5 Implementing Security Standards Across the Enterprise
- › 3.6 Evaluating Policy Compliance and Effectiveness

• 4 Advanced Threat Modeling and Risk Assessment Techniques — 6

classes

- › 4.1 Understanding Advanced Threat Modeling Concepts
- › 4.2 Identifying Potential Threats in Enterprise Systems
- › 4.3 Analyzing Attack Vectors and Vulnerabilities
- › 4.4 Applying Risk Assessment Methodologies
- › 4.5 Integrating Threat Intelligence into Risk Models
- › 4.6 Evaluating and Prioritizing Security Risks

• 5 Designing Resilient Security Architectures for Emerging Technologies — 6 classes

- › 5.1 Understanding Emerging Technologies and Their Security Challenges
- › 5.2 Analyzing Threat Landscapes in Modern Tech Environments
- › 5.3 Evaluating Security Architecture Principles for Resilience
- › 5.4 Designing Adaptive Security Controls for Emerging Technologies
- › 5.5 Integrating Secure Design Patterns into Innovative Solutions
- › 5.6 Assessing the Effectiveness of Resilient Security Architectures

• 1 Understanding Cybersecurity Leadership Fundamentals — 6

classes

- › 1.1 Defining Cybersecurity Leadership Essentials
- › 1.2 Exploring the Role of a CISO in an Organization
- › 1.3 Identifying Key Leadership Traits for Cybersecurity
- › 1.4 Understanding the Cybersecurity Leadership Landscape
- › 1.5 Analyzing Leadership Challenges in Cybersecurity
- › 1.6 Applying Leadership Strategies to Cybersecurity Issues

• 2 Developing Strategic Cybersecurity Vision and Policies — 6 classes

- › 2.1 Understanding the Role of Vision in Cybersecurity Strategy
- › 2.2 Analyzing the Components of a Strategic Cybersecurity Vision
- › 2.3 Crafting a Vision Statement Aligned with Organizational Goals
- › 2.4 Developing Robust Cybersecurity Policies: Key Considerations
- › 2.5 Integrating Legal and Regulatory Requirements into Policies
- › 2.6 Evaluating and Revising Cybersecurity Vision and Policies

• 3 Building and Leading High-Performance Cybersecurity Teams —

6 classes

- › 3.1 Understanding Team Dynamics in Cybersecurity
- › 3.2 Identifying Key Roles and Skills in Cybersecurity Teams
- › 3.3 Developing Effective Communication Strategies
- › 3.4 Fostering a Culture of Continuous Learning
- › 3.5 Implementing Collaborative Problem-Solving Techniques
- › 3.6 Evaluating and Enhancing Team Performance

• 4 Navigating Risk Management and Incident Response — 6 classes

- › 4.1 Understanding the Fundamentals of Risk Management
- › 4.2 Identifying and Assessing Cybersecurity Risks
- › 4.3 Developing Strategies for Risk Mitigation
- › 4.4 Implementing an Effective Incident Response Plan
- › 4.5 Analyzing Incident Responses and Lessons Learned
- › 4.6 Enhancing Leadership Skills in Crisis Management

• 5 Influencing Organizational Culture and Executive Communication

— 6 classes

- › 5.1 Understanding Organizational Culture in Cybersecurity
- › 5.2 Analyzing the Role of Leadership in Shaping Culture
- › 5.3 Strategies for Communicating Cybersecurity Vision to Executives
- › 5.4 Building Trust and Influence with Executive Teams
- › 5.5 Facilitating Executive Buy-In for Security Initiatives
- › 5.6 Evaluating and Adjusting Organizational Culture and Communication

• 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
- › 3.6 Assessing and Improving Standard Adherence

• 4 Legal Implications of Information Security Breaches — 6 classes

- › 4.1 Understanding Information Security Breaches and Legal Consequences
- › 4.2 Exploring Data Protection Regulations and Compliance Requirements
- › 4.3 Analyzing Case Studies of Security Breach Consequences
- › 4.4 Identifying Cybersecurity Offenses and Legal Repercussions
- › 4.5 Evaluating the Role of Standards in Legal Compliance
- › 4.6 Implementing Best Practices to Mitigate Legal Risks

• 5 Developing a Compliance and Audit Strategy — 6 classes

- › 5.1 Understanding Compliance Frameworks
- › 5.2 Identifying Key Legislation and Standards
- › 5.3 Mapping Business Processes to Compliance Requirements
- › 5.4 Designing a Risk-Based Audit Plan
- › 5.5 Implementing Effective Compliance Monitoring Techniques
- › 5.6 Evaluating Compliance and Audit Strategies for Continuous Improvement

• 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