

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

Master Certificate in Cyber Security Governance & Risk

Leadership 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-L • IT Centres

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

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

CURRICULUM

1

Advanced Cyber Security Governance

5 chapters · 30 classes85 marks

• 1 Foundations of Cyber Security Governance — 6 classes

› 1.1 Exploring Cyber Security Governance: Concepts and Importance

› 1.2 Analyzing Governance Frameworks: Standards and Best Practices

› 1.3 Identifying Key Stakeholders in Cyber Security Governance

› 1.4 Assessing Cyber Risks: Tools and Methodologies

› 1.5 Developing a Cyber Security Governance Strategy

› 1.6 Applying Governance Principles to Real-world Scenarios

• 2 Developing Cyber Security Policies and Standards — 6 classes

› 2.1 Understanding the Role of Cyber Security Policies

› 2.2 Identifying Key Components of Effective Cyber Policies

› 2.3 Analyzing Current Cyber Security Standards

› 2.4 Aligning Cyber Standards with Organizational Objectives

› 2.5 Crafting Comprehensive Cyber Security Procedures

› 2.6 Evaluating and Updating Cyber Policies Regularly

• 3 Risk Management Strategies in Cyber Security — 6 classes

› 3.1 Understanding Key Concepts in Cyber Risk Management

› 3.2 Identifying and Analyzing Cyber Threats

› 3.3 Assessing Vulnerabilities within an Organization

› 3.4 Developing Effective Risk Mitigation Strategies

› 3.5 Implementing Cyber Risk Control Measures

› 3.6 Evaluating Risk Management Outcomes and Adjustments

• 4 Integrating Cyber Security into Corporate Governance — 6 classes

› 4.1 Exploring the Role of Cyber Security in Corporate Governance

› 4.2 Identifying Key Cyber Security Policies for Governance Frameworks

› 4.3 Understanding the Impact of Cyber Risks on Business Strategy

› 4.4 Analyzing Board Responsibilities in Cyber Security Oversight

› 4.5 Developing Effective Cyber Security Governance Models

› 4.6 Integrating Cyber Security into Corporate Governance Practices

• 5 Leadership in Cyber Security Governance — 6 classes

› 5.1 Understanding the Role of Leadership in Cyber Security

› 5.2 Analyzing Key Leadership Qualities for Effective Cyber Governance

› 5.3 Evaluating Risk Management Strategies Led by Cyber Leaders

› 5.4 Implementing Leadership-Informed Security Policies and Protocols

› 5.5 Fostering a Security-Aware Culture Through Effective Leadership

› 5.6 Assessing the Impact of Leadership on Cyber Security Outcomes

• 1 Understanding Regulatory Frameworks in Cyber Security — 6 classes

- › 1.1 Introduction to Regulatory Frameworks in Cyber Security
- › 1.2 Identifying Key Cyber Security Regulations and Standards
- › 1.3 Analyzing the Impact of Compliance on Cyber Security Strategy
- › 1.4 Comparing Global Cyber Security Regulatory Requirements
- › 1.5 Understanding the Role of Governance in Policy Formulation
- › 1.6 Applying Regulatory Frameworks in Cyber Risk Management

• 2 Principles of Policy Formulation in Cyber Security — 6 classes

- › 2.1 Understanding the Fundamentals of Cyber Security Policies
- › 2.2 Identifying Key Components of Effective Policy Formulation
- › 2.3 Analyzing Regulatory Compliance Requirements in Cyber Security
- › 2.4 Designing Custom Policies for Diverse Organizational Needs
- › 2.5 Implementing Cyber Security Policies within Governance Frameworks
- › 2.6 Evaluating and Revising Policies for Continuous Improvement

• 3 Developing Risk Management Strategies — 6 classes

- › 3.1 Understanding Risk Management Fundamentals
- › 3.2 Identifying and Evaluating Potential Risks
- › 3.3 Developing Risk Mitigation Strategies
- › 3.4 Integrating Compliance Requirements into Risk Management
- › 3.5 Designing Risk Policies and Procedures
- › 3.6 Applying Risk Management Strategies in Real-World Scenarios

• 4 Implementing Compliance and Governance Controls — 6 classes

- › 4.1 Understanding Compliance Regulations in Cyber Security
- › 4.2 Identifying Key Governance Frameworks
- › 4.3 Establishing Policy Formulation Techniques
- › 4.4 Designing Effective Compliance Controls
- › 4.5 Implementing Governance Strategies in Practice
- › 4.6 Evaluating and Updating Compliance Measures

• 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 The Role of Leadership in Cyber Security Governance — 6 classes

- › 1.1 Understanding Leadership Responsibilities in Cyber Security
- › 1.2 Recognizing the Impact of Leadership on Cyber Security Culture
- › 1.3 Identifying Key Components of Cyber Security Governance
- › 1.4 Analyzing Decision-Making Processes in Cyber Security Management
- › 1.5 Developing Leadership Skills for Effective Cyber Risk Management
- › 1.6 Applying Leadership Strategies to Enhance Cyber Security Posture

• 2 Strategic Risk Management for Cyber Security Leaders — 6 classes

- › 2.1 Understanding the Fundamentals of Cyber Security Risk
- › 2.2 Identifying and Assessing Threats and Vulnerabilities
- › 2.3 Analyzing Risk Scenarios in Cyber Security
- › 2.4 Prioritizing Risks Based on Business Impact
- › 2.5 Implementing Risk Mitigation Strategies
- › 2.6 Evaluating the Effectiveness of Risk Management Practices

• 3 Establishing a Cyber Security Culture and Awareness — 6 classes

- › 3.1 Understanding the Importance of Cyber Security Culture
- › 3.2 Identifying Key Elements of Successful Security Awareness
- › 3.3 Integrating Cyber Security into Organizational Values
- › 3.4 Developing Effective Communication Strategies for Awareness
- › 3.5 Engaging Employees to Foster a Security-First Mindset
- › 3.6 Evaluating and Enhancing Cyber Security Culture Continuously

• 4 Legal, Ethical, and Compliance Considerations in Cyber Security — 6 classes

- › 4.1 Understanding Cyber Security Legal Frameworks
- › 4.2 Exploring Ethical Principles in Cyber Security
- › 4.3 Analyzing Data Protection and Privacy Regulations
- › 4.4 Examining Compliance Standards and Best Practices
- › 4.5 Recognizing the Implications of Non-Compliance
- › 4.6 Applying Legal and Ethical Knowledge in Leadership Decisions

• 5 Crisis Management and Incident Response Leadership — 6 classes

- › 5.1 Understanding Crisis Management in Cyber Security
- › 5.2 Identifying Cyber Incidents and Threats
- › 5.3 Developing an Effective Incident Response Plan
- › 5.4 Coordinating a Cyber Incident Response Team
- › 5.5 Implementing Communication Strategies During a Crisis
- › 5.6 Evaluating and Improving Incident Response Actions

• 1 Understanding Emerging Technologies in Cyber Security — 6 classes

- › 1.1 Exploring the Role of Emerging Technologies in Cyber Security
- › 1.2 Identifying Key Emerging Technologies and Their Applications
- › 1.3 Analyzing the Impact of Artificial Intelligence in Security Protocols
- › 1.4 Evaluating Blockchain for Enhanced Security Measures
- › 1.5 Investigating the Use of Quantum Computing in Risk Mitigation
- › 1.6 Applying Emerging Technologies in Cyber Security Strategies

• 2 The Role of Artificial Intelligence and Machine Learning — 6 classes

- › 2.1 Understanding AI and Machine Learning in Cyber Security
- › 2.2 Identifying Key AI Technologies Affecting Cyber Security
- › 2.3 Exploring Machine Learning Applications in Risk Management
- › 2.4 Analyzing AI-driven Threat Detection and Response
- › 2.5 Evaluating AI's Role in Enhancing Cyber Defense Strategies
- › 2.6 Integrating AI and Machine Learning in Cyber Security Governance

• 3 Blockchain Applications in Security Protocols — 6 classes

- › 3.1 Understanding Blockchain Technology and Its Role in Security
- › 3.2 Exploring Cryptographic Functions in Blockchain
- › 3.3 Analyzing Blockchain-based Security Protocols
- › 3.4 Evaluating the Impact of Blockchain on Risk Management
- › 3.5 Assessing Real-world Applications of Blockchain in Cyber Security
- › 3.6 Designing Secure Systems Using Blockchain Principles

• 4 Implications of Quantum Computing for Cyber Security — 6 classes

- › 4.1 Understanding the Basics of Quantum Computing
- › 4.2 Exploring the Potential of Quantum Algorithms in Cyber Security
- › 4.3 Examining the Threats of Quantum Computing to Current Encryption Methods
- › 4.4 Analyzing Quantum-Resistant Cryptography Solutions
- › 4.5 Evaluating the Impact of Quantum Computing on Cyber Security Infrastructure
- › 4.6 Planning for Quantum Readiness in Cyber Security Strategy

• 5 Formulating Governance Strategies for Emerging Technologies — 6 classes

- › 5.1 Understanding Emerging Technologies and Their Risks
- › 5.2 Identifying Key Challenges in Governing Emerging Technologies
- › 5.3 Analyzing Regulatory Frameworks for Emerging Tech
- › 5.4 Developing Strategic Goals for Technology Governance
- › 5.5 Designing Organizational Structures for Tech Oversight
- › 5.6 Applying Governance Models to Emerging Technology Risks

• 1 Understanding Risk in Cyber Environments — 6 classes

- › 1.1 Identifying Cyber Threats and Vulnerabilities
- › 1.2 Analyzing Potential Impacts of Cyber Risks
- › 1.3 Evaluating Risk Likelihood in Digital Environments
- › 1.4 Developing Strategies to Mitigate Cyber Risks
- › 1.5 Implementing Risk Controls and Measures
- › 1.6 Monitoring and Reviewing Risk Management Effectiveness

• 2 Risk Assessment and Measurement Techniques — 6 classes

- › 2.1 Understanding the Fundamentals of Risk Assessment
- › 2.2 Identifying and Categorizing Potential Risks
- › 2.3 Exploring Qualitative Risk Measurement Techniques
- › 2.4 Implementing Quantitative Risk Analysis Tools
- › 2.5 Evaluating Risks: Likelihood and Impact Assessment
- › 2.6 Applying Risk Measurement in Real-World Scenarios

• 3 Developing Risk Management Strategies — 6 classes

- › 3.1 Understanding the Fundamentals of Risk Management
- › 3.2 Identifying and Categorizing Organizational Risks
- › 3.3 Evaluating Risk Impact and Likelihood
- › 3.4 Developing Effective Risk Response Strategies
- › 3.5 Implementing Risk Mitigation Controls
- › 3.6 Monitoring and Reviewing Risk Management Processes

• 4 Control Implementation and Effectiveness — 6 classes

- › 4.1 Understanding Control Objectives in Cyber Security
- › 4.2 Identifying and Selecting Appropriate Controls
- › 4.3 Implementing Controls: Best Practices
- › 4.4 Evaluating Control Effectiveness
- › 4.5 Testing and Reviewing Control Performance
- › 4.6 Enhancing Security Through Continuous Control Improvement

• 5 Governance and Continuous Risk Monitoring — 6 classes

- › 5.1 Understanding Governance in Cyber Security
- › 5.2 Exploring the Principles of Risk Management
- › 5.3 Identifying Key Risk Indicators (KRIs)
- › 5.4 Implementing Continuous Risk Monitoring
- › 5.5 Analyzing Risk Monitoring Data for Governance
- › 5.6 Applying Governance Strategies to Mitigate Risks

• 1 Foundations of Strategic Information Assurance — 6 classes

- › 1.1 Understanding the Role of Information Assurance in Cyber Security
- › 1.2 Identifying Key Elements of Information Assurance Frameworks
- › 1.3 Exploring Strategic Risk Management Principles
- › 1.4 Analyzing Threats and Vulnerabilities in Information Systems
- › 1.5 Implementing Information Assurance Policies and Practices
- › 1.6 Evaluating Metrics for Information Assurance Performance

• 2 Regulatory Frameworks and Compliance — 6 classes

- › 2.1 Understanding Cybersecurity Regulations and Their Importance
- › 2.2 Identifying Key International and National Regulatory Frameworks
- › 2.3 Analyzing the Impact of Compliance on Business Operations
- › 2.4 Assessing Compliance Requirements for Information Assurance
- › 2.5 Creating Strategies for Meeting Regulatory Obligations
- › 2.6 Implementing Compliance Practices in Cybersecurity Governance

• 3 Risk Assessment and Management Processes — 6 classes

- › 3.1 Understanding Risk in Cyber Security Contexts
- › 3.2 Identifying and Categorizing Cyber Risks
- › 3.3 Analyzing Risk Impact and Probability
- › 3.4 Developing Risk Mitigation Strategies
- › 3.5 Implementing Risk Management Frameworks
- › 3.6 Monitoring and Evaluating Risk Management Effectiveness

• 4 Developing Information Assurance Policies and Strategies — 6 classes

- › 4.1 Understanding the Purpose of Information Assurance Policies
- › 4.2 Identifying Key Components of Information Assurance Strategies
- › 4.3 Analyzing Risks and Threats in Information Security
- › 4.4 Crafting Comprehensive Information Assurance Policies
- › 4.5 Implementing Strategic Information Assurance Measures
- › 4.6 Evaluating and Improving Information Assurance Strategies

• 5 Leadership and Decision-Making in Cybersecurity Governance — 6 classes

- › 5.1 Understanding Leadership Roles in Cybersecurity
- › 5.2 Analyzing Decision-Making Processes in Cyber Risk Management
- › 5.3 Evaluating Leadership Strategies for Information Assurance
- › 5.4 Implementing Effective Governance Models in Cybersecurity
- › 5.5 Identifying and Mitigating Leadership Challenges in Cyber Governance
- › 5.6 Applying Decision-Making Frameworks in Cybersecurity Governance