

# LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

## ISO 18788 — Management Systems for Private Security Operations

*ISO Certification Programme*



---

### LAPT — London Academy of Professional Training

**Address** 85 Great Portland Street, W1W 7LT, London, United Kingdom

**Email** [info@lapt.org](mailto:info@lapt.org)

**Telephone** +44 7513 283044

**Web** [lapt.org](http://lapt.org)

**Reference** SSR-PCR-18788 • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

|               |                                                |
|---------------|------------------------------------------------|
| REFERENCE     | SSR-PCR-18788                                  |
| AWARD         | Certificate                                    |
| ASSESSMENT    | 430 marks — 258 to pass (60%)                  |
| PREREQUISITES | None                                           |
| VALIDITY      | Lifetime                                       |
| AWARDING BODY | LAPT — London Academy of Professional Training |

CURRICULUM

1

Designing Security Policies and Procedures

5 chapters · 30 classes 45 marks

• 1 Foundations of Security Policy Development — 6 classes

› 1.1 Define Key Concepts in Security Policy Development

› 1.2 Analyze the Importance of Compliance and Standards

› 1.3 Assess Risk Management Principles for Security Policies

› 1.4 Identify Stakeholders and Their Roles in Policy Creation

› 1.5 Formulate Clear Objectives for Security Policies

› 1.6 Develop a Framework for Implementing Security Procedures

• 2 Risk Assessment and Management in Security Policies — 6 classes

› 2.1 Identify Risk Factors for Security Operations

› 2.2 Analyze Vulnerabilities in Security Practices

› 2.3 Evaluate Potential Threats and Impacts

› 2.4 Develop Risk Mitigation Strategies for Security Policies

› 2.5 Implement Risk Management Techniques in Procedures

› 2.6 Review and Adjust Security Plans Based on Risk Assessment

• 3 Legal and Regulatory Considerations in Security Policies — 6 classes

› 3.1 Identify Key Legal Frameworks Impacting Security Policies

› 3.2 Analyze Regulatory Requirements for Security Operations

› 3.3 Assess the Role of Compliance in Security Policy Development

› 3.4 Evaluate Risk Management Principles in Legal Contexts

› 3.5 Integrate Human Rights Considerations into Security Procedures

› 3.6 Develop a Compliance Checklist for Security Policy Implementation

• 4 Integrating Best Practices into Security Procedures — 6 classes

› 4.1 Assess Current Security Protocols Using Best Practices

› 4.2 Identify Key Stakeholders for Security Policy Development

› 4.3 Develop Security Procedures Aligned with ISO 18788 Standards

› 4.4 Create a Framework for Effective Security Policy Communication

› 4.5 Implement Strategies for Continuous Improvement in Security Practices

› 4.6 Evaluate the Effectiveness of Security Procedures and Policies

• 5 Evaluating and Updating Security Policies and Procedures — 6 classes

› 5.1 Assess Current Security Policies for Effectiveness

› 5.2 Identify Gaps and Areas for Improvement

› 5.3 Create a Framework for Policy Evaluation

› 5.4 Implement Feedback Mechanisms for Continuous Improvement

› 5.5 Develop an Action Plan for Updating Procedures

› 5.6 Communicate Changes and Revisions to Stakeholders

**• 1 Understanding ISO 18788: Core Principles and Framework** — 6 classes

- › 1.1 Define ISO 18788 and Its Importance in Security Operations
- › 1.2 Identify Core Principles of ISO 18788 Standards
- › 1.3 Explore the Framework of ISO 18788 Management Systems
- › 1.4 Analyze the Role of Leadership in ISO 18788 Implementation
- › 1.5 Assess the Benefits of Adhering to ISO 18788 Standards
- › 1.6 Apply ISO 18788 Principles to Real-World Security Scenarios

**• 2 Key Components of ISO 18788: Risk Management and Control Measures** — 6 classes

- › 2.1 Identify Key Components of ISO 18788
- › 2.2 Analyze the Importance of Risk Management in Security Operations
- › 2.3 Assess Common Risk Factors in Private Security Settings
- › 2.4 Develop Control Measures for Identified Risks
- › 2.5 Implement Risk Management Strategies in Real-World Scenarios
- › 2.6 Evaluate the Effectiveness of Control Measures and Adjust Accordingly

**• 3 Implementing ISO 18788: Steps and Best Practices** — 6 classes

- › 3.1 Identify Key Principles of ISO 18788 Standards
- › 3.2 Assess Organizational Readiness for ISO 18788 Implementation
- › 3.3 Develop an Effective ISO 18788 Implementation Plan
- › 3.4 Establish Documentation and Record-Keeping Systems
- › 3.5 Train Personnel on ISO 18788 Compliance Requirements
- › 3.6 Evaluate and Improve ISO 18788 Implementation Outcomes

**• 4 Monitoring and Measuring Compliance with ISO 18788** — 6 classes

- › 4.1 Define Key Terms in ISO 18788 Compliance Monitoring
- › 4.2 Identify Components of a Compliance Monitoring Framework
- › 4.3 Explore Methods for Measuring Compliance with ISO 18788
- › 4.4 Analyze Data Collection Techniques for ISO 18788 Compliance
- › 4.5 Evaluate Compliance Monitoring Tools and Technologies
- › 4.6 Develop a Compliance Monitoring Plan for Security Operations

**• 5 Continuous Improvement and Future Trends in ISO 18788 Standards** — 6 classes

- › 5.1 Analyze the Role of Continuous Improvement in ISO 18788
- › 5.2 Identify Key Components of the Continuous Improvement Process
- › 5.3 Explore Future Trends Impacting ISO 18788 Standards
- › 5.4 Evaluate Case Studies of Successful Implementation
- › 5.5 Develop a Personal Action Plan for Implementing Improvements
- › 5.6 Create Metrics to Measure Improvements in ISO 18788 Practices

**• 1 Foundations of Leadership in Private Security** — 6 classes

- › 1.1 Define Leadership Principles in Private Security
- › 1.2 Identify Key Leadership Styles Relevant to Security Teams
- › 1.3 Analyze the Role of Communication in Effective Leadership
- › 1.4 Assess Team Dynamics and Their Impact on Leadership
- › 1.5 Develop Strategies for Conflict Resolution in Security Teams
- › 1.6 Implement Leadership Best Practices for Team Development

**• 2 Effective Communication Strategies for Security Teams** — 6 classes

- › 2.1 Identify Key Communication Barriers in Security Teams
- › 2.2 Develop Active Listening Skills for Effective Team Interaction
- › 2.3 Formulate Clear Message Delivery Techniques for Security Operations
- › 2.4 Utilize Non-Verbal Communication to Enhance Team Cohesion
- › 2.5 Implement Conflict Resolution Strategies within Security Teams
- › 2.6 Evaluate Communication Effectiveness and Gather Team Feedback

**• 3 Building and Sustaining High-Performing Teams** — 6 classes

- › 3.1 Define the Characteristics of High-Performing Teams
- › 3.2 Identify Leadership Styles That Foster Team Success
- › 3.3 Utilize Effective Communication Strategies Within Teams
- › 3.4 Implement Techniques for Building Trust Among Team Members
- › 3.5 Develop Conflict Resolution Skills for Team Dynamics
- › 3.6 Assess and Sustain Team Performance Through Continuous Feedback

**• 4 Conflict Resolution and Decision-Making in Security Contexts** — 6 classes

- › 4.1 Identify Common Sources of Conflict in Security Operations
- › 4.2 Analyze the Impact of Conflict on Team Dynamics
- › 4.3 Explore Conflict Resolution Models Applicable to Security Teams
- › 4.4 Develop Effective Communication Strategies for Conflict Resolution
- › 4.5 Practice Decision-Making Techniques in High-Stress Scenarios
- › 4.6 Implement a Conflict Resolution Plan for Security Operations

**• 5 Leading Change and Innovation in Security Operations** — 6 classes

- › 5.1 Identify Key Drivers of Change in Security Operations
- › 5.2 Assess the Impact of Innovation on Team Dynamics
- › 5.3 Develop a Vision for Change in Security Management
- › 5.4 Facilitate Effective Communication During Transition
- › 5.5 Implement Strategies for Encouraging Team Adaptability
- › 5.6 Evaluate the Success of Change Initiatives in Security Contexts

### • 1 Understanding Operational Security Management Frameworks — 6 classes

- › 1.1 Define Operational Security Management in the Context of ISO 18788
- › 1.2 Identify Key Components of Operational Security Management Frameworks
- › 1.3 Analyze the Relationship Between Risk Assessment and Operational Security
- › 1.4 Explore Best Practices for Implementing Security Management Systems
- › 1.5 Evaluate Compliance Standards Related to ISO 18788
- › 1.6 Develop a Case Study on Operational Security Management Implementation

### • 2 Risk Assessment and Analysis Techniques — 6 classes

- › 2.1 Identify Key Risks in Operational Security
- › 2.2 Analyze Vulnerabilities in Security Protocols
- › 2.3 Evaluate Threat Levels Using Qualitative Methods
- › 2.4 Conduct Quantitative Risk Assessment Techniques
- › 2.5 Prioritize Risks for Effective Mitigation Strategies
- › 2.6 Implement a Risk Management Action Plan

### • 3 Developing Security Policies and Procedures — 6 classes

- › 3.1 Assess Security Needs for Effective Policy Development
- › 3.2 Identify Key Stakeholders in Security Operations
- › 3.3 Draft Comprehensive Security Policies and Procedures
- › 3.4 Integrate Compliance Standards into Security Framework
- › 3.5 Communicate Security Policies to Stakeholders
- › 3.6 Evaluate and Revise Security Policies for Continuous Improvement

### • 4 Implementing Security Operations and Controls — 6 classes

- › 4.1 Assess Security Needs Within an Operational Context
- › 4.2 Design Effective Security Controls Based on Risk Assessment
- › 4.3 Implement Training Programs for Security Personnel
- › 4.4 Monitor and Evaluate Security Procedures for Compliance
- › 4.5 Develop Incident Response Plans for Security Breaches
- › 4.6 Review and Update Security Policies Based on Operational Feedback

### • 5 Monitoring, Review, and Continuous Improvement in Security Operations — 6 classes

- › 5.1 Assessing Current Monitoring Practices in Security Operations
- › 5.2 Identifying Key Performance Indicators for Security Effectiveness
- › 5.3 Conducting Effective Reviews of Security Policies and Procedures
- › 5.4 Utilizing Feedback Mechanisms for Operational Improvement
- › 5.5 Implementing Continuous Improvement Strategies in Security Operations
- › 5.6 Documenting and Communicating Changes in Security Practices

### • 1 Understanding Performance Evaluation Frameworks in Security Operations — 6 classes

- › 1.1 Define Key Performance Indicators for Effective Security Operations
- › 1.2 Analyze Performance Evaluation Frameworks Used in Security Management
- › 1.3 Identify Stakeholder Roles in Performance Evaluation Processes
- › 1.4 Compare Quantitative and Qualitative Assessment Methods in Security
- › 1.5 Implement Continuous Improvement Strategies for Security Operations
- › 1.6 Develop a Performance Review Plan for Security Personnel

### • 2 Key Performance Indicators (KPIs) for Security Management — 6 classes

- › 2.1 Define Key Performance Indicators for Security Management
- › 2.2 Identify Essential Metrics for Security Operations
- › 2.3 Analyze Current Performance Using KPIs
- › 2.4 Integrate KPIs into Security Management Frameworks
- › 2.5 Develop Improvement Strategies Based on KPI Analysis
- › 2.6 Communicate KPI Results and Action Plans to Stakeholders

### • 3 Data Collection and Analysis Techniques in Performance Evaluation — 6 classes

- › 3.1 Identify Key Performance Indicators for Security Operations
- › 3.2 Explore Quantitative Data Collection Methods
- › 3.3 Analyze Qualitative Data to Improve Performance
- › 3.4 Utilize Software Tools for Effective Data Management
- › 3.5 Interpret Data Trends to Enhance Decision Making
- › 3.6 Develop Action Plans Based on Performance Analysis

### • 4 Continuous Improvement Strategies in Security Operations — 6 classes

- › 4.1 Identify Key Performance Indicators for Security Operations
- › 4.2 Analyze Current Performance Data to Highlight Improvement Areas
- › 4.3 Implement Effective Feedback Mechanisms within Security Teams
- › 4.4 Develop Action Plans for Targeted Performance Improvements
- › 4.5 Utilize Technology to Enhance Continuous Improvement Processes
- › 4.6 Evaluate the Impact of Improvement Strategies on Security Outcomes

### • 5 Integrating Lessons Learned into Security Management Practices — 6 classes

- › 5.1 Identify Key Lessons from Security Incidents
- › 5.2 Analyze and Categorize Lessons Learned
- › 5.3 Develop Actionable Improvement Strategies
- › 5.4 Integrate Lessons Learned into Existing Protocols
- › 5.5 Create a Continuous Improvement Feedback Loop
- › 5.6 Evaluate the Impact of Integrated Lessons on Security Operations

**• 1 Understanding Risk Management Principles and Terminology — 6**

classes

- › 1.1 Define Key Risk Management Terms and Concepts
- › 1.2 Explore the Importance of Risk Management in Security Operations
- › 1.3 Identify Types of Risks in Private Security Environments
- › 1.4 Examine the Risk Management Framework Process
- › 1.5 Analyze Real-World Case Studies of Risk Management Failures
- › 1.6 Develop a Basic Risk Assessment Tool for Security Scenarios

**• 2 Identifying and Assessing Security Risks — 6 classes**

- › 2.1 Define Key Security Risk Concepts
- › 2.2 Identify Common Security Risks in Operations
- › 2.3 Analyze the Impact of Identified Risks
- › 2.4 Explore Risk Assessment Techniques
- › 2.5 Develop a Risk Assessment Matrix
- › 2.6 Apply Risk Assessment Findings to Security Planning

**• 3 Designing and Implementing Risk Mitigation Strategies — 6 classes**

- › 3.1 Identify Key Risks in Private Security Operations
- › 3.2 Analyze Impact and Likelihood of Identified Risks
- › 3.3 Develop Risk Mitigation Strategies for High-Priority Risks
- › 3.4 Integrate Risk Mitigation into Security Management Framework
- › 3.5 Implement Risk Mitigation Strategies: Best Practices
- › 3.6 Monitor and Review the Effectiveness of Risk Mitigation Strategies

**• 4 Monitoring and Reviewing Risk Management Processes — 6**

classes

- › 4.1 Identify Key Performance Indicators for Risk Management Monitoring
- › 4.2 Evaluate Current Risk Management Processes and Gaps
- › 4.3 Develop Strategies for Effective Risk Mitigation
- › 4.4 Implement Auditing Techniques for Risk Management Assessment
- › 4.5 Review and Revise Risk Management Policies Regularly
- › 4.6 Communicate Risk Management Findings and Improvements Effectively

**• 5 Integrating ISO 18788 Standards into Risk Management Practices**

— 6 classes

- › 5.1 Define ISO 18788 Standards and Their Relevance to Risk Management
- › 5.2 Identify Key Components of a Risk Management Framework in ISO 18788
- › 5.3 Assess Existing Risk Management Practices Against ISO 18788 Standards
- › 5.4 Develop an Implementation Plan for ISO 18788 in Security Operations
- › 5.5 Evaluate Risks and Opportunities in the Context of ISO 18788 Compliance
- › 5.6 Create a Continuous Improvement Strategy Leveraging ISO 18788 Guidelines