

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 31000PCR — Risk Management in 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

Telephone +44 7513 283044

Web lapt.org

Reference SSR-PCR-31000PCR • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	SSR-PCR-31000PCR
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1

Crisis Management and Response

5 chapters · 30 classes85 marks

• 1 Understanding Crisis Management Frameworks — 6 classes

› 1.1 Define Crisis Management and Its Importance in Security Operations

› 1.2 Identify Key Components of Crisis Management Frameworks

› 1.3 Analyze Different Types of Crises Affecting Security Operations

› 1.4 Explore the Roles and Responsibilities in Crisis Management Teams

› 1.5 Develop a Basic Crisis Response Plan Using Framework Concepts

› 1.6 Evaluate Real-World Case Studies to Apply Crisis Management Frameworks

• 2 Risk Assessment in Crisis Scenarios — 6 classes

› 2.1 Identify Key Risks in Crisis Scenarios

› 2.2 Assess Impact and Likelihood of Risks

› 2.3 Develop Risk Scoring and Prioritization Techniques

› 2.4 Create a Risk Mitigation Strategy

› 2.5 Implement Risk Monitoring Tools and Techniques

› 2.6 Review and Revise Risk Assessments in Practice

• 3 Crisis Communication Strategies — 6 classes

› 3.1 Analyze Key Components of Effective Crisis Communication

› 3.2 Identify Stakeholders and Tailor Messages for Each Audience

› 3.3 Develop a Crisis Communication Plan Framework

› 3.4 Implement Real-time Communication Strategies During a Crisis

› 3.5 Evaluate the Impact of Crisis Communication Post-Incident

› 3.6 Create Role-playing Scenarios to Practice Crisis Messaging

• 4 Developing Crisis Response Plans — 6 classes

› 4.1 Identify Key Components of a Crisis Response Plan

› 4.2 Assess Potential Risks and Impact Scenarios

› 4.3 Develop Stakeholder Communication Strategies

› 4.4 Establish Roles and Responsibilities in Crisis Situations

› 4.5 Design Effective Training and Simulation Exercises

› 4.6 Evaluate and Update Crisis Response Plans Regularly

• 5 Evaluating and Learning from Crisis Responses — 6 classes

› 5.1 Analyze Past Crisis Responses for Effectiveness

› 5.2 Identify Key Metrics for Evaluating Crisis Management

› 5.3 Develop a Framework for Post-Crisis Review

› 5.4 Conduct a SWOT Analysis of Crisis Responses

› 5.5 Create Action Plans for Improvement Based on Findings

› 5.6 Present Findings and Recommendations to Stakeholders

• 1 Foundations of Leadership in Security Operations — 6 classes

- › 1.1 Define Key Leadership Concepts in Security Operations
- › 1.2 Identify Core Responsibilities of Security Leaders
- › 1.3 Analyze Leadership Styles Effectively Used in Security
- › 1.4 Develop Communication Strategies for Security Leadership
- › 1.5 Assess the Role of Emotional Intelligence in Leadership
- › 1.6 Apply Leadership Principles to Real-World Security Scenarios

• 2 Developing Strategic Risk Management Skills — 6 classes

- › 2.1 Assessing Organizational Risks Using SWOT Analysis
- › 2.2 Identifying Key Stakeholders in Risk Management
- › 2.3 Formulating Strategies to Mitigate Risks
- › 2.4 Developing a Risk Management Action Plan
- › 2.5 Communicating Risk Management Plans Effectively
- › 2.6 Evaluating the Effectiveness of Risk Management Strategies

• 3 Building and Leading Effective Security Teams — 6 classes

- › 3.1 Identify Key Roles and Responsibilities in Security Teams
- › 3.2 Develop Communication Strategies for Effective Leadership
- › 3.3 Assess Team Dynamics and Foster Collaborative Work
- › 3.4 Implement Training Programs for Skill Development
- › 3.5 Evaluate Team Performance and Provide Constructive Feedback
- › 3.6 Cultivate a Positive Team Culture to Enhance Morale

• 4 Fostering a Culture of Security Awareness — 6 classes

- › 4.1 Define Security Awareness and Its Importance in Operations
- › 4.2 Identify Key Components of a Security Culture
- › 4.3 Assess Current Levels of Security Awareness in Your Team
- › 4.4 Develop Strategies to Enhance Security Awareness
- › 4.5 Implementing Security Awareness Training Programs
- › 4.6 Evaluate the Effectiveness of Security Awareness Initiatives

• 5 Evaluating Leadership Impact on Security Outcomes — 6 classes

- › 5.1 Define Leadership and Its Role in Security Operations
- › 5.2 Identify Key Leadership Styles Impacting Security Outcomes
- › 5.3 Assess the Relationship Between Leadership Decision-Making and Security Risks
- › 5.4 Evaluate Real-World Case Studies of Leadership Impact on Security Effectiveness
- › 5.5 Develop Metrics for Measuring Leadership Effectiveness in Security Contexts
- › 5.6 Create Action Plans to Enhance Leadership Practices for Better Security Outcomes

• 1 Understanding Legal Frameworks in Security Operations — 6 classes

- › 1.1 Identify Key Legal Frameworks in Security Operations
- › 1.2 Explore Ethical Considerations in Risk Management
- › 1.3 Analyze Relevant Legislation Impacting Security Protocols
- › 1.4 Examine Case Studies of Legal Challenges in Security
- › 1.5 Assess the Role of Compliance in Security Operations
- › 1.6 Develop a Plan for Integrating Legal Standards into Security Practices

• 2 Ethical Principles and Responsibilities in Security Management — 6 classes

- › 2.1 Identify Ethical Principles in Security Management
- › 2.2 Analyze Legal Frameworks Impacting Security Operations
- › 2.3 Evaluate Responsibilities of Security Professionals
- › 2.4 Assess the Impact of Ethical Decisions on Security Outcomes
- › 2.5 Apply Ethical Principles in Real-World Scenarios
- › 2.6 Develop Strategies for Ethical Conflict Resolution in Security

• 3 Balancing Risk Management and Legal Compliance — 6 classes

- › 3.1 Understand Legal Frameworks in Risk Management
- › 3.2 Identify Key Regulations Affecting Security Operations
- › 3.3 Analyze Case Studies on Legal Violations in Security
- › 3.4 Evaluate Ethical Dilemmas in Risk Decisions
- › 3.5 Develop a Compliance Checklist for Security Practices
- › 3.6 Implement Strategies to Balance Risk and Legal Compliance

• 4 Data Protection and Privacy Laws in Security Contexts — 6 classes

- › 4.1 Understand Data Protection Principles in Security Operations
- › 4.2 Explore Key Privacy Laws Relevant to Security Practices
- › 4.3 Identify Data Handling Responsibilities for Security Personnel
- › 4.4 Assess Risks Related to Data Breaches in Security Contexts
- › 4.5 Implement Best Practices for Data Privacy Compliance
- › 4.6 Evaluate Legal Consequences of Non-Compliance in Security

• 5 Case Studies on Legal and Ethical Dilemmas in Security — 6 classes

- › 5.1 Analyze Case Studies of Ethical Dilemmas in Security
- › 5.2 Evaluate the Legal Implications of Security Breaches
- › 5.3 Discuss the Role of Ethics in Security Decision-Making
- › 5.4 Identify Key Legal Frameworks Impacting Security Operations
- › 5.5 Explore the Consequences of Ethical Violations in Security
- › 5.6 Develop Strategies for Navigating Legal and Ethical Challenges in Security

• 1 Understanding the Importance of Monitoring in Risk Management

— 6 classes

- › 1.1 Define the Role of Monitoring in Effective Risk Management
- › 1.2 Identify Key Indicators for Risk Monitoring
- › 1.3 Assess Current Monitoring Practices in Your Organization
- › 1.4 Analyze the Impact of Inadequate Monitoring on Risk Management
- › 1.5 Develop a Practical Monitoring Plan for Risk Management
- › 1.6 Evaluate the Effectiveness of Your Risk Monitoring Strategies

• 2 Frameworks and Standards for Risk Monitoring — 6 classes

- › 2.1 Identify Key Frameworks in Risk Monitoring
- › 2.2 Analyze Standards for Effective Risk Management
- › 2.3 Evaluate Risk Monitoring Practices in Security Operations
- › 2.4 Develop Metrics for Assessing Risk Management Effectiveness
- › 2.5 Implement Continuous Improvement Strategies in Risk Monitoring
- › 2.6 Communicate Findings and Recommendations for Risk Practices

• 3 Tools and Techniques for Effective Risk Assessment Monitoring

— 6 classes

- › 3.1 Identify Key Risk Indicators for Monitoring
- › 3.2 Analyze Data Collection Methods in Risk Assessment
- › 3.3 Evaluate Qualitative vs Quantitative Risk Assessment Tools
- › 3.4 Implement a Risk Monitoring Framework in Security Operations
- › 3.5 Develop Continuous Improvement Strategies for Risk Management
- › 3.6 Conduct a Risk Assessment Review and Reporting Process

• 4 Establishing KPIs and Metrics for Risk Management — 6 classes

- › 4.1 Identify Key Performance Indicators for Risk Management
- › 4.2 Define Qualitative and Quantitative Metrics for Assessment
- › 4.3 Develop a Framework for KPI Measurement and Evaluation
- › 4.4 Align KPIs with Organizational Objectives and Risk Appetite
- › 4.5 Analyze Data Collection Methods for Effective Metrics
- › 4.6 Review and Adjust KPIs Based on Risk Management Outcomes

• 5 Continuous Improvement through Monitoring Feedback Loops — 6 classes

- › 5.1 Understand Feedback Loops in Risk Management
- › 5.2 Identify Key Metrics for Monitoring Risks
- › 5.3 Analyze Risk Management Data for Insights
- › 5.4 Implement Changes Based on Feedback Analysis
- › 5.5 Facilitate Stakeholder Engagement in Continuous Improvement
- › 5.6 Develop an Action Plan for Enhanced Risk Practices

• 1 Fundamentals of Risk Assessment in Security Operations — 6 classes

- › 1.1 Identify Key Elements of Risk Assessment in Security Operations
- › 1.2 Analyze Types of Risks Relevant to Security Operations
- › 1.3 Evaluate Existing Risk Assessment Frameworks in Practice
- › 1.4 Apply Risk Assessment Techniques to Real-World Scenarios
- › 1.5 Develop a Comprehensive Risk Management Plan for Security Operations
- › 1.6 Review and Update Risk Assessment Processes for Continuous Improvement

• 2 Identifying and Analyzing Security Risks — 6 classes

- › 2.1 Define Key Security Risk Concepts
- › 2.2 Recognize Potential Security Threats
- › 2.3 Analyze Vulnerabilities in Security Systems
- › 2.4 Evaluate the Impact of Identified Risks
- › 2.5 Prioritize Security Risks for Action
- › 2.6 Develop a Risk Assessment Report

• 3 Risk Evaluation Strategies and Methodologies — 6 classes

- › 3.1 Identify Key Risk Evaluation Criteria
- › 3.2 Analyze Qualitative Risk Assessment Techniques
- › 3.3 Examine Quantitative Risk Evaluation Methods
- › 3.4 Compare Risk Tolerance Levels Across Organizations
- › 3.5 Implement Risk Prioritization Frameworks
- › 3.6 Develop a Comprehensive Risk Evaluation Report

• 4 Developing Effective Risk Mitigation Plans — 6 classes

- › 4.1 Identify Key Risks for Mitigation Planning
- › 4.2 Analyze Risk Impact and Likelihood
- › 4.3 Develop Targeted Mitigation Strategies
- › 4.4 Prioritize Mitigation Initiatives
- › 4.5 Implement Mitigation Plans Effectively
- › 4.6 Evaluate and Adjust Mitigation Strategies

• 5 Monitoring and Reviewing Risk Management Practices — 6 classes

- › 5.1 Identify Key Performance Indicators for Risk Management
- › 5.2 Develop a Framework for Regular Risk Monitoring
- › 5.3 Analyse Data Collection Methods for Effective Reviews
- › 5.4 Implement Continuous Improvement Strategies in Risk Management
- › 5.5 Conduct a Case Study on Successful Risk Management Practices
- › 5.6 Present Findings and Recommendations for Risk Mitigation

• 1 Fundamentals of Risk Management in Security Operations — 6

classes

- › 1.1 Identify Key Concepts of Risk Management in Security Operations
- › 1.2 Analyze the Importance of Risk Assessment in Security Contexts
- › 1.3 Evaluate Common Risk Management Frameworks Used in Security
- › 1.4 Apply Risk Identification Techniques to Security Scenarios
- › 1.5 Develop Risk Mitigation Strategies for Security Operations
- › 1.6 Create a Risk Management Plan Tailored to Security Needs

• 2 ISO 31000: Understanding the Risk Management Framework — 6

classes

- › 2.1 Define Key Components of ISO 31000 Framework
- › 2.2 Analyze the Principles of Effective Risk Management
- › 2.3 Explore the Risk Management Process Stages
- › 2.4 Evaluate Risk Assessment Techniques in ISO 31000
- › 2.5 Develop a Risk Management Plan Using ISO 31000
- › 2.6 Implement Monitoring and Review Strategies for Risk Management

• 3 Risk Assessment Process in Security Operations — 6 classes

- › 3.1 Identify Critical Assets within Security Operations
- › 3.2 Evaluate Potential Risks to Security Assets
- › 3.3 Analyze Vulnerabilities in Security Processes
- › 3.4 Assess the Impact of Identified Risks
- › 3.5 Prioritize Risks for Management Attention
- › 3.6 Develop Mitigation Strategies for Key Risks

• 4 Implementing Risk Treatment Strategies — 6 classes

- › 4.1 Identify Risk Treatment Options for Security Operations
- › 4.2 Assess Effectiveness of Treatment Strategies
- › 4.3 Develop Action Plans for Risk Treatment Implementation
- › 4.4 Allocate Resources for Risk Treatment Measures
- › 4.5 Monitor and Review Risk Treatment Outcomes
- › 4.6 Communicate Risk Treatment Strategies to Stakeholders

• 5 Monitoring and Reviewing the Risk Management Framework — 6

classes

- › 5.1 Analyze Current Risk Management Practices
- › 5.2 Identify Key Performance Indicators for Risk Management
- › 5.3 Evaluate the Effectiveness of Risk Mitigation Strategies
- › 5.4 Conduct Internal Audits of the Risk Management Framework
- › 5.5 Implement Continuous Improvement Processes for Risk Management
- › 5.6 Prepare Comprehensive Risk Management Review Reports