

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 28000PCR — Security Management for Supply Chain

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-28000PCR • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	SSR-PCR-28000PCR
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 Strategies

5 chapters · 30 classes85 marks

• 1 Understanding Crisis Management Frameworks in Supply Chains

— 6 classes

› 1.1 Define Crisis Management and Its Importance in Supply Chains

› 1.2 Identify Key Components of Crisis Management Frameworks

› 1.3 Analyze Different Types of Crises Affecting Supply Chains

› 1.4 Explore Risk Assessment Techniques for Crisis Preparedness

› 1.5 Develop Crisis Response Plans for Supply Chain Scenarios

› 1.6 Evaluate Case Studies of Effective Crisis Management in Supply Chains

• 2 Identifying Risks and Vulnerabilities in Supply Chains

— 6 classes

› 2.1 Analyze Supply Chain Components for Vulnerabilities

› 2.2 Assess Risk Levels in Supply Chain Contexts

› 2.3 Identify External Threats Impacting Supply Chains

› 2.4 Evaluate Internal Operational Risks in Supply Chains

› 2.5 Prioritize Risks Based on Impact and Likelihood

› 2.6 Develop Risk Mitigation Strategies for Supply Chains

• 3 Crisis Preparedness and Response Planning

— 6 classes

› 3.1 Assess Current Crisis Vulnerabilities in Supply Chains

› 3.2 Develop Comprehensive Crisis Response Frameworks

› 3.3 Identify Key Stakeholders for Crisis Management

› 3.4 Create Scenario-Based Crisis Simulation Exercises

› 3.5 Establish Communication Protocols for Crisis Situations

› 3.6 Evaluate and Update Crisis Management Plans Regularly

• 4 Crisis Management Training and Simulation

— 6 classes

› 4.1 Identify Key Components of Crisis Management

› 4.2 Analyze Real-World Crisis Scenarios

› 4.3 Develop Effective Crisis Communication Plans

› 4.4 Implement Crisis Response Strategies

› 4.5 Conduct Crisis Management Simulations

› 4.6 Evaluate Crisis Management Outcomes and Lessons Learned

• 5 Evaluating and Learning from Crisis Management Outcomes

— 6 classes

› 5.1 Analyze Crisis Management Outcomes

› 5.2 Identify Key Performance Indicators for Success

› 5.3 Conduct a SWOT Analysis on Crisis Responses

› 5.4 Gather and Interpret Stakeholder Feedback

› 5.5 Develop Best Practices from Previous Crises

› 5.6 Create a Continuous Improvement Plan for Future Crises

• 1 Foundations of Security Management Leadership — 6 classes

- › 1.1 Define Key Concepts of Security Management Leadership
- › 1.2 Examine the Role of Leadership in Security Management
- › 1.3 Analyze Leadership Styles in the Context of Security Management
- › 1.4 Identify Core Competencies for Security Management Leaders
- › 1.5 Explore Ethical Considerations in Security Leadership
- › 1.6 Apply Leadership Strategies to Real-World Security Challenges

• 2 Building a Security-Oriented Culture — 6 classes

- › 2.1 Define Security Culture and Its Importance in Supply Chain Management
- › 2.2 Identify Key Components of a Security-Oriented Culture
- › 2.3 Assess Current Organizational Culture and Security Practices
- › 2.4 Develop Strategies for Enhancing Security Awareness Among Employees
- › 2.5 Implement Communication Techniques to Promote a Security-Focused Mindset
- › 2.6 Evaluate the Impact of Leadership on Sustaining a Security-Oriented Culture

• 3 Risk Assessment and Management in Supply Chains — 6 classes

- › 3.1 Identify Key Risks in Supply Chains
- › 3.2 Analyze the Impact of Identified Risks
- › 3.3 Evaluate Risk Management Strategies
- › 3.4 Develop a Risk Management Plan
- › 3.5 Implement Risk Mitigation Techniques
- › 3.6 Monitor and Review Risk Management Effectiveness

• 4 Developing and Implementing Security Policies — 6 classes

- › 4.1 Analyze Current Security Risks in Supply Chain Operations
- › 4.2 Define Key Components of Effective Security Policies
- › 4.3 Develop Security Policy Framework for Supply Chain Management
- › 4.4 Engage Stakeholders in the Policy Development Process
- › 4.5 Implement Security Policies Across Supply Chain Activities
- › 4.6 Evaluate and Revise Security Policies for Continuous Improvement

• 5 Leadership in Crisis Management and Response — 6 classes

- › 5.1 Analyze Crisis Scenarios Impacting Supply Chains
- › 5.2 Develop Leadership Strategies for Crisis Response
- › 5.3 Communicate Effectively During a Crisis
- › 5.4 Evaluate Risk Management Frameworks in Leadership
- › 5.5 Implement Decision-Making Processes in High-Pressure Situations
- › 5.6 Create a Post-Crisis Evaluation Plan for Continuous Improvement

• 1 Understanding Performance Evaluation in Supply Chain Security — 6 classes

- › 1.1 Define Key Performance Indicators for Supply Chain Security
- › 1.2 Identify Stakeholders Involved in Performance Evaluation
- › 1.3 Examine Quantitative vs. Qualitative Performance Metrics
- › 1.4 Analyze Data Collection Methods for Performance Evaluation
- › 1.5 Implement Continuous Improvement Strategies in Evaluations
- › 1.6 Create a Performance Evaluation Report for Stakeholder Review

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

- › 2.1 Define Key Performance Indicators (KPIs) in Security Management
- › 2.2 Analyze the Importance of KPIs for Supply Chain Security
- › 2.3 Identify the Characteristics of Effective KPIs
- › 2.4 Develop KPIs Aligned with Security Management Objectives
- › 2.5 Evaluate Existing KPIs for Relevance and Effectiveness
- › 2.6 Create a KPI Monitoring and Reporting Framework

• 3 Data Collection Methods for Performance Evaluation — 6 classes

- › 3.1 Identify Key Performance Indicators for Supply Chain Evaluation
- › 3.2 Explore Qualitative Data Collection Techniques in Performance Evaluation
- › 3.3 Analyze Quantitative Data Collection Methods for Effective Reporting
- › 3.4 Evaluate the Role of Surveys in Gathering Performance Feedback
- › 3.5 Implement Case Studies as a Data Collection Tool for Performance Insights
- › 3.6 Determine Best Practices for Integrating Data Collection into Supply Chain Management

• 4 Analyzing Performance Data for Security Enhancement — 6 classes

- › 4.1 Identify Key Performance Indicators for Security Assessment
- › 4.2 Collect and Organize Performance Data from Supply Chains
- › 4.3 Analyze Data Trends to Spot Security Vulnerabilities
- › 4.4 Utilize Risk Assessment Tools to Measure Performance Impact
- › 4.5 Develop Actionable Strategies Based on Data Analysis
- › 4.6 Present Findings and Recommendations for Security Enhancements

• 5 Developing Action Plans Based on Performance Evaluation Outcomes — 6 classes

- › 5.1 Analyze Performance Evaluation Data to Identify Gaps
- › 5.2 Set SMART Objectives for Improvement Based on Findings
- › 5.3 Design Strategic Action Plans Tailored to Performance Outcomes
- › 5.4 Allocate Resources Effectively to Implement Action Plans
- › 5.5 Establish Metrics for Monitoring Progress and Effectiveness
- › 5.6 Review and Revise Action Plans Based on Continuous Feedback

• 1 Understanding Policy Frameworks in Supply Chain Security — 6 classes

- › 1.1 Define Key Components of Policy Frameworks in Supply Chain Security
- › 1.2 Identify Legal and Regulatory Requirements Impacting Supply Chain Security Policies
- › 1.3 Analyze Risk Assessment Methods for Effective Policy Development
- › 1.4 Explore Stakeholder Roles in Policy Formulation and Implementation
- › 1.5 Develop a Model Policy Framework for Supply Chain Security
- › 1.6 Evaluate the Effectiveness of Policies Through Monitoring and Review Mechanisms

• 2 Risk Assessment and Management in Policy Development — 6 classes

- › 2.1 Identify Key Risks in Supply Chain Management
- › 2.2 Evaluate the Impact of Identified Risks on Policies
- › 2.3 Develop Risk Mitigation Strategies for Policy Enhancement
- › 2.4 Integrate Risk Management into Policy Development Processes
- › 2.5 Monitor and Assess the Effectiveness of Risk Management Policies
- › 2.6 Communicate Risk Management Policies to Stakeholders

• 3 Stakeholder Engagement and Policy Buy-In — 6 classes

- › 3.1 Identify Key Stakeholders in Supply Chain Security
- › 3.2 Analyze Stakeholder Needs and Expectations
- › 3.3 Develop Effective Communication Strategies for Engagement
- › 3.4 Create Inclusive Policy Drafts for Stakeholder Feedback
- › 3.5 Facilitate Stakeholder Workshops for Policy Buy-In
- › 3.6 Evaluate Stakeholder Feedback and Revise Policies Accordingly

• 4 Implementation Strategies for Security Policies — 6 classes

- › 4.1 Analyze Current Security Policies for Effectiveness
- › 4.2 Identify Key Stakeholders in Policy Implementation
- › 4.3 Develop Action Plans for Security Policy Rollout
- › 4.4 Design Communication Strategies for Policy Awareness
- › 4.5 Evaluate Compliance Mechanisms for Security Policies
- › 4.6 Assess Continuous Improvement Strategies in Security Management

• 5 Monitoring, Evaluation, and Continuous Improvement of Policies — 6 classes

- › 5.1 Define Key Performance Indicators for Policy Monitoring
- › 5.2 Develop a Structured Evaluation Framework for Policies
- › 5.3 Implement Feedback Mechanisms for Policy Assessment
- › 5.4 Analyze Data to Evaluate Policy Effectiveness
- › 5.5 Identify Areas for Improvement in Existing Policies
- › 5.6 Create an Action Plan for Policy Continuous Improvement

• 1 Fundamentals of Risk Identification in Supply Chains — 6 classes

- › 1.1 Define Key Concepts in Supply Chain Risk
- › 1.2 Identify Common Risks in Supply Chains
- › 1.3 Analyze the Impact of Identified Risks
- › 1.4 Explore Risk Assessment Techniques for Supply Chains
- › 1.5 Develop Risk Identification Tools and Templates
- › 1.6 Apply Risk Identification Methods to Real-World Scenarios

• 2 Analyzing Internal and External Risks — 6 classes

- › 2.1 Define Internal and External Risks in Supply Chain Management
- › 2.2 Identify Key Internal Risks Through Team Collaboration
- › 2.3 Assess External Risks Using Market Analysis Techniques
- › 2.4 Evaluate the Impact of Identified Risks on Operations
- › 2.5 Develop Risk Mitigation Strategies for Internal and External Risks
- › 2.6 Create a Risk Assessment Report for Stakeholder Review

• 3 Risk Assessment Methodologies — 6 classes

- › 3.1 Understand Risk Assessment Methodologies and Their Importance
- › 3.2 Identify Key Components of a Risk Assessment Process
- › 3.3 Explore Qualitative Risk Assessment Techniques
- › 3.4 Analyze Quantitative Risk Assessment Approaches
- › 3.5 Compare and Contrast Different Risk Assessment Frameworks
- › 3.6 Apply Risk Assessment Methodologies to a Supply Chain Scenario

• 4 Quantitative and Qualitative Risk Evaluation Techniques — 6 classes

- › 4.1 Compare Quantitative and Qualitative Risk Evaluation Techniques
- › 4.2 Identify Key Metrics for Quantitative Risk Assessment
- › 4.3 Develop a Qualitative Risk Matrix for Prioritization
- › 4.4 Analyze Probability and Impact in Risk Scenarios
- › 4.5 Integrate Both Techniques for Comprehensive Risk Evaluation
- › 4.6 Apply Risk Evaluation Techniques to Case Studies

• 5 Developing Risk Mitigation Strategies — 6 classes

- › 5.1 Identify Potential Risks in Supply Chain Processes
- › 5.2 Analyze the Impact of Identified Risks
- › 5.3 Prioritize Risks Based on Severity and Likelihood
- › 5.4 Develop Tailored Mitigation Strategies for High-Priority Risks
- › 5.5 Evaluate the Effectiveness of Risk Mitigation Strategies
- › 5.6 Communicate Risk Management Plans to Stakeholders

• 1 Understanding Security Management Frameworks in Supply Chains — 6 classes

- › 1.1 Define Security Management Frameworks in Supply Chains
- › 1.2 Identify Key Components of Security Management Frameworks
- › 1.3 Analyze the Role of ISO 28000 in Supply Chain Security
- › 1.4 Evaluate the Benefits of Implementing Security Management Frameworks
- › 1.5 Develop Strategies for Risk Assessment in Supply Chains
- › 1.6 Apply Security Management Frameworks to Real-World Scenarios

• 2 Identifying and Assessing Security Risks in Supply Chains — 6 classes

- › 2.1 Define Key Security Risks in Supply Chains
- › 2.2 Explore the Impact of Security Risks on Supply Chain Operations
- › 2.3 Identify Common Vulnerabilities in Supply Chain Processes
- › 2.4 Conduct a Risk Assessment Framework for Supply Chain Risks
- › 2.5 Analyze Case Studies of Supply Chain Security Breaches
- › 2.6 Develop a Risk Mitigation Strategy for Supply Chain Security

• 3 Implementing Security Policies and Procedures — 6 classes

- › 3.1 Assessing Current Security Policies for Effective Implementation
- › 3.2 Identifying Key Stakeholders in the Security Management Process
- › 3.3 Developing Clear and Actionable Security Procedures
- › 3.4 Communicating Security Policies to All Supply Chain Participants
- › 3.5 Monitoring Compliance with Security Policies and Procedures
- › 3.6 Evaluating and Adjusting Security Policies for Continuous Improvement

• 4 Monitoring and Reviewing Security Management Systems — 6 classes

- › 4.1 Assess Current Security Management Systems
- › 4.2 Identify Key Performance Indicators for Security
- › 4.3 Analyze Data and Trends in Security Performance
- › 4.4 Conduct Risk Assessments in Security Frameworks
- › 4.5 Develop an Improvement Plan for Security Management
- › 4.6 Review and Revise Security Policies and Procedures

• 5 Integrating Security Management Frameworks with Business Strategy — 6 classes

- › 5.1 Analyze the Role of Security Management in Business Strategy
- › 5.2 Identify Key Components of Security Management Frameworks
- › 5.3 Assess the Impact of Security Threats on Supply Chain Operations
- › 5.4 Develop Strategies for Integrating Security and Business Goals
- › 5.5 Create a Security Management Plan Aligned with Business Objectives
- › 5.6 Evaluate the Effectiveness of Security Integrations in a Business Context