

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 22398 — Security and Resilience Guidelines for Exercises

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-22398 • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	SSR-PCR-22398
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1

Communication and Coordination

5 chapters · 30 classes 45 marks

• 1 Understanding Communication Principles in Security Contexts — 6 classes

› 1.1 Analyze the Importance of Clear Communication in Security Operations

› 1.2 Identify Key Communication Models Relevant to Security Contexts

› 1.3 Explore Techniques for Effective Message Delivery in Crisis Situations

› 1.4 Examine the Role of Active Listening in Security Coordination

› 1.5 Evaluate Communication Tools and Technologies for Security Exercises

› 1.6 Design a Communication Strategy for Effective Response Coordination

• 2 Establishing Effective Communication Strategies for Emergency Scenarios — 6 classes

› 2.1 Identify Key Communication Stakeholders in Emergencies

› 2.2 Analyze Effective Communication Models for Crisis Situations

› 2.3 Develop Clear Messaging for Diverse Audiences

› 2.4 Establish Communication Channels for Real-Time Coordination

› 2.5 Evaluate Tools and Technologies for Emergency Communication

› 2.6 Conduct a Simulated Exercise to Test Communication Strategies

• 3 Coordination Mechanisms Among Stakeholders in Security Operations — 6 classes

› 3.1 Identify Key Stakeholders in Security Operations

› 3.2 Analyze Communication Channels for Effective Coordination

› 3.3 Develop Coordination Strategies for Crisis Scenarios

› 3.4 Evaluate the Role of Technology in Stakeholder Communication

› 3.5 Implement Best Practices for Information Sharing

› 3.6 Assess the Effectiveness of Coordination Mechanisms Post-Exercise

• 4 Utilizing Technology for Enhanced Communication in Exercises — 6 classes

› 4.1 Explore Digital Communication Tools for Exercises

› 4.2 Assess the Role of Social Media in Crisis Communication

› 4.3 Implement Real-Time Collaboration Platforms for Team Coordination

› 4.4 Utilize Data Analytics for Effective Decision-Making During Exercises

› 4.5 Develop a Communication Strategy Using Mobile Technologies

› 4.6 Evaluate the Impact of Emerging Technologies on Exercise Communication

• 5 Evaluating Communication and Coordination Effectiveness Post-Exercise — 6 classes

› 5.1 Identify Key Communication Metrics from Exercises

› 5.2 Assess Coordination Challenges Encountered During Exercises

› 5.3 Analyze Feedback from Participants on Communication Effectiveness

› 5.4 Compare Pre-Defined Communication Goals with Post-Exercise Outcomes

› 5.5 Develop Recommendations for Improving Future Communication Strategies

› 5.6 Implement a Continuous Improvement Plan for Coordination and Communication

• 1 Fundamentals of Evaluation Techniques in Security Exercises —

6 classes

- › 1.1 Define Key Evaluation Terminology in Security Exercises
- › 1.2 Explore the Purpose and Importance of Evaluation Techniques
- › 1.3 Identify Different Types of Evaluation Techniques Used in Security Exercises
- › 1.4 Analyze Key Components of an Effective Evaluation Framework
- › 1.5 Apply Evaluation Techniques to Real-World Security Scenarios
- › 1.6 Develop a Comprehensive Evaluation Report Based on Exercise Outcomes

• 2 Designing Evaluation Frameworks for Security Scenarios —

6 classes

- › 2.1 Identify Key Criteria for Evaluating Security Exercises
- › 2.2 Develop Measurable Objectives for Evaluation Frameworks
- › 2.3 Design Evaluation Tools for Security Scenario Assessments
- › 2.4 Implement Data Collection Methods for Exercise Evaluations
- › 2.5 Analyze Evaluation Results to Enhance Security Preparedness
- › 2.6 Create an Action Plan Based on Evaluation Insights

• 3 Qualitative vs Quantitative Evaluation Methods —

- › 3.1 Distinguish Between Qualitative and Quantitative Evaluation Methods
- › 3.2 Identify Key Characteristics of Qualitative Evaluation Techniques
- › 3.3 Explore Quantitative Evaluation Tools for Data Collection
- › 3.4 Analyze the Strengths and Weaknesses of Qualitative Methods
- › 3.5 Assess the Impact of Quantitative Data on Decision Making
- › 3.6 Integrate Qualitative and Quantitative Approaches for Comprehensive Evaluation

• 4 Data Collection Techniques for Exercise Evaluation —

6 classes

- › 4.1 Identify Key Data Collection Methods for Evaluation
- › 4.2 Apply Qualitative Data Collection Techniques in Exercises
- › 4.3 Implement Quantitative Data Collection Strategies
- › 4.4 Analyze the Relevance of Collected Data for Improvement
- › 4.5 Integrate Participant Feedback into Evaluation Processes
- › 4.6 Design a Comprehensive Data Collection Plan for Future Exercises

• 5 Analyzing and Reporting Evaluation Outcomes —

6 classes

- › 5.1 Define Key Evaluation Outcomes in Exercises
- › 5.2 Identify Methods for Collecting Evaluation Data
- › 5.3 Analyze Quantitative and Qualitative Evaluation Results
- › 5.4 Develop Effective Reporting Formats for Outcomes
- › 5.5 Utilize Visual Aids to Present Evaluation Findings
- › 5.6 Create Actionable Recommendations Based on Evaluation Outcomes

• 1 Understanding ISO 22398: Framework and Principles for Security Exercises —

6 classes

- › 1.1 Define ISO 22398: Key Concepts and Terminology
- › 1.2 Identify the Benefits of Implementing ISO 22398 in Security Exercises
- › 1.3 Explore the Framework Structure of ISO 22398
- › 1.4 Analyze the Principles Guiding Security Exercises under ISO 22398
- › 1.5 Develop a Basic Exercise Scenario Using ISO 22398 Guidelines
- › 1.6 Evaluate Exercises Based on ISO 22398: Best Practices and Lessons Learned

• 2 Identifying Objectives and Audience for Effective Exercise Design —

6 classes

- › 2.1 Define Exercise Goals for Resilience Training
- › 2.2 Analyze Stakeholder Needs for Exercise Development
- › 2.3 Identify Target Audience Characteristics for Effective Engagement
- › 2.4 Develop Specific Learning Objectives for Exercises
- › 2.5 Align Objectives with ISO 22398 Guidelines
- › 2.6 Create an Audience-Centric Exercise Design Framework

• 3 Crafting Realistic Scenarios: Threats, Risks, and Context —

6 classes

- › 3.1 Identify Key Threats in Exercise Scenarios
- › 3.2 Assess Risks Associated with Specific Threats
- › 3.3 Analyze Contextual Factors Influencing Scenarios
- › 3.4 Develop Realistic Exercise Scenarios Based on Threats and Risks
- › 3.5 Integrate Contextual Factors into Scenario Design
- › 3.6 Evaluate Scenario Realism and Relevance for Exercises

• 4 Developing Exercise Formats: Types and Methodologies —

6 classes

- › 4.1 Identify Key Stakeholders for Exercise Formats
- › 4.2 Analyze Different Exercise Types and Their Purposes
- › 4.3 Evaluate Methodologies for Successful Exercise Execution
- › 4.4 Design an Inclusive Tabletop Exercise Framework
- › 4.5 Develop Scenarios to Enhance Realism and Engagement
- › 4.6 Implement Feedback Mechanisms to Refine Exercise Formats

• 5 Evaluating Exercise Outcomes: Metrics and Continuous Improvement —

6 classes

- › 5.1 Define Key Metrics for Evaluating Exercise Outcomes
- › 5.2 Develop Criteria for Successful Exercise Evaluation
- › 5.3 Implement Data Collection Techniques for Exercises
- › 5.4 Analyze Exercise Results to Identify Strengths and Weaknesses
- › 5.5 Create Action Plans for Continuous Improvement Based on Findings
- › 5.6 Execute Follow-Up Evaluations to Measure Improvement Over Time

• 1 Fundamentals of Leadership in Security Exercises — 6 classes

- › 1.1 Define Leadership Roles in Security Exercises
- › 1.2 Explain the Importance of Effective Communication
- › 1.3 Identify Key Leadership Qualities for Crisis Situations
- › 1.4 Analyze Decision-Making Processes in Security Leadership
- › 1.5 Develop Strategies for Team Motivation During Exercises
- › 1.6 Evaluate Leadership Performance Post-Exercise

• 2 Understanding ISO 22398 Standards and Guidelines — 6 classes

- › 2.1 Explore the Fundamentals of ISO 22398 Standards
- › 2.2 Identify Key Components of Security and Resilience Guidelines
- › 2.3 Analyze Leadership Roles in Security Exercises
- › 2.4 Evaluate Best Practices for Implementing ISO 22398
- › 2.5 Develop a Framework for Conducting Effective Security Exercises
- › 2.6 Assess the Impact of ISO 22398 on Organizational Preparedness

• 3 Strategic Planning for Security Exercises — 6 classes

- › 3.1 Define Strategic Objectives for Security Exercises
- › 3.2 Assess Risks and Vulnerabilities in Security Contexts
- › 3.3 Develop Comprehensive Exercise Scenarios
- › 3.4 Identify Stakeholders and Allocate Roles and Responsibilities
- › 3.5 Establish Evaluation Metrics for Exercise Outcomes
- › 3.6 Create a Framework for Continuous Improvement in Security Exercises

• 4 Leadership Roles and Responsibilities in Exercises — 6 classes

- › 4.1 Define Leadership Roles in Security Exercises
- › 4.2 Identify Essential Responsibilities of Exercise Leaders
- › 4.3 Explore Decision-Making Strategies During Exercises
- › 4.4 Analyze the Importance of Communication in Leadership
- › 4.5 Implement Feedback Mechanisms for Effective Leadership
- › 4.6 Assess Leadership Impact on Exercise Outcomes

• 5 Evaluating and Improving Security Exercise Leadership — 6 classes

- › 5.1 Assessing Current Leadership Practices in Security Exercises
- › 5.2 Identifying Key Leadership Skills for Effective Exercise Management
- › 5.3 Establishing Metrics for Evaluating Exercise Leadership Success
- › 5.4 Gathering Feedback from Participants to Enhance Leadership Effectiveness
- › 5.5 Developing Action Plans for Improvement Based on Evaluation Results
- › 5.6 Implementing Continuous Development Strategies for Security Exercise Leaders

• 1 Understanding Risk Assessment Principles — 6 classes

- › 1.1 Identify Key Concepts of Risk Assessment
- › 1.2 Analyze Types of Risks in Different Environments
- › 1.3 Evaluate the Importance of Risk Assessment in Resilience
- › 1.4 Apply Risk Assessment Frameworks to Real-World Scenarios
- › 1.5 Develop Risk Mitigation Strategies Based on Assessment Findings
- › 1.6 Review and Refine Risk Assessment Processes for Continuous Improvement

• 2 Identifying and Analyzing Threats and Vulnerabilities — 6 classes

- › 2.1 Define and Distinguish Between Threats and Vulnerabilities
- › 2.2 Explore Sources of Threats in Various Contexts
- › 2.3 Conduct a SWOT Analysis to Identify Vulnerabilities
- › 2.4 Assess the Impact of Identified Threats on Operations
- › 2.5 Prioritize Vulnerabilities Based on Risk Level
- › 2.6 Develop Action Plans to Mitigate Identified Threats

• 3 Risk Evaluation and Prioritization Methods — 6 classes

- › 3.1 Define Key Risk Evaluation Terms and Concepts
- › 3.2 Identify Different Risk Assessment Approaches
- › 3.3 Analyze the Role of Data in Risk Evaluation
- › 3.4 Apply a Risk Prioritization Matrix in Practice
- › 3.5 Evaluate Case Studies of Risk Management Outcomes
- › 3.6 Develop a Risk Prioritization Strategy for Your Organization

• 4 Developing Risk Management Strategies — 6 classes

- › 4.1 Identify Key Risks in Your Organization's Context
- › 4.2 Analyze the Impact of Identified Risks on Operations
- › 4.3 Evaluate Existing Risk Management Capability and Resources
- › 4.4 Develop Mitigation Strategies for High-Priority Risks
- › 4.5 Create a Risk Communication Plan for Stakeholders
- › 4.6 Implement and Monitor Risk Management Strategies Effectively

• 5 Monitoring and Reviewing Risk Management Practices — 6 classes

- › 5.1 Identify Key Risk Indicators for Monitoring
- › 5.2 Develop a Framework for Risk Assessment Review
- › 5.3 Analyze Data from Previous Risk Management Practices
- › 5.4 Implement Continuous Monitoring Techniques
- › 5.5 Review and Revise Risk Management Strategies
- › 5.6 Evaluate the Effectiveness of Risk Management Exercises

• 1 Introduction to Scenario Development for ISO 22398 Exercises —

6 classes

- › 1.1 Identify Key Elements of Scenario Development
- › 1.2 Explore the Importance of Realism in Scenarios
- › 1.3 Analyze Different Types of Scenarios for Exercises
- › 1.4 Define Stakeholder Involvement in Scenario Creation
- › 1.5 Construct a Basic Scenario Framework
- › 1.6 Evaluate Scenarios for Effectiveness and Relevance

• 2 Identifying Key Threats and Vulnerabilities — 6 classes

- › 2.1 Examine Current Threat Landscape
- › 2.2 Analyze Organizational Vulnerabilities
- › 2.3 Identify Critical Assets
- › 2.4 Assess Impact of Key Threats
- › 2.5 Prioritize Threats and Vulnerabilities
- › 2.6 Develop Mitigation Strategies

• 3 Crafting Realistic Scenarios: Best Practices — 6 classes

- › 3.1 Define Key Objectives for Scenario Development
- › 3.2 Identify Stakeholder Needs and Perspectives
- › 3.3 Build a Framework for Realistic Scenarios
- › 3.4 Utilize Historical Data to Inform Scenario Creation
- › 3.5 Integrate Variables for Dynamic Scenario Outcomes
- › 3.6 Evaluate and Refine Scenarios through Feedback

• 4 Integrating Stakeholder Perspectives in Scenario Design — 6

classes

- › 4.1 Identify Key Stakeholders for Scenario Development
- › 4.2 Analyze Stakeholder Needs and Expectations
- › 4.3 Engage Stakeholders in the Scenario Creation Process
- › 4.4 Incorporate Diverse Perspectives into Scenarios
- › 4.5 Evaluate Scenarios Through Stakeholder Feedback
- › 4.6 Apply Stakeholder Insights to Enhance Scenario Realism

• 5 Evaluating and Refining Scenarios for Effective Exercises — 6

classes

- › 5.1 Assess Current Scenarios for Realism and Relevance
- › 5.2 Identify Key Variables Influencing Scenario Outcomes
- › 5.3 Develop Evaluation Criteria for Scenario Effectiveness
- › 5.4 Conduct Collaborative Reviews to Enhance Scenarios
- › 5.5 Integrate Feedback to Refine Scenario Details
- › 5.6 Test and Validate Scenarios Through Simulation Exercises