

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 12931 — Performance Criteria for Authentication Tools

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-12931 • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	SSR-PCR-12931
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1 Advanced Security Measures 5 chapters · 30 classes 65 marks • 1 Fundamentals of Authentication Tools in Security — 6 classes › 1.1 Define Key Concepts of Authentication Tools › 1.2 Explore Different Types of Authentication Methods › 1.3 Assess the Importance of ISO Standards in Authentication › 1.4 Examine Performance Criteria for Authentication Tools › 1.5 Identify Real-World Applications of Authentication Tools › 1.6 Develop a Strategic Plan for Implementing Authentication Solutions • 2 ISO 12931 Standards: An Overview — 6 classes › 2.1 Define ISO 12931 and its Importance in Security › 2.2 Identify Key Performance Criteria for Authentication Tools › 2.3 Explain the Role of ISO 12931 in Enhancing Security Measures › 2.4 Compare ISO 12931 with Other Security Standards › 2.5 Analyze Case Studies of ISO 12931 Implementation › 2.6 Develop a Strategy for Integrating ISO 12931 in Organizational Security • 3 Performance Criteria for Authentication Tools — 6 classes › 3.1 Analyze the Importance of Performance Criteria in Authentication Tools › 3.2 Identify Key Performance Indicators for Effective Authentication › 3.3 Evaluate Different Types of Authentication Methods Based on ISO 12931 › 3.4 Compare and Contrast Security Measures in Authentication Performance › 3.5 Implement Best Practices for Measuring Authentication Tool Effectiveness › 3.6 Develop a Strategy for Continuous Improvement in Authentication Performance

• 4 Implementation of Authentication Technologies — 6 classes

› 4.1 Identify Key Authentication Technologies in Modern Security Systems

› 4.2 Analyze the Effectiveness of Biometrics in Authentication

› 4.3 Evaluate Multi-Factor Authentication Techniques and Their Applications

› 4.4 Assess the Integration of Authentication Technologies with Existing Security Frameworks

› 4.5 Develop Strategies for Implementing Authentication Technologies in Organizations

› 4.6 Create a Compliance Checklist for ISO 12931 Certification Requirements

• 5 Evaluating and Improving Authentication Systems — 6 classes

› 5.1 Assess Existing Authentication Methods for Effectiveness

› 5.2 Identify Weaknesses in Current Authentication Systems

› 5.3 Apply ISO 12931 Criteria to Enhance Authentication Tools

› 5.4 Explore Innovations in Authentication Technology

› 5.5 Develop Strategies for Improving User Experience with Authentication

› 5.6 Create a Comprehensive Improvement Plan for Authentication Systems

• 1 Understanding Evaluation Frameworks in ISO 12931 — 6 classes

- › 1.1 Define Key Concepts in Evaluation Frameworks
- › 1.2 Explore ISO 12931 Standards and Requirements
- › 1.3 Identify Evaluation Criteria and Performance Indicators
- › 1.4 Analyze Case Studies of Effective Evaluations
- › 1.5 Develop a Framework for Continuous Improvement
- › 1.6 Implement Evaluation Strategies in Real-World Scenarios

• 2 Identifying Key Performance Indicators for Authentication Tools

— 6 classes

- › 2.1 Define Key Performance Indicators for Authentication Tools
- › 2.2 Analyze Existing Metrics and Their Relevance
- › 2.3 Establish a Framework for Performance Assessment
- › 2.4 Develop Strategies for Continuous Improvement of KPIs
- › 2.5 Implement Regular Review Processes for KPI Effectiveness
- › 2.6 Communicate KPI Results and Insights to Stakeholders

• 3 Methods for Collecting and Analyzing Performance Data — 6

classes

- › 3.1 Identify Key Performance Indicators for Authentication Tools
- › 3.2 Select Appropriate Data Collection Methods for Performance Evaluation
- › 3.3 Design a Data Collection Framework for Continuous Improvement
- › 3.4 Analyze Collected Performance Data Using Statistical Techniques
- › 3.5 Evaluate the Effectiveness of Authentication Tools Based on Data Insights
- › 3.6 Implement Strategies for Continuous Improvement of Performance Metrics

• 4 Implementing Continuous Improvement Strategies — 6 classes

- › 4.1 Analyze Current Practices to Identify Improvement Areas
- › 4.2 Develop Key Performance Indicators for Continuous Improvement
- › 4.3 Create an Action Plan for Implementing Improvement Strategies
- › 4.4 Engage Stakeholders in the Continuous Improvement Process
- › 4.5 Monitor Progress and Evaluate the Effectiveness of Strategies
- › 4.6 Foster a Culture of Continuous Improvement within the Organization

• 5 Case Studies in Evaluation and Improvement of Security Systems

— 6 classes

- › 5.1 Analyze Case Studies of Security System Failures
- › 5.2 Identify Key Factors in Successful Security Implementations
- › 5.3 Evaluate Methodologies for Continuous Improvement in Security
- › 5.4 Apply Performance Criteria to Real-World Security Scenarios
- › 5.5 Develop Improvement Plans Based on Evaluation Findings
- › 5.6 Present and Review Security Improvement Recommendations

• 1 Understanding the ISO 12931 Framework and Its Importance in Security — 6 classes

- › 1.1 Define the ISO 12931 Framework and Its Key Components
- › 1.2 Explain the Significance of ISO 12931 in Security Practices
- › 1.3 Identify the Main Compliance Requirements of ISO 12931
- › 1.4 Analyze the Benefits of Implementing ISO 12931 in Organizations
- › 1.5 Evaluate Real-World Examples of ISO 12931 Implementation
- › 1.6 Develop an Action Plan for Achieving ISO 12931 Compliance

• 2 Key Compliance Requirements of ISO 12931 — 6 classes

- › 2.1 Identify Key Definitions and Terminology of ISO 12931
- › 2.2 Analyze the Core Compliance Requirements of ISO 12931
- › 2.3 Evaluate the Roles and Responsibilities in ISO 12931 Compliance
- › 2.4 Explore the Impact of Non-Compliance under ISO 12931
- › 2.5 Develop Strategies for Achieving ISO 12931 Compliance
- › 2.6 Apply Compliance Requirements through Case Studies and Scenarios

• 3 Performance Criteria for Authentication Tools under ISO 12931 —

6 classes

- › 3.1 Identify Key Performance Criteria for Authentication Tools
- › 3.2 Analyze ISO 12931 Compliance Requirements
- › 3.3 Evaluate Effectiveness of Authentication Tools
- › 3.4 Compare Different Authentication Methods According to ISO Standards
- › 3.5 Develop an Implementation Plan for Compliance with ISO 12931
- › 3.6 Assess Real-World Applications of Authentication Tools in Compliance

• 4 Implementing ISO 12931 Compliance within Organizations — 6

classes

- › 4.1 Assess Existing Compliance Frameworks for ISO 12931
- › 4.2 Identify Key Stakeholders for Implementation
- › 4.3 Develop Training Plans for Staff on ISO 12931 Standards
- › 4.4 Create an Action Plan for Compliance Integration
- › 4.5 Monitor and Evaluate Compliance Progress Regularly
- › 4.6 Implement Continuous Improvement Strategies for Compliance

• 5 Auditing and Continuous Improvement of ISO 12931 Compliance

— 6 classes

- › 5.1 Define ISO 12931 Compliance Requirements
- › 5.2 Identify Key Auditing Tools for Compliance Assessment
- › 5.3 Establish a Framework for Conducting ISO 12931 Audits
- › 5.4 Analyze Audit Findings and Identify Improvement Areas
- › 5.5 Develop Action Plans to Address Compliance Gaps
- › 5.6 Implement Continuous Improvement Strategies for ISO 12931 Compliance

• 1 Foundational Concepts of Authentication Metrics — 6 classes

- › 1.1 Define Authentication Metrics and Their Importance
- › 1.2 Explore Types of Authentication Tools and Their Uses
- › 1.3 Identify Key Performance Indicators for Authentication Tools
- › 1.4 Analyze Evaluation Methods for Authentication Performance
- › 1.5 Examine Case Studies of Authentication Tool Success
- › 1.6 Develop a Framework for Measuring Authentication Effectiveness

• 2 Frameworks for Evaluating Authentication Tools — 6 classes

- › 2.1 Understanding Performance Metrics for Authentication Tools
- › 2.2 Exploring Key Frameworks for Evaluation
- › 2.3 Analyzing ISO 12931 Standards in Authentication Tools
- › 2.4 Identifying Critical Success Factors for Tools Assessment
- › 2.5 Applying Evaluation Techniques to Real-World Scenarios
- › 2.6 Enhancing Tool Selection with Performance Insights

• 3 Key Performance Indicators (KPIs) for Authentication Tools — 6 classes

- › 3.1 Define Key Performance Indicators for Authentication Tools
- › 3.2 Identify Characteristics of Effective KPIs
- › 3.3 Analyze the Role of KPIs in Authentication Performance
- › 3.4 Develop Meaningful KPIs for Specific Authentication Use Cases
- › 3.5 Evaluate Existing KPIs Against ISO 12931 Standards
- › 3.6 Implement Strategies for Monitoring and Reporting KPIs

• 4 Advanced Techniques for Performance Assessment — 6 classes

- › 4.1 Evaluate Existing Performance Metrics for Authentication Tools
- › 4.2 Analyze Advanced Techniques for Data Collection
- › 4.3 Compare Performance Assessment Models in Authentication
- › 4.4 Design a Customized Performance Assessment Framework
- › 4.5 Implement Real-World Case Studies on Performance Assessment
- › 4.6 Develop Recommendations for Continuous Improvement in Authentication Performance

• 5 Best Practices and Future Directions in Authentication Performance — 6 classes

- › 5.1 Identify Best Practices in Authentication Tool Performance
- › 5.2 Evaluate Current Performance Metrics for Authentication
- › 5.3 Analyze Challenges in Authentication Tool Implementation
- › 5.4 Explore Future Trends in Authentication Technologies
- › 5.5 Develop Strategies for Enhancing Authentication Performance
- › 5.6 Create an Action Plan for Implementing Best Practices

• 1 Understanding Risk Management Frameworks in ISO Security — 6 classes

- › 1.1 Define Risk Management Frameworks in ISO Security
- › 1.2 Identify Key Components of ISO 12931 Standards
- › 1.3 Analyze Risk Assessment Techniques in ISO Frameworks
- › 1.4 Evaluate the Role of Authentication Tools in Risk Management
- › 1.5 Develop a Risk Management Strategy Based on ISO Guidelines
- › 1.6 Apply Risk Management Principles to Real-World Scenarios

• 2 Identifying and Assessing Risks in Crime Protection Strategies — 6 classes

- › 2.1 Define Key Risk Concepts in Crime Protection
- › 2.2 Identify Common Risks in Crime Protection Strategies
- › 2.3 Assess Vulnerabilities in Current Crime Protection Measures
- › 2.4 Evaluate Impact of Identified Risks on Crime Strategies
- › 2.5 Prioritize Risks Using a Risk Assessment Matrix
- › 2.6 Develop Mitigation Strategies for High-Priority Risks

• 3 Developing Effective Risk Mitigation Plans — 6 classes

- › 3.1 Identify Key Risks in Authentication Tool Performance
- › 3.2 Analyze Risk Impact and Likelihood for Effective Mitigation
- › 3.3 Develop Targeted Mitigation Strategies for High-Risk Areas
- › 3.4 Create a Risk Mitigation Plan Framework Using ISO 12931 Standards
- › 3.5 Implement Monitoring and Review Procedures for Continuous Improvement
- › 3.6 Communicate Risk Management Strategies to Stakeholders Effectively

• 4 Implementing Risk Management Tools and Techniques — 6 classes

- › 4.1 Identify Key Risk Management Tools
- › 4.2 Analyze Risk Assessment Techniques
- › 4.3 Evaluate Effectiveness of Authentication Tools
- › 4.4 Develop a Risk Mitigation Strategy
- › 4.5 Implement Risk Management Frameworks
- › 4.6 Review and Adapt Risk Management Practices

• 5 Evaluating and Reviewing Risk Management Strategies — 6 classes

- › 5.1 Assess Current Risk Management Strategies
- › 5.2 Identify Key Performance Indicators for Evaluation
- › 5.3 Analyze Risk Management Effectiveness Through Data
- › 5.4 Review Case Studies on Risk Management Success and Failure
- › 5.5 Develop Action Plans for Strategy Improvement
- › 5.6 Share Best Practices for Continuous Risk Management Adaptation

• 1 Understanding ISO 12931: A Framework for Authentication Tools

— 6 classes

- › 1.1 Define ISO 12931 and Its Importance in Security
- › 1.2 Identify Key Components of Authentication Tools
- › 1.3 Analyze the Performance Criteria in ISO 12931
- › 1.4 Evaluate the Impact of Authentication Tools on Security Protocols
- › 1.5 Develop a Strategy for Implementing ISO 12931 in Teams
- › 1.6 Create a Case Study Presentation on ISO 12931 Applications

• 2 Key Performance Criteria for Security Leadership — 6 classes

- › 2.1 Define Key Performance Criteria for Security Leadership
- › 2.2 Identify Essential Authentication Tools for Security Protocols
- › 2.3 Analyze the Impact of Leadership on Security Outcomes
- › 2.4 Evaluate Performance Metrics within Security Teams
- › 2.5 Develop Action Plans to Enhance Security Leadership Effectiveness
- › 2.6 Implement Best Practices for Continuous Improvement in Security Protocols

• 3 Establishing Effective Security Protocols — 6 classes

- › 3.1 Analyze Current Security Practices in Your Organization
- › 3.2 Identify Key Threats and Vulnerabilities in Security Protocols
- › 3.3 Develop Clear and Comprehensive Security Protocol Guidelines
- › 3.4 Implement Training Programs for Team Members on Security Protocols
- › 3.5 Evaluate the Effectiveness of Existing Security Measures
- › 3.6 Foster a Culture of Continuous Improvement in Security Practices

• 4 Team Dynamics and Leadership in Security Operations — 6 classes

- › 4.1 Analyze Team Roles in Security Operations
- › 4.2 Develop Effective Communication Strategies for Leadership
- › 4.3 Implement Conflict Resolution Techniques in Security Teams
- › 4.4 Assess the Impact of Team Dynamics on Security Protocols
- › 4.5 Create a Collaborative Environment for Security Operations
- › 4.6 Evaluate Leadership Styles in the Context of Team Performance

• 5 Evaluating and Enhancing Security Leadership Performance — 6 classes

- › 5.1 Assessing Current Security Leadership Practices
- › 5.2 Identifying Key Performance Indicators for Leaders
- › 5.3 Analyzing Common Challenges in Security Leadership
- › 5.4 Developing Strategies for Leadership Improvement
- › 5.5 Implementing Feedback Mechanisms in Teams
- › 5.6 Measuring the Impact of Enhanced Leadership on Security Outcomes