LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001SMC — Information Security in Smart City Systems

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 MGT-SMC-27001SMC • ISO Management & Services

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	30	180	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**MGT-SMC-27001SMC**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Compliance and Auditing

5 chapters · 30 classes · **65 marks**

• 1 Understanding Compliance in Smart City Frameworks — 6 classes

- › 1.1 Define Compliance Metrics in Smart City Systems
- › 1.2 Identify Key Regulatory Frameworks Affecting Smart City Compliance
- › 1.3 Analyze Risk Assessment Processes for Smart City Operations
- › 1.4 Explore the Role of Auditing in Smart City Compliance
- › 1.5 Develop an Action Plan for Compliance Improvement in Smart Cities
- › 1.6 Implement Continuous Monitoring Strategies for Compliance Assurance

• 2 Key Auditing Standards and Best Practices — 6 classes

- › 2.1 Identify Key Auditing Standards in Information Security
- › 2.2 Analyze Best Practices for Compliance in Smart City Systems
- › 2.3 Evaluate the Role of Leadership in Audit Processes
- › 2.4 Develop a Compliance Checklist for ISO 27001SMC
- › 2.5 Apply Risk Assessment Techniques in Auditing Smart Cities
- › 2.6 Create an Action Plan for Implementing Auditing Best Practices

• 3 Conducting Compliance Audits in Smart City Environments — 6 classes

- › 3.1 Define Compliance Requirements for Smart City Systems
- › 3.2 Identify Key Stakeholders in Compliance Audit Processes
- › 3.3 Develop an Audit Plan Tailored to Smart City Environments
- › 3.4 Execute Compliance Audits Using Best Practices
- › 3.5 Evaluate Audit Findings and Identify Non-Compliance Risks
- › 3.6 Communicate Audit Results and Recommend Corrective Actions

• 4 Identifying and Mitigating Compliance Risks — 6 classes

- › 4.1 Analyze Common Compliance Risks in Smart Cities
- › 4.2 Assess Current Compliance Measures and Gaps
- › 4.3 Identify Key Stakeholders for Compliance Risk Management
- › 4.4 Develop Mitigation Strategies for Identified Risks
- › 4.5 Create a Compliance Risk Assessment Framework
- › 4.6 Implement and Monitor Compliance Risk Mitigation Plans

• 5 Creating and Implementing Auditing Frameworks — 6 classes

- › 5.1 Define Key Concepts in Auditing Frameworks
- › 5.2 Identify Compliance Requirements for Smart City Systems
- › 5.3 Develop a Risk Assessment Methodology for Auditing
- › 5.4 Create Templates for Audit Documentation and Reporting
- › 5.5 Implement Continuous Monitoring Strategies for Compliance
- › 5.6 Evaluate Audit Outcomes and Enhance Framework Effectiveness

2 Cybersecurity Strategies

5 chapters · 30 classes **65 marks**

- **1 Understanding Cybersecurity Fundamentals in Smart Cities** — 6 classes
  - 1.1 Define Key Concepts in Cybersecurity for Smart Cities
  - 1.2 Identify Common Cyber Threats in Smart City Environments
  - 1.3 Explore the Role of Security Frameworks in Cyber Resilience
  - 1.4 Analyze the Impact of Data Privacy Regulations on Cybersecurity
  - 1.5 Examine Best Practices for Securing Smart City Infrastructure
  - 1.6 Develop a Basic Cybersecurity Strategy for Smart City Projects
- **2 Risk Assessment and Management in Smart City Environments** — 6 classes
  - 2.1 Identify Key Risks in Smart City Systems
  - 2.2 Analyze Vulnerabilities within Urban Infrastructure
  - 2.3 Evaluate Impact and Likelihood of Cyber Threats
  - 2.4 Develop Risk Mitigation Strategies for Smart Cities
  - 2.5 Implement Monitoring Techniques for Ongoing Risk Assessment
  - 2.6 Communicate Risk Management Findings to Stakeholders
- **3 Implementing Cybersecurity Frameworks and Standards** — 6 classes
  - 3.1 Analyze Key Cybersecurity Frameworks for Smart Cities
  - 3.2 Evaluate ISO 27001 Standards in Urban Environments
  - 3.3 Identify Challenges in Implementing Cybersecurity Frameworks
  - 3.4 Develop a Cybersecurity Implementation Plan for Smart City Systems
  - 3.5 Assess the Effectiveness of Cybersecurity Policies and Procedures
  - 3.6 Create a Response Strategy for Cybersecurity Incidents in Smart Cities
- **4 Incident Response Planning for Smart City Cyber Threats** — 6 classes
  - 4.1 Assessing Cyber Threats in Smart City Infrastructure
  - 4.2 Establishing Roles and Responsibilities in Incident Response
  - 4.3 Developing Communication Strategies for Incident Management
  - 4.4 Creating Playbooks for Common Cyber Incidents
  - 4.5 Conducting Tabletop Exercises for Smart City Scenarios
  - 4.6 Reviewing and Updating Incident Response Plans Regularly
- **5 Future Trends in Cybersecurity for Smart Cities** — 6 classes
  - 5.1 Analyze Emerging Cybersecurity Technologies for Smart Cities
  - 5.2 Evaluate the Impact of IoT on Cybersecurity Protocols
  - 5.3 Explore AI and Machine Learning in Cyber Threat Detection
  - 5.4 Assess the Role of Blockchain in Secure Smart City Infrastructure
  - 5.5 Develop Proactive Cybersecurity Strategies for Urban Environments
  - 5.6 Implement Risk Management Frameworks in Smart City Projects

3 Data Privacy and Protection

5 chapters · 30 classes **85 marks**

- **1 Understanding Data Privacy Regulations in Smart Cities** — 6 classes
  - 1.1 Identify Key Data Privacy Regulations Impacting Smart Cities
  - 1.2 Analyze the Role of GDPR in Protecting Citizen Data
  - 1.3 Explore Data Protection Principles Relevant to Smart City Initiatives
  - 1.4 Evaluate Compliance Strategies for Data Privacy in Urban Systems
  - 1.5 Assess the Implications of Data Breaches in Smart City Contexts
  - 1.6 Develop a Data Protection Framework for Smart City Projects
- **2 Risk Assessment and Management for Data Protection** — 6 classes
  - 2.1 Identify Critical Data Assets in Smart City Systems
  - 2.2 Assess Threats and Vulnerabilities to Data Privacy
  - 2.3 Evaluate the Impact of Data Breaches on Stakeholders
  - 2.4 Perform Risk Analysis for Data Protection in Smart Cities
  - 2.5 Develop Mitigation Strategies for Identified Risks
  - 2.6 Implement and Review Risk Management Procedures
- **3 Implementing Data Protection by Design and by Default** — 6 classes
  - 3.1 Understand the Principles of Data Protection by Design
  - 3.2 Identify Stakeholders in Smart City Data Protection
  - 3.3 Analyze Data Flow and Identify Privacy Risks
  - 3.4 Develop Strategies for Data Minimization
  - 3.5 Implement Default Settings for Maximum Privacy
  - 3.6 Evaluate and Monitor Data Protection Measures
- **4 Anonymization and Pseudonymization Techniques** — 6 classes
  - 4.1 Define Anonymization and Pseudonymization Techniques
  - 4.2 Explore the Legal Framework Surrounding Data Anonymization
  - 4.3 Identify Use Cases for Anonymization in Smart City Systems
  - 4.4 Compare Anonymization and Pseudonymization: Key Differences
  - 4.5 Analyze the Impact of Data Anonymization on User Privacy
  - 4.6 Implement a Basic Anonymization Strategy for Smart City Data
- **5 Incident Response and Data Breach Management in Smart Cities** — 6 classes
  - 5.1 Identify key components of an incident response plan for smart cities
  - 5.2 Analyze common data breach scenarios in smart city environments
  - 5.3 Assess legal and regulatory requirements for data breach management
  - 5.4 Develop a communication strategy for reporting data breaches
  - 5.5 Implement immediate response actions in a simulated breach scenario
  - 5.6 Evaluate post-incident review processes for continuous improvement

4 Implementing ISMS

5 chapters · 30 classes **65 marks**

- **1 Understanding the Framework of ISMS in Smart City Contexts** — 6 classes
  - 1.1 Define the Key Components of ISMS in Smart Cities
  - 1.2 Explore the ISO 27001 Framework and Its Relevance
  - 1.3 Identify Stakeholders and Their Roles in ISMS Implementation
  - 1.4 Assess Risks Specific to Smart City Information Systems
  - 1.5 Develop Policies and Procedures for ISMS Governance
  - 1.6 Evaluate the Effectiveness of ISMS in Smart City Projects
- **2 Risk Assessment and Management for Smart City Systems** — 6 classes
  - 2.1 Identify Potential Risks in Smart City Systems
  - 2.2 Analyze Risk Impact and Likelihood
  - 2.3 Prioritize Risks for Smart City Management
  - 2.4 Develop Mitigation Strategies for Identified Risks
  - 2.5 Implement Risk Management Procedures in Smart City Projects
  - 2.6 Evaluate Continuous Improvement of Risk Management Practices
- **3 Development and Implementation of ISMS Policies** — 6 classes
  - 3.1 Analyze Current Security Needs for ISMS Development
  - 3.2 Define Key Components of Effective ISMS Policies
  - 3.3 Evaluate Risk Management Strategies for Smart City Systems
  - 3.4 Formulate Clear Objectives for ISMS Implementation
  - 3.5 Draft and Review ISMS Policies for Compliance and Effectiveness
  - 3.6 Implement Training Programs to Support ISMS Adoption
- **4 Monitoring and Reviewing ISMS Effectiveness** — 6 classes
  - 4.1 Define Key Performance Indicators for ISMS Monitoring
  - 4.2 Develop Monitoring Strategies for Smart City Systems
  - 4.3 Implement Tools and Techniques for ISMS Reviews
  - 4.4 Analyze Data from ISMS Monitoring Activities
  - 4.5 Conduct Effective ISMS Review Meetings and Feedback Sessions
  - 4.6 Integrate Continuous Improvement Practices into ISMS Management
- **5 Leadership and Culture in Enhancing ISMS Adoption** — 6 classes
  - 5.1 Define Leadership Roles in ISMS Adoption
  - 5.2 Identify Cultural Barriers to ISMS Implementation
  - 5.3 Develop a Vision for Information Security in Smart Cities
  - 5.4 Foster a Culture of Security Awareness Among Stakeholders
  - 5.5 Implement Communication Strategies for ISMS Culture Shift
  - 5.6 Evaluate Leadership Impact on ISMS Adoption Success

5 Introduction to ISO 27001

5 chapters · 30 classes **65 marks**

- **1 Understanding the Fundamentals of Information Security Standards** — 6 classes
  - 1.1 Define Key Terms in Information Security Standards
  - 1.2 Explore the Purpose and Importance of ISO 27001
  - 1.3 Identify Core Principles of Information Security Management
  - 1.4 Examine the Structure of ISO 27001 Documentation
  - 1.5 Outline the Benefits of Compliance with ISO 27001
  - 1.6 Apply Information Security Standards to Smart City Systems
- **2 Key Components and Structure of ISO 27001** — 6 classes
  - 2.1 Identify the Purpose and Scope of ISO 27001
  - 2.2 Explore the Context of the Organization in ISO 27001
  - 2.3 Define Information Security Risks and Opportunities
  - 2.4 Understand the Structure of ISO 27001 Clauses
  - 2.5 Analyze the Requirements of an Information Security Management System (ISMS)
  - 2.6 Apply ISO 27001 Key Components to Smart City Systems
- **3 Risk Management Principles in ISO 27001** — 6 classes
  - 3.1 Understand the Importance of Risk Management in ISO 27001
  - 3.2 Identify Key Concepts and Terminology in Risk Management
  - 3.3 Explore the Risk Management Process in ISO 27001
  - 3.4 Analyze Different Types of Risks in Smart City Systems
  - 3.5 Assess the Impact and Likelihood of Identified Risks
  - 3.6 Develop Risk Treatment Plans in Compliance with ISO 27001
- **4 Implementation Strategies for ISO 27001 in Smart City Systems** — 6 classes
  - 4.1 Understand the Core Principles of ISO 27001
  - 4.2 Identify Key Stakeholders in Smart City Systems
  - 4.3 Assess Current Information Security Posture in Smart Cities
  - 4.4 Develop a Risk Management Framework for Smart City Environments
  - 4.5 Establish an Implementation Roadmap for ISO 27001 Compliance
  - 4.6 Monitor and Review the Effectiveness of ISO 27001 Strategies
- **5 Certification Process and Continuous Improvement in ISO 27001** — 6 classes
  - 5.1 Understand the ISO 27001 Certification Process
  - 5.2 Identify Key Steps in Preparing for ISO 27001 Certification
  - 5.3 Explore Auditing Techniques for ISO 27001 Compliance
  - 5.4 Recognize the Role of Leadership in ISO 27001 Implementation
  - 5.5 Analyze Continuous Improvement Strategies in ISO 27001
  - 5.6 Develop an Action Plan for Sustaining ISO 27001 Compliance

6 Risk Management in Smart Cities

5 chapters · 30 classes **85 marks**

- **1 Fundamentals of Risk Management in Smart Cities** — 6 classes
  - 1.1 Define Risk Management Concepts in Smart Cities
  - 1.2 Identify Key Risks Specific to Smart City Systems
  - 1.3 Evaluate the Impact of Risks on Smart City Operations
  - 1.4 Develop Risk Assessment Criteria for Smart Cities
  - 1.5 Formulate Mitigation Strategies for Identified Risks
  - 1.6 Implement a Risk Management Framework for Smart City Projects
- **2 Identifying and Assessing Risks in Smart City Infrastructure** — 6 classes
  - 2.1 Define Key Risks in Smart City Infrastructure
  - 2.2 Analyze Vulnerabilities in Smart City Systems
  - 2.3 Evaluate the Impact of Risks on Smart City Operations
  - 2.4 Prioritize Risks Based on Likelihood and Consequence
  - 2.5 Develop Risk Assessment Frameworks for Smart Cities
  - 2.6 Implement Risk Mitigation Strategies in Urban Environments
- **3 Mitigation Strategies for Information Security Risks** — 6 classes
  - 3.1 Identify Key Information Security Risks in Smart City Systems
  - 3.2 Evaluate the Impact of Risks on Smart City Operations
  - 3.3 Develop Effective Risk Mitigation Strategies for Smart Cities
  - 3.4 Implement Best Practices for Risk Management in Smart City Projects
  - 3.5 Assess the Effectiveness of Information Security Controls
  - 3.6 Create a Continuous Improvement Plan for Risk Management
- **4 Developing a Risk Management Framework for Smart Cities** — 6 classes
  - 4.1 Define Key Components of a Risk Management Framework
  - 4.2 Assess Risks in Smart City Environments
  - 4.3 Identify Stakeholders and Their Roles in Risk Management
  - 4.4 Develop Mitigation Strategies for Identified Risks
  - 4.5 Establish Monitoring and Review Processes for Risk Management
  - 4.6 Implement a Risk Communication Plan for Smart Cities
- **5 Continuous Monitoring and Improvement of Risk Management Practices** — 6 classes
  - 5.1 Assess Current Risk Monitoring Practices in Smart Cities
  - 5.2 Identify Key Performance Indicators for Risk Management
  - 5.3 Develop Strategies for Continuous Risk Assessment
  - 5.4 Implement Tools for Real-time Risk Monitoring
  - 5.5 Analyze Data to Improve Risk Management Decisions
  - 5.6 Foster a Culture of Continuous Improvement in Risk Practices