LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27400 — IoT Security and Privacy Guidelines

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 IIT-IOT-27400 • ISO IT & Related Technologies

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	**IIT-IOT-27400**
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 Standards

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

- **1 Understanding ISO 27400: Overview and Objectives** — 6 classes
  - 1.1 Define ISO 27400 and Its Importance in IoT Security
  - 1.2 Identify Key Objectives of ISO 27400 Guidelines
  - 1.3 Explore the Scope of IoT Security and Privacy Standards
  - 1.4 Analyze the Benefits of ISO 27400 Compliance for Organizations
  - 1.5 Evaluate Real-world Applications of ISO 27400 in IoT Solutions
  - 1.6 Formulate an Action Plan for Implementing ISO 27400 in Your Organization
- **2 Key Principles of IoT Security and Privacy** — 6 classes
  - 2.1 Identify Key Principles of IoT Security
  - 2.2 Analyze Privacy Implications in IoT Systems
  - 2.3 Explore Risk Assessment Techniques for IoT
  - 2.4 Evaluate Compliance with ISO 27400 Standards
  - 2.5 Develop a Security Framework for IoT Devices
  - 2.6 Implement Privacy-Enhancing Technologies in IoT Solutions
- **3 Compliance Requirements: A Detailed Examination** — 6 classes
  - 3.1 Identify Key Compliance Requirements in IoT Security
  - 3.2 Analyze the Impact of Compliance on IoT Privacy Standards
  - 3.3 Evaluate Current Regulations Relevant to IoT Security
  - 3.4 Compare ISO 27400 with Other IoT Security Frameworks
  - 3.5 Assess Organizational Readiness for Compliance Implementation
  - 3.6 Develop a Compliance Action Plan for IoT Security
- **4 Implementing Best Practices for Compliance** — 6 classes
  - 4.1 Identify Key Compliance Frameworks for IoT Security
  - 4.2 Assess Current Practices Against ISO 27400 Standards
  - 4.3 Develop a Risk Management Strategy for IoT Deployment
  - 4.4 Implement Data Privacy Measures According to Guidelines
  - 4.5 Establish Continuous Monitoring and Reporting Mechanisms
  - 4.6 Foster a Culture of Compliance and Security Awareness
- **5 Assessments, Audits, and Continuous Improvement** — 6 classes
  - 5.1 Identify Key Components of Assessments in IoT Security
  - 5.2 Conduct a Risk Assessment for IoT Devices and Systems
  - 5.3 Evaluate Audit Protocols for Compliance with ISO 27400
  - 5.4 Analyze Findings from Security Audits and Assessments
  - 5.5 Develop Continuous Improvement Plans Based on Audit Results
  - 5.6 Implement Best Practices for Ongoing Compliance and Assessment

2 Data Privacy Measures

5 chapters · 30 classes **65 marks**

- **1 Understanding Data Privacy in IoT Ecosystems** — 6 classes
  - 1.1 Define Key Concepts of Data Privacy in IoT
  - 1.2 Identify Data Privacy Risks in IoT Ecosystems
  - 1.3 Evaluate Regulatory Frameworks Affecting IoT Privacy
  - 1.4 Analyze Best Practices for Data Collection in IoT
  - 1.5 Implement Privacy-Enhancing Technologies in IoT
  - 1.6 Develop a Data Privacy Strategy for IoT Devices
- **2 Identifying Personal Data in IoT Systems** — 6 classes
  - 2.1 Define Personal Data in the Context of IoT Systems
  - 2.2 Recognize Different Types of Personal Data in IoT Devices
  - 2.3 Assess the Impact of Data Collection on User Privacy
  - 2.4 Identify Data Flow within IoT Systems and Personal Data Traceability
  - 2.5 Evaluate Regulatory Requirements for Personal Data in IoT
  - 2.6 Develop Strategies for Minimizing Personal Data Exposure in IoT
- **3 Implementing Data Minimization Strategies** — 6 classes
  - 3.1 Define Data Minimization and Its Importance in IoT Security
  - 3.2 Identify Key Principles of Data Minimization Strategies
  - 3.3 Assess Current Data Collection Practices for Minimization Opportunities
  - 3.4 Develop a Data Minimization Policy for Your Organization
  - 3.5 Implement Practical Data Minimization Techniques in IoT Devices
  - 3.6 Evaluate the Effectiveness of Data Minimization Strategies Post-Implementation
- **4 Assessing Risks to Data Privacy in IoT** — 6 classes
  - 4.1 Identify Key Data Privacy Risks in IoT Environments
  - 4.2 Analyze Common Vulnerabilities Affecting IoT Devices
  - 4.3 Evaluate the Impact of Data Breaches on Privacy
  - 4.4 Assess Regulatory Compliance Standards for IoT Data Privacy
  - 4.5 Develop Risk Mitigation Strategies for IoT Data Privacy Risks
  - 4.6 Implement a Privacy Risk Assessment Framework for IoT Deployments
- **5 Establishing Compliance and Governance for Data Privacy** — 6 classes
  - 5.1 Identify Key Components of Data Privacy Regulations
  - 5.2 Analyze Organizational Roles in Data Governance
  - 5.3 Develop a Data Privacy Compliance Framework
  - 5.4 Assess Risks Associated with Data Handling Practices
  - 5.5 Implement Monitoring Tools for Compliance Auditing
  - 5.6 Communicate Data Privacy Policies Across the Organization

3 Implementation of Security Protocols

5 chapters · 30 classes **45 marks**

- **1 Understanding IoT Security Frameworks and Standards** — 6 classes
  - 1.1 Define Key Concepts of IoT Security Frameworks
  - 1.2 Identify Relevant Standards for IoT Security
  - 1.3 Analyze the Role of ISO 27400 in IoT Security
  - 1.4 Compare Different IoT Security Frameworks
  - 1.5 Evaluate Security Protocols for IoT Implementation
  - 1.6 Develop a Security Protocol Action Plan for IoT
- **2 Core Security Protocols for IoT Implementation** — 6 classes
  - 2.1 Identify Key Security Protocols for IoT Systems
  - 2.2 Evaluate Encryption Techniques for Data Protection
  - 2.3 Implement Authentication Mechanisms for Device Security
  - 2.4 Assess Vulnerability Management Strategies for IoT
  - 2.5 Monitor and Maintain Security Protocols in IoT Environments
  - 2.6 Develop a Response Plan for IoT Security Breaches
- **3 Risk Assessment and Vulnerability Analysis in IoT Networks** — 6 classes
  - 3.1 Identify IoT Network Assets for Risk Assessment
  - 3.2 Analyze Potential Threats in IoT Environments
  - 3.3 Evaluate Vulnerabilities in IoT Device Configurations
  - 3.4 Assess Impact and Likelihood of IoT Security Risks
  - 3.5 Develop a Risk Prioritization Strategy for IoT Networks
  - 3.6 Create an Action Plan for Mitigating IoT Vulnerabilities
- **4 Developing a Comprehensive IoT Security Policy** — 6 classes
  - 4.1 Identify Key Components of an IoT Security Policy
  - 4.2 Conduct a Risk Assessment for IoT Devices
  - 4.3 Define Access Control Measures for IoT Networks
  - 4.4 Establish Data Encryption Standards for IoT Communication
  - 4.5 Develop Incident Response Procedures for IoT Security Breaches
  - 4.6 Review and Update IoT Security Policies Regularly
- **5 Implementing and Testing Security Measures in IoT Deployments** — 6 classes
  - 5.1 Identify Key Security Risks in IoT Deployments
  - 5.2 Select Appropriate Security Protocols for IoT Devices
  - 5.3 Develop a Security Implementation Plan for IoT Systems
  - 5.4 Configure Security Settings in IoT Devices
  - 5.5 Conduct Vulnerability Assessments on IoT Implementations
  - 5.6 Evaluate the Effectiveness of Security Measures in IoT Deployments

4 IoT Security Frameworks

5 chapters · 30 classes **105 marks**

- **1 Introduction to IoT Security Concepts and Threat Landscapes** — 6 classes
  - 1.1 Define and Explore Key IoT Security Concepts
  - 1.2 Identify Common IoT Threats and Vulnerabilities
  - 1.3 Analyze Real-world IoT Security Breaches and Impacts
  - 1.4 Discuss Regulatory Requirements in IoT Security
  - 1.5 Evaluate Existing IoT Security Frameworks
  - 1.6 Develop a Basic IoT Security Risk Assessment Plan
- **2 Understanding IoT Security Frameworks and Standards** — 6 classes
  - 2.1 Explore the Importance of IoT Security Frameworks
  - 2.2 Identify Key Components of IoT Security Standards
  - 2.3 Analyze Current IoT Security Frameworks
  - 2.4 Compare Global IoT Security Standards
  - 2.5 Evaluate Best Practices for Implementing IoT Security Frameworks
  - 2.6 Develop a Strategy for IoT Security Compliance
- **3 Risk Assessment and Management in IoT Environments** — 6 classes
  - 3.1 Identify Key Risks in IoT Environments
  - 3.2 Analyze Threat Vectors Specific to IoT Devices
  - 3.3 Evaluate Vulnerabilities in IoT Systems
  - 3.4 Prioritize Risks Based on Impact and Likelihood
  - 3.5 Develop Risk Mitigation Strategies for IoT Solutions
  - 3.6 Implement a Continuous Risk Management Process in IoT
- **4 Implementing Security Controls in IoT Architectures** — 6 classes
  - 4.1 Identify Key Security Challenges in IoT Architectures
  - 4.2 Assess Risk Factors for IoT Devices and Networks
  - 4.3 Develop a Security Control Framework for IoT Implementations
  - 4.4 Implement Cryptographic Measures for Data Protection in IoT
  - 4.5 Establish Access Control Mechanisms for IoT Applications
  - 4.6 Evaluate and Adapt Security Controls for Evolving IoT Threats
- **5 Emerging Trends and Future Directions in IoT Security** — 6 classes
  - 5.1 Analyze Emerging IoT Security Threats and Vulnerabilities
  - 5.2 Examine Current Security Frameworks in IoT
  - 5.3 Explore Privacy Considerations in IoT Development
  - 5.4 Discuss the Role of AI in Enhancing IoT Security
  - 5.5 Evaluate Future Trends in IoT Security Technologies
  - 5.6 Implement Best Practices for Future-proofing IoT Security

5 Risk Management in IoT

5 chapters · 30 classes **85 marks**

- **1 Understanding IoT Ecosystems and Risk Factors** — 6 classes
  - 1.1 Identify Components of the IoT Ecosystem
  - 1.2 Analyze Potential Risk Factors in IoT
  - 1.3 Examine the Interconnectedness of IoT Devices
  - 1.4 Evaluate Security Challenges in IoT Implementations
  - 1.5 Assess Privacy Implications in IoT Data Management
  - 1.6 Develop a Risk Management Strategy for IoT Solutions
- **2 Identifying and Assessing Risks in IoT Systems** — 6 classes
  - 2.1 Define Key Risk Concepts in IoT Systems
  - 2.2 Identify Common IoT Vulnerabilities and Threats
  - 2.3 Analyze the Impact of Risks on IoT Operations
  - 2.4 Assess Likelihood and Severity of IoT Risks
  - 2.5 Develop Risk Assessment Matrices for IoT Scenarios
  - 2.6 Create a Risk Mitigation Plan for IoT Systems
- **3 Implementing Security Controls and Privacy Measures** — 6 classes
  - 3.1 Identify Security Risks in IoT Systems
  - 3.2 Assess Privacy Vulnerabilities in IoT Applications
  - 3.3 Implement Fundamental Security Controls for IoT
  - 3.4 Establish Data Privacy Measures for IoT Devices
  - 3.5 Create an Incident Response Plan for IoT Security Breaches
  - 3.6 Evaluate and Update Security Practices in IoT Regularly
- **4 Monitoring and Responding to IoT Security Incidents** — 6 classes
  - 4.1 Identify Key Indicators of IoT Security Incidents
  - 4.2 Establish Effective Monitoring Protocols for IoT Systems
  - 4.3 Analyze Vulnerabilities in IoT Threat Landscapes
  - 4.4 Develop Incident Response Strategies for IoT Security Breaches
  - 4.5 Implement Communication Plans for Stakeholders During Incidents
  - 4.6 Evaluate and Improve IoT Security Postures After Incidents
- **5 Compliance and Governance in IoT Risk Management** — 6 classes
  - 5.1 Understand IoT Compliance Regulations
  - 5.2 Identify Key Governance Frameworks for IoT
  - 5.3 Assess Privacy Risks in IoT Environments
  - 5.4 Develop IoT Risk Management Policies
  - 5.5 Implement Monitoring Mechanisms for Compliance
  - 5.6 Evaluate the Effectiveness of IoT Governance Practices

6 Strategic Leadership in Security

5 chapters · 30 classes **65 marks**

- **1 Understanding IoT Security Risks and Challenges** — 6 classes
  - 1.1 Identify Key IoT Security Risks
  - 1.2 Analyze Common Challenges in IoT Implementations
  - 1.3 Evaluate Consequences of IoT Security Breaches
  - 1.4 Apply Risk Assessment Techniques to IoT Systems
  - 1.5 Develop Strategies to Mitigate IoT Security Risks
  - 1.6 Present an IoT Security Action Plan for Your Organization
- **2 Frameworks for Effective IoT Security Leadership** — 6 classes
  - 2.1 Analyze the Importance of IoT Security Leadership in Contemporary Frameworks
  - 2.2 Identify Key Components of Effective IoT Security Frameworks
  - 2.3 Evaluate Existing IoT Security Frameworks for Their Efficacy
  - 2.4 Develop Best Practices for Implementing IoT Security Frameworks
  - 2.5 Create a Strategic Plan for Enhancing IoT Security Leadership
  - 2.6 Implement a Case Study to Apply IoT Security Frameworks in Real-World Scenarios
- **3 Developing a Strategic Security Roadmap for IoT** — 6 classes
  - 3.1 Identify Key Components of an IoT Security Roadmap
  - 3.2 Analyze Current IoT Threat Landscape for Strategic Planning
  - 3.3 Establish Security Objectives Aligned with Business Goals
  - 3.4 Develop Risk Assessment Framework for IoT Devices
  - 3.5 Create Actionable Initiatives for Enhancing IoT Security
  - 3.6 Evaluate and Iterate the Strategic Security Roadmap
- **4 Cultivating a Security-First Culture within Organizations** — 6 classes
  - 4.1 Define a Security-First Culture: Key Principles and Concepts
  - 4.2 Assess Current Organizational Practices in Security
  - 4.3 Identify Stakeholders and Their Roles in Promoting Security
  - 4.4 Develop a Communication Strategy for Security Awareness
  - 4.5 Implement Training Programs that Foster a Security Mindset
  - 4.6 Evaluate and Adapt Security Policies for Continuous Improvement
- **5 Evaluating and Responding to IoT Security Incidents** — 6 classes
  - 5.1 Identify Key IoT Security Incident Indicators
  - 5.2 Assess the Impact of IoT Security Breaches
  - 5.3 Analyze Historical IoT Security Incident Case Studies
  - 5.4 Develop a Response Plan for IoT Security Incidents
  - 5.5 Implement Effective Communication Strategies During Incidents
  - 5.6 Evaluate and Improve Incident Response Processes