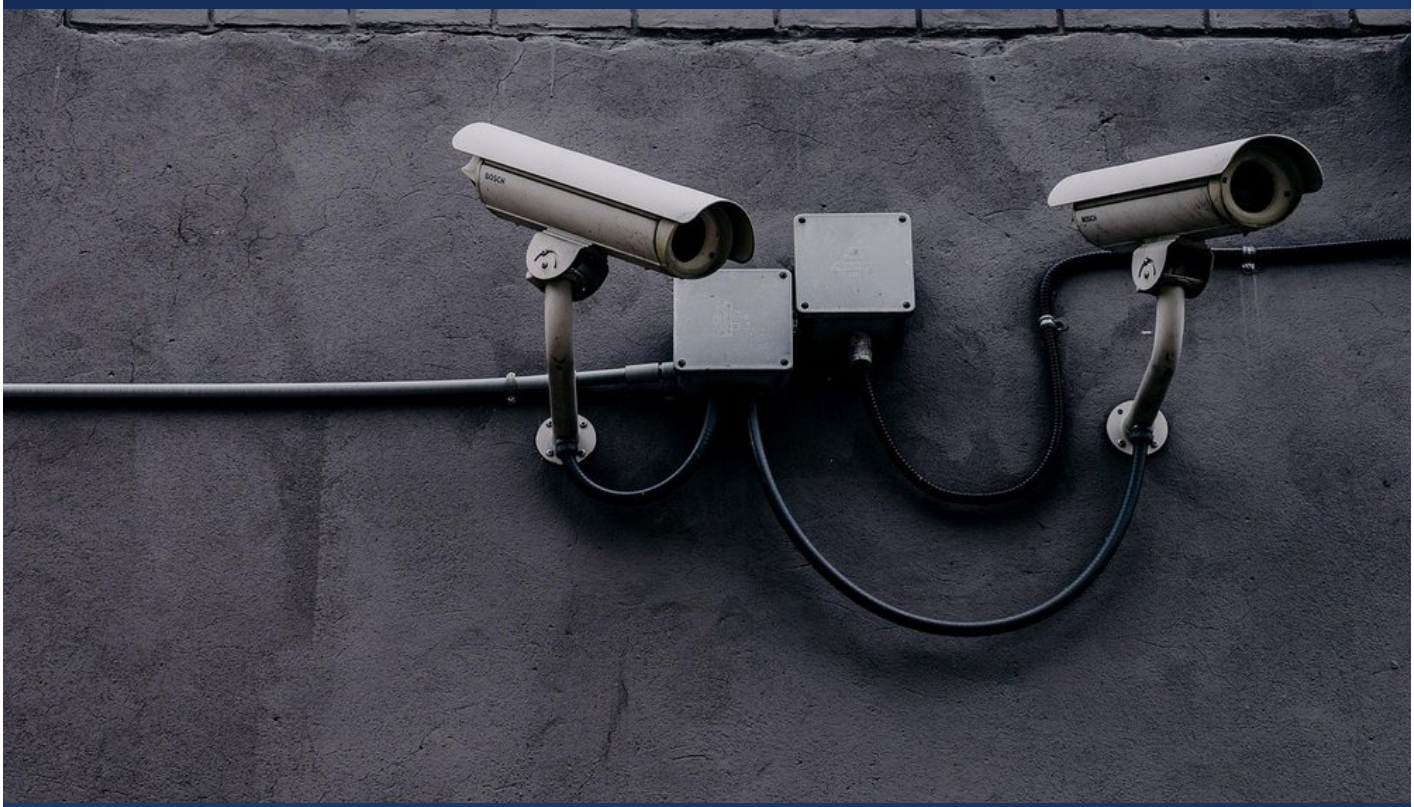
LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27402 — IoT Device Baseline Security Requirements

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-27402 • 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-27402**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Incident Response Strategies

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

- **1 Understanding Incident Response Frameworks in IoT** — 6 classes
  - 1.1 Define the Key Components of an Incident Response Framework in IoT
  - 1.2 Identify Common Security Incidents Affecting IoT Devices
  - 1.3 Explore the Phases of Incident Response Specific to IoT
  - 1.4 Analyze Case Studies of IoT Incident Responses
  - 1.5 Develop a Customized Incident Response Plan for IoT Devices
  - 1.6 Evaluate the Effectiveness of Incident Response Strategies in IoT
- **2 Identifying and Classifying IoT Security Incidents** — 6 classes
  - 2.1 Define IoT Security Incidents and Their Impact
  - 2.2 Recognize Common Types of IoT Security Incidents
  - 2.3 Analyze Real-World Case Studies of IoT Incidents
  - 2.4 Utilize Frameworks to Classify IoT Security Incidents
  - 2.5 Develop Criteria for Prioritizing Incident Response
  - 2.6 Apply Classification Strategies to Simulated IoT Scenarios
- **3 Developing an IoT Incident Response Plan** — 6 classes
  - 3.1 Define the Key Components of an IoT Incident Response Plan
  - 3.2 Identify Roles and Responsibilities in Incident Response Teams
  - 3.3 Assess Risks and Prioritize IoT Threat Scenarios
  - 3.4 Develop Effective Detection and Monitoring Strategies for IoT Incidents
  - 3.5 Create a Communication Plan for Stakeholders During an Incident
  - 3.6 Evaluate and Test the IoT Incident Response Plan Through Simulations
- **4 Executing Incident Response Procedures for IoT Devices** — 6 classes
  - 4.1 Identify IoT Device Vulnerabilities in Incident Response
  - 4.2 Develop an Incident Response Plan for IoT Devices
  - 4.3 Implement Detection Techniques for IoT Security Incidents
  - 4.4 Execute Containment Strategies for IoT Incidents
  - 4.5 Conduct Post-Incident Analysis and Review for IoT Devices
  - 4.6 Communicate Incident Response Outcomes to Stakeholders
- **5 Post-Incident Analysis and Continuous Improvement in IoT** — 6 classes
  - 5.1 Analyze Post-Incident Reports to Identify Root Causes
  - 5.2 Evaluate Incident Response Effectiveness and Gaps
  - 5.3 Engage Stakeholders in Lessons Learned Discussions
  - 5.4 Develop Actionable Recommendations for Future Incidents
  - 5.5 Implement Changes to Improve IoT Device Security Protocols
  - 5.6 Create a Continuous Improvement Framework for Incident Response

2 Introduction to IoT Security

5 chapters · 30 classes **85 marks**

- **1 Understanding IoT and Its Security Implications** — 6 classes
  - 1.1 Define the Internet of Things and Its Components
  - 1.2 Explore Common Security Threats in IoT Environments
  - 1.3 Identify Key Security Standards for IoT Devices
  - 1.4 Analyze Real-World IoT Security Breaches
  - 1.5 Assess Risk Management Strategies for IoT Deployments
  - 1.6 Develop an Action Plan for Enhancing IoT Device Security
- **2 Core Principles of IoT Security Frameworks** — 6 classes
  - 2.1 Define Key IoT Security Concepts
  - 2.2 Identify Common Threats to IoT Devices
  - 2.3 Explore the Importance of Security Frameworks
  - 2.4 Analyze ISO 27402 Security Requirements
  - 2.5 Evaluate Risk Management Practices for IoT
  - 2.6 Develop a Basic IoT Security Strategy
- **3 Evaluating Security Risks in IoT Deployments** — 6 classes
  - 3.1 Identify Common Security Risks in IoT Devices
  - 3.2 Assess Vulnerabilities in IoT Infrastructure
  - 3.3 Analyze Threat Models for IoT Environments
  - 3.4 Evaluate the Impact of Security Breaches on IoT Systems
  - 3.5 Prioritize Risks and Develop Mitigation Strategies
  - 3.6 Apply Best Practices for Continuous Security Assessment in IoT
- **4 Implementing Baseline Security Requirements for IoT Devices** — 6 classes
  - 4.1 Identify the Key Baseline Security Requirements for IoT Devices
  - 4.2 Assess the Current Security Posture of IoT Devices
  - 4.3 Develop a Risk Management Framework for IoT Security
  - 4.4 Implement Access Control Measures for IoT Devices
  - 4.5 Establish Data Protection Strategies for IoT Systems
  - 4.6 Evaluate the Effectiveness of Implemented Security Controls in IoT Devices
- **5 Future Trends and Challenges in IoT Security** — 6 classes
  - 5.1 Analyze Emerging Trends in IoT Security
  - 5.2 Identify Key Challenges Facing IoT Security Today
  - 5.3 Examine Case Studies on Recent IoT Security Breaches
  - 5.4 Evaluate Future Technologies Impacting IoT Security
  - 5.5 Develop Strategic Solutions for IoT Security Challenges
  - 5.6 Propose Best Practices for Securing Future IoT Devices

3 ISO 27402 Framework Analysis

5 chapters · 30 classes **85 marks**

- **1 Understanding ISO 27402: Objectives and Scope** — 6 classes
  - 1.1 Analyze the Objectives of ISO 27402
  - 1.2 Identify Key Components of the ISO 27402 Framework
  - 1.3 Explore the Importance of IoT Device Security
  - 1.4 Examine the Scope and Applicability of ISO 27402
  - 1.5 Evaluate Compliance Requirements for Leadership
  - 1.6 Apply ISO 27402 Principles to Real-world Scenarios
- **2 Core Principles of IoT Security Frameworks** — 6 classes
  - 2.1 Identify Key Components of IoT Security Frameworks
  - 2.2 Analyze Risks Associated with IoT Devices
  - 2.3 Distinguish Between Security Levels in IoT Frameworks
  - 2.4 Evaluate the Impact of Security Breaches on IoT Systems
  - 2.5 Apply Core Principles to Develop a Security Strategy
  - 2.6 Recommend Best Practices for Implementing ISO 27402
- **3 Identifying Security Requirements for IoT Devices** — 6 classes
  - 3.1 Analyze Current IoT Security Landscape
  - 3.2 Identify Key Components of ISO 27402 Standards
  - 3.3 Conduct a Risk Assessment for IoT Devices
  - 3.4 Define Security Requirements Based on Risk Analysis
  - 3.5 Evaluate Existing IoT Devices Against ISO Standards
  - 3.6 Develop an Action Plan for Implementing Security Requirements
- **4 Implementation Strategies for Compliance** — 6 classes
  - 4.1 Assess Current Compliance Status Against ISO 27402
  - 4.2 Identify Key Stakeholders for Implementation Strategy
  - 4.3 Develop a Risk Assessment Framework for IoT Devices
  - 4.4 Create an Action Plan for Addressing Compliance Gaps
  - 4.5 Monitor and Evaluate Implementation Progress Regularly
  - 4.6 Communicate Compliance Strategies to All Stakeholders
- **5 Evaluating and Maintaining Security Standards** — 6 classes
  - 5.1 Analyze Current Security Standards Against ISO 27402
  - 5.2 Identify Gaps in IoT Device Security Compliance
  - 5.3 Implement Effective Assessment Tools for Security Evaluation
  - 5.4 Develop a Structured Plan for Security Maintenance
  - 5.5 Review Case Studies of Security Standard Failures
  - 5.6 Create an Actionable Security Improvement Checklist

4 Leadership and Communication in Security

5 chapters · 30 classes **65 marks**

- **1 Understanding Leadership Styles in IoT Security** — 6 classes
  - 1.1 Explore Leadership Theories Relevant to IoT Security
  - 1.2 Assess the Impact of Different Leadership Styles on Team Dynamics
  - 1.3 Identify Effective Communication Strategies for Security Leadership
  - 1.4 Analyze Case Studies of Leadership in IoT Security Breaches
  - 1.5 Develop a Personal Leadership Philosophy for IoT Security
  - 1.6 Implement Leadership Strategies to Enhance IoT Security Communications
- **2 Effective Communication Strategies for Security Leadership** — 6 classes
  - 2.1 Define Key Communication Principles for Security Leadership
  - 2.2 Identify Stakeholder Communication Needs in Security Contexts
  - 2.3 Develop Clear Messaging for Cybersecurity Strategies
  - 2.4 Facilitate Active Listening Techniques for Leadership
  - 2.5 Practice Crisis Communication Scenarios in Security Operations
  - 2.6 Evaluate the Impact of Communication on Security Team Effectiveness
- **3 Building a Security-focused Team Culture** — 6 classes
  - 3.1 Define Core Values for a Security-focused Team
  - 3.2 Communicate Security Objectives Clearly to Your Team
  - 3.3 Foster Open Communication and Feedback about Security Practices
  - 3.4 Encourage Team Collaboration on Security Challenges
  - 3.5 Recognize and Reward Security-focused Behaviors
  - 3.6 Develop a Continuous Improvement Plan for Security Awareness
- **4 Risk Management and Decision-Making in IoT Security** — 6 classes
  - 4.1 Identify Key Risks in IoT Security Framework
  - 4.2 Analyze Risk Impacts on IoT Devices and Systems
  - 4.3 Develop Risk Mitigation Strategies for IoT Environments
  - 4.4 Evaluate Decision-Making Models in IoT Security Context
  - 4.5 Create a Risk Management Plan for IoT Device Implementation
  - 4.6 Communicate and Present IoT Security Risks to Stakeholders
- **5 Engaging Stakeholders for Effective Security Governance** — 6 classes
  - 5.1 Identify Key Stakeholders in Security Governance
  - 5.2 Analyze Stakeholder Needs and Expectations
  - 5.3 Develop Effective Communication Strategies for Security Initiatives
  - 5.4 Foster Collaboration Among Stakeholders for Enhanced Security Outcomes
  - 5.5 Evaluate Stakeholder Engagement Techniques and Their Impact
  - 5.6 Implement Continuous Feedback Mechanisms for Security Governance

5 Risk Management in IoT

5 chapters · 30 classes **65 marks**

- **1 Understanding IoT Ecosystems and their Vulnerabilities** — 6 classes
  - 1.1 Identify Key Components of IoT Ecosystems
  - 1.2 Analyze Common Vulnerabilities in IoT Devices
  - 1.3 Explore Threats to IoT Data Integrity and Privacy
  - 1.4 Assess the Impact of Vulnerabilities on Stakeholders
  - 1.5 Develop Strategies for Mitigating IoT Risks
  - 1.6 Create a Security Action Plan for an IoT Ecosystem
- **2 Fundamentals of Risk Management in IoT** — 6 classes
  - 2.1 Understand Key Terms in IoT Risk Management
  - 2.2 Identify Potential Risks Associated with IoT Devices
  - 2.3 Analyze the Impact of Risks on IoT Operations
  - 2.4 Evaluate Current Security Frameworks for IoT Risk Management
  - 2.5 Develop Mitigation Strategies for Identified IoT Risks
  - 2.6 Implement a Risk Assessment Process for IoT Projects
- **3 Implementing Security Controls in IoT Deployments** — 6 classes
  - 3.1 Identify Key Security Controls for IoT Deployments
  - 3.2 Assess Risk Factors Unique to IoT Devices
  - 3.3 Implement Authentication Mechanisms in IoT Systems
  - 3.4 Apply Data Encryption Techniques for IoT Security
  - 3.5 Monitor and Respond to Security Incidents in IoT Networks
  - 3.6 Evaluate the Effectiveness of Security Controls in IoT
- **4 Compliance and Regulatory Frameworks for IoT Security** — 6 classes
  - 4.1 Identify Key Compliance Standards for IoT Security
  - 4.2 Analyze the Role of ISO 27402 in IoT Risk Management
  - 4.3 Evaluate Regulatory Requirements Impacting IoT Devices
  - 4.4 Explore Regional Variations in IoT Security Compliance
  - 4.5 Develop a Compliance Checklist for IoT Implementations
  - 4.6 Create an Action Plan for Continuous Compliance Monitoring
- **5 Incident Response and Recovery in IoT Environments** — 6 classes
  - 5.1 Identify Key Components of Incident Response in IoT
  - 5.2 Assess Risks Associated with IoT Incidents
  - 5.3 Develop an Incident Response Plan for IoT Devices
  - 5.4 Implement Detection and Analysis Strategies for IoT Incidents
  - 5.5 Execute Response and Mitigation Procedures in IoT Environments
  - 5.6 Review and Update Recovery Strategies Post-Incident in IoT

6 Security Policy Development

5 chapters · 30 classes **65 marks**

- **1 Understanding IoT Security and ISO 27402 Framework** — 6 classes
  - 1.1 Analyze the Importance of IoT Security in Today's Digital Landscape
  - 1.2 Identify Key Components of the ISO 27402 Framework
  - 1.3 Examine Risk Management Strategies for IoT Devices
  - 1.4 Develop Guidelines for Establishing IoT Security Policies
  - 1.5 Evaluate Implementation Challenges of ISO 27402 in Organizations
  - 1.6 Create an Action Plan for Compliance with ISO 27402 Standards
- **2 Identifying Security Threats and Vulnerabilities in IoT Devices** — 6 classes
  - 2.1 Define IoT Security Threats and Vulnerabilities
  - 2.2 Analyze Common IoT Device Attack Vectors
  - 2.3 Explore Real-World IoT Security Breaches
  - 2.4 Assess the Impact of Vulnerabilities on Device Functionality
  - 2.5 Identify Risk Assessment Techniques for IoT Devices
  - 2.6 Develop a Mitigation Strategy for IoT Security Threats
- **3 Developing Comprehensive Security Policies for IoT** — 6 classes
  - 3.1 Identify Core Components of IoT Device Security Policies
  - 3.2 Analyze Risks and Threats in IoT Environments
  - 3.3 Establish Framework for Security Policy Development
  - 3.4 Integrate Stakeholder Input into Security Policy Creation
  - 3.5 Develop Guidelines for Compliance with ISO 27402 Standards
  - 3.6 Evaluate and Revise Security Policies for Continuous Improvement
- **4 Implementing and Enforcing IoT Security Policies** — 6 classes
  - 4.1 Identify Key IoT Security Policy Objectives
  - 4.2 Assess Current IoT Security Vulnerabilities
  - 4.3 Develop Comprehensive IoT Security Policies
  - 4.4 Communicate Policies to Key Stakeholders
  - 4.5 Monitor and Enforce IoT Security Policies
  - 4.6 Review and Update IoT Security Policies Regularly
- **5 Monitoring and Updating Security Policies for IoT Sustainability** — 6 classes
  - 5.1 Identify Key Metrics for Monitoring IoT Security Policies
  - 5.2 Analyze Existing IoT Security Policies for Gaps
  - 5.3 Develop a Framework for Regular Security Policy Review
  - 5.4 Implement Strategies for Real-Time Security Incident Monitoring
  - 5.5 Evaluate the Effectiveness of Security Policy Updates
  - 5.6 Communicate Policy Changes to Stakeholders Effectively