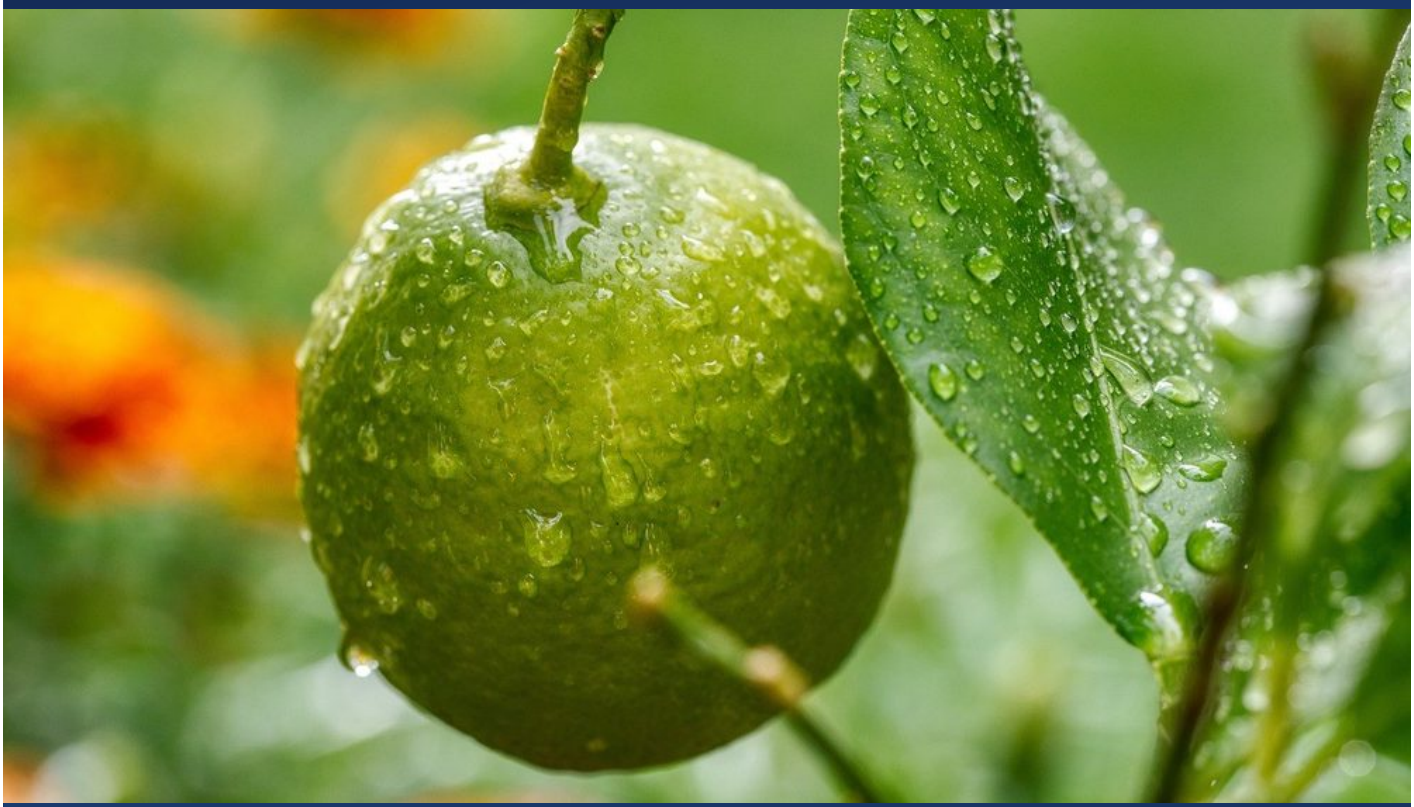
LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

# ISO 27034SFT — Application Security

*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-SFT-27034SFT • ISO IT & Related Technologies


UKPRN 10067351 • Registered in England and Wales, company 4984798

| 6 | 20 | 120 | 430 | 60% | Lifetime |
|---|---|---|---|---|---|
| SUBJECTS | CHAPTERS | CLASSES | TOTAL MARKS | PASS MARK | VALIDITY |

## AT A GLANCE

| | |
|---|---|
| REFERENCE | **IIT-SFT-27034SFT** |
| AWARD | **Certificate** |
| ASSESSMENT | **430 marks — 258 to pass (60%)** |
| PREREQUISITES | **None** |
| VALIDITY | **Lifetime** |
| AWARDING BODY | **LAPT — London Academy of Professional Training** |

## CURRICULUM

### 1 Application Security Fundamentals

5 chapters · 30 classes · **85 marks**

- **1 Understanding Application Security Principles** — 6 classes
  - 1.1 Identify Key Application Security Principles
  - 1.2 Analyze Common Application Vulnerabilities
  - 1.3 Evaluate the Role of Threat Modeling in Security
  - 1.4 Apply Secure Coding Practices in Development
  - 1.5 Assess the Importance of Security Testing Methods
  - 1.6 Develop Security Awareness for Application Users
- **2 Threat Modeling and Risk Assessment** — 6 classes
  - 2.1 Identify Threats in Application Security
  - 2.2 Analyze Vulnerabilities in Software Environments
  - 2.3 Assess Impact and Likelihood of Threats
  - 2.4 Develop Risk Mitigation Strategies
  - 2.5 Create a Threat Model for Real-World Applications
  - 2.6 Review and Update Risk Assessment Practices
- **3 Secure Software Development Lifecycle (SDLC)** — 6 classes
  - 3.1 Define the Secure Software Development Lifecycle (SDLC) Model
  - 3.2 Identify Key Phases in the Secure SDLC Process
  - 3.3 Analyze Security Requirements During the Planning Phase
  - 3.4 Implement Security Best Practices in Design and Development
  - 3.5 Conduct Security Testing and Vulnerability Assessments
  - 3.6 Establish Continuous Improvement Strategies for SDLC Security
- **4 Application Security Testing Techniques** — 6 classes
  - 4.1 Identify Key Application Security Testing Techniques
  - 4.2 Explore Static Application Security Testing (SAST) Methods
  - 4.3 Implement Dynamic Application Security Testing (DAST) Practices
  - 4.4 Analyze the Role of Interactive Application Security Testing (IAST)
  - 4.5 Evaluate Security Testing Tools and Frameworks
  - 4.6 Develop a Comprehensive Application Security Testing Strategy
- **5 Implementing Security Controls and Best Practices** — 6 classes
  - 5.1 Identify and Assess Security Risks in Applications
  - 5.2 Implement Security Frameworks for Application Development
  - 5.3 Establish Security Controls for Data Protection
  - 5.4 Monitor and Test Application Security Posture
  - 5.5 Develop Best Practices for Secure Coding
  - 5.6 Create an Incident Response Plan for Application Vulnerabilities

## 2 Designing Secure Applications

5 chapters · 30 classes **65 marks**

- **1 Understanding Application Security Concepts and Frameworks** — 6 classes
  - 1.1 Define Key Application Security Terms and Concepts
  - 1.2 Explore Common Security Threats in Software Development
  - 1.3 Analyze Security Frameworks Relevant to Application Security
  - 1.4 Identify the Components of a Secure Application Design
  - 1.5 Evaluate Security Standards and Compliance Requirements
  - 1.6 Implement Best Practices for Secure Application Development
- **2 Identifying Threats and Vulnerabilities in Applications** — 6 classes
  - 2.1 Analyze Common Application Threats
  - 2.2 Identify Vulnerability Types in Software
  - 2.3 Assess the Impact of Security Breaches
  - 2.4 Evaluate Risk Assessment Methodologies
  - 2.5 Explore Real-World Application Vulnerability Case Studies
  - 2.6 Implement Strategies for Threat Mitigation
- **3 Secure Software Development Lifecycle (SDLC) Practices** — 6 classes
  - 3.1 Identify Key Phases of the Secure SDLC
  - 3.2 Analyze Security Requirements in Software Design
  - 3.3 Implement Threat Modeling Techniques
  - 3.4 Integrate Security Testing Methods in Development
  - 3.5 Establish Secure Code Review Practices
  - 3.6 Develop a Continuous Improvement Plan for Security
- **4 Implementing Security Controls and Countermeasures** — 6 classes
  - 4.1 Identify Key Security Vulnerabilities in Application Design
  - 4.2 Assess Threat Models for Your Application Environment
  - 4.3 Implement Authentication Mechanisms to Enhance Security
  - 4.4 Apply Data Protection Techniques for Sensitive Information
  - 4.5 Integrate Logging and Monitoring Features for Incident Response
  - 4.6 Evaluate and Optimize Security Controls in Application Lifecycle
- **5 Conducting Security Testing and Assessment for Applications** — 6 classes
  - 5.1 Identify Application Security Requirements
  - 5.2 Explore Common Security Testing Methods
  - 5.3 Develop a Security Testing Plan
  - 5.4 Conduct Static Application Security Testing
  - 5.5 Execute Dynamic Application Security Testing
  - 5.6 Analyze and Report Security Testing Results

## 3 ISO 27034 Compliance

5 chapters · 30 classes **65 marks**

- **1 Understanding ISO 27034: Framework and Objectives** — 6 classes
  - 1.1 Define the Key Concepts of ISO 27034
  - 1.2 Identify the Core Objectives of ISO 27034 Framework
  - 1.3 Explore the Structure of ISO 27034 Compliance Guidelines
  - 1.4 Analyze the Importance of Application Security in ISO 27034
  - 1.5 Discuss the Roles and Responsibilities in ISO 27034 Compliance
  - 1.6 Implement Best Practices for Adhering to ISO 27034 Standards
- **2 Risk Management and Assessment in Application Security** — 6 classes
  - 2.1 Identify Key Risks in Application Security
  - 2.2 Analyze Threat Vectors in Application Environments
  - 2.3 Assess Vulnerabilities in Software Development Life Cycle
  - 2.4 Implement Risk Mitigation Strategies for Applications
  - 2.5 Monitor and Review Risk Management Processes
  - 2.6 Prepare for Compliance Audits in Application Security
- **3 Integrating Security Controls into the Software Development Lifecycle** — 6 classes
  - 3.1 Analyze the Importance of Security in the Software Development Lifecycle
  - 3.2 Identify Key Security Controls for Development Phases
  - 3.3 Implement Security Requirements in Design Specifications
  - 3.4 Integrate Security Testing into Development Processes
  - 3.5 Evaluate Security Outcomes and Remediation Strategies
  - 3.6 Communicate Security Practices to Development Teams Effectively
- **4 Testing and Validation of Application Security Measures** — 6 classes
  - 4.1 Assess Current Application Security Measures
  - 4.2 Identify Key Testing Methodologies for Application Security
  - 4.3 Develop a Validation Strategy for Security Controls
  - 4.4 Execute Penetration Testing Procedures
  - 4.5 Analyze Testing Results and Interpret Findings
  - 4.6 Implement Continuous Improvement Based on Validation Feedback
- **5 Continuous Improvement and Compliance Monitoring** — 6 classes
  - 5.1 Analyze Current Compliance Status Against ISO 27034 Standards
  - 5.2 Identify Gaps in Application Security Compliance
  - 5.3 Develop Continuous Improvement Strategies for Compliance Monitoring
  - 5.4 Implement Automated Tools for Compliance Tracking
  - 5.5 Review and Revise Policies Based on Compliance Monitoring Feedback
  - 5.6 Evaluate the Effectiveness of Continuous Improvement Initiatives

## 4 Leadership and Management in Application Security

0 chapters **65 marks**

## 5 Practical Application Security Tests

0 chapters **65 marks**

## 6 Risk Assessment and Management

5 chapters · 30 classes **85 marks**

- **1 Fundamentals of Risk Assessment in Application Security** — 6 classes
  - 1.1 Define Key Concepts in Risk Assessment for Application Security
  - 1.2 Identify Common Risks Associated with Applications
  - 1.3 Analyze the Impact of Application Vulnerabilities
  - 1.4 Evaluate Risk Assessment Methodologies in Application Security
  - 1.5 Develop a Risk Management Plan for Application Security
  - 1.6 Implement Risk Mitigation Strategies in Application Development
- **2 Identifying Risks in Software Applications** — 6 classes
  - 2.1 Define Key Concepts of Risk in Software Applications
  - 2.2 Identify Common Threats in Software Development
  - 2.3 Analyze Vulnerabilities in Existing Software Solutions
  - 2.4 Assess the Impact of Identified Risks
  - 2.5 Prioritize Risks Based on Likelihood and Impact
  - 2.6 Develop Mitigation Strategies for High-Priority Risks
- **3 Analyzing and Prioritizing Risks** — 6 classes
  - 3.1 Identify Critical Assets for Risk Assessment
  - 3.2 Conduct a Preliminary Risk Analysis
  - 3.3 Evaluate Potential Threats and Vulnerabilities
  - 3.4 Assess the Impact and Likelihood of Risks
  - 3.5 Prioritize Risks for Effective Management
  - 3.6 Develop a Risk Mitigation Strategy
- **4 Mitigating Risks through Security Controls** — 6 classes
  - 4.1 Identify Key Risks in Application Security
  - 4.2 Analyze Vulnerabilities and Threats
  - 4.3 Evaluate the Effectiveness of Current Security Controls
  - 4.4 Prioritize Risks Based on Impact and Likelihood
  - 4.5 Develop Mitigation Strategies for Critical Risks
  - 4.6 Implement and Monitor Security Controls for Continuous Improvement
- **5 Monitoring and Reviewing Risk Management Practices** — 6 classes
  - 5.1 Analyze Current Risk Management Practices
  - 5.2 Identify Key Performance Indicators for Risk Assessment
  - 5.3 Evaluate Effectiveness of Monitoring Tools and Techniques
  - 5.4 Conduct a Risk Management Review Meeting
  - 5.5 Develop Action Plans for Risk Mitigation Strategies
  - 5.6 Report Findings and Recommendations for Continuous Improvement