

# LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

## ISO 27005RSK — Information Security Risk Management

*ISO Certification Programme*



---

### LAPT — London Academy of Professional Training

**Address** 85 Great Portland Street, W1W 7LT, London, United Kingdom

**Email** [info@lapt.org](mailto:info@lapt.org)

**Telephone** +44 7513 283044

**Web** [lapt.org](http://lapt.org)

**Reference** SSR-RSK-27005RSK • ISO Security Safety & Risk

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

|               |                                                |
|---------------|------------------------------------------------|
| REFERENCE     | SSR-RSK-27005RSK                               |
| AWARD         | Certificate                                    |
| ASSESSMENT    | 430 marks — 258 to pass (60%)                  |
| PREREQUISITES | None                                           |
| VALIDITY      | Lifetime                                       |
| AWARDING BODY | LAPT — London Academy of Professional Training |

CURRICULUM

1

Governance and Compliance

5 chapters · 30 classes 65 marks

• 1 Fundamentals of Governance in Information Security — 6 classes

› 1.1 Define Key Principles of Governance in Information Security

› 1.2 Explore Regulatory Frameworks Impacting Information Security

› 1.3 Analyze Roles and Responsibilities in Information Security Governance

› 1.4 Identify Best Practices for Developing an Information Security Policy

› 1.5 Evaluate Risk Management Strategies in Information Security Governance

› 1.6 Implement Governance Frameworks for Effective Information Security Compliance

• 2 Legal and Regulatory Frameworks for Compliance — 6 classes

› 2.1 Identify Key Legal Frameworks Impacting Information Security

› 2.2 Analyze UK GDPR Requirements for Data Protection Compliance

› 2.3 Examine the Role of the Data Protection Act in Risk Management

› 2.4 Evaluate the Implications of the Freedom of Information Act

› 2.5 Assess Compliance Strategies for Sector-Specific Regulations

› 2.6 Develop a Risk Mitigation Action Plan Based on Legal Compliance

• 3 Establishing an Information Security Governance Structure — 6 classes

› 3.1 Define Key Components of Information Security Governance

› 3.2 Identify Stakeholders and Their Roles in Governance Structure

› 3.3 Develop Policies and Procedures for Information Security

› 3.4 Establish Communication Channels for Governance Oversight

› 3.5 Implement a Risk Management Framework within Governance

› 3.6 Evaluate and Adapt the Governance Structure for Continuous Improvement

• 4 Risk Assessment and Management Strategies — 6 classes

› 4.1 Identify Key Components of Risk Assessment

› 4.2 Analyze Potential Risks in Information Security

› 4.3 Evaluate Risk Management Frameworks and Methodologies

› 4.4 Develop Risk Mitigation Strategies for Identified Risks

› 4.5 Implement Monitoring and Review Processes for Risk Management

› 4.6 Communicate Risk Management Plans to Stakeholders

• 5 Continuous Improvement and Assurance in Governance — 6 classes

› 5.1 Evaluate Current Governance Frameworks for Improvement Opportunities

› 5.2 Analyze Compliance Gaps Using Risk Assessment Techniques

› 5.3 Implement Feedback Loops for Continuous Improvement

› 5.4 Develop Key Performance Indicators for Governance Effectiveness

› 5.5 Foster a Culture of Continuous Improvement in Governance Practices

› 5.6 Create an Assurance Plan to Monitor Governance Enhancements

### • 1 Fundamentals of Risk Management Leadership — 6 classes

- › 1.1 Define Key Concepts in Risk Management Leadership
- › 1.2 Identify Roles and Responsibilities in Risk Management Teams
- › 1.3 Analyze the Importance of Stakeholder Engagement in Risk Management
- › 1.4 Evaluate Frameworks for Effective Risk Management Leadership
- › 1.5 Develop Strategies for Communicating Risk to Leadership
- › 1.6 Apply Risk Management Leadership Skills in Real-World Scenarios

### • 2 Establishing a Risk Management Culture — 6 classes

- › 2.1 Define the Importance of a Risk Management Culture
- › 2.2 Identify Key Elements of an Effective Risk Culture
- › 2.3 Assess Current Organizational Risk Attitudes
- › 2.4 Develop Strategies to Promote Risk Awareness
- › 2.5 Implement Communication Channels for Risk Management
- › 2.6 Evaluate and Sustain Risk Management Practices

### • 3 Stakeholder Engagement and Communication in Risk Management — 6 classes

- › 3.1 Identify Key Stakeholders in Risk Management
- › 3.2 Analyze Stakeholder Interests and Influence
- › 3.3 Develop Effective Communication Strategies for Stakeholders
- › 3.4 Engage Stakeholders through Active Listening Techniques
- › 3.5 Implement Continuous Feedback Loops with Stakeholders
- › 3.6 Evaluate the Impact of Stakeholder Engagement on Risk Outcomes

### • 4 Developing and Implementing a Risk Management Strategy — 6 classes

- › 4.1 Define Key Components of a Risk Management Strategy
- › 4.2 Analyze Organizational Context for Risk Management Implementation
- › 4.3 Identify Stakeholders and Their Roles in Risk Management
- › 4.4 Develop Risk Assessment Methodologies for Effective Strategy
- › 4.5 Create a Communication Plan for Risk Management Strategies
- › 4.6 Evaluate and Adjust the Risk Management Strategy for Continuous Improvement

### • 5 Evaluating and Improving Risk Management Practices — 6 classes

- › 5.1 Assess Current Risk Management Practices
- › 5.2 Identify Gaps in Risk Management Protocols
- › 5.3 Analyze Stakeholder Feedback on Risk Management
- › 5.4 Develop Strategies for Risk Management Improvement
- › 5.5 Implement Changes to Enhance Risk Management Effectiveness
- › 5.6 Measure and Evaluate the Impact of Risk Management Enhancements

### • 1 Introduction to Information Security Risk Management — 6 classes

- › 1.1 Define Key Concepts in Information Security Risk Management
- › 1.2 Identify Sources of Information Security Risks
- › 1.3 Analyze the Impact of Risks on Organizational Assets
- › 1.4 Evaluate Existing Risk Management Frameworks
- › 1.5 Map Risk Scenarios to Potential Threats and Vulnerabilities
- › 1.6 Develop a Risk Identification Plan for Your Organization

### • 2 Frameworks and Standards for Risk Identification — 6 classes

- › 2.1 Explore Key Frameworks for Risk Identification
- › 2.2 Analyze ISO 27005 Standards and Their Importance
- › 2.3 Compare Risk Assessment Models in Different Industries
- › 2.4 Identify Stakeholders in the Risk Management Process
- › 2.5 Apply Risk Identification Techniques Using Case Studies
- › 2.6 Evaluate Framework Effectiveness in Organizational Contexts

### • 3 Techniques for Risk Identification — 6 classes

- › 3.1 Explore Qualitative Risk Identification Techniques
- › 3.2 Apply Quantitative Risk Assessment Methods
- › 3.3 Evaluate Common Threat Sources and Vulnerabilities
- › 3.4 Utilize Risk Assessment Tools and Software
- › 3.5 Engage Stakeholders in the Risk Identification Process
- › 3.6 Develop a Comprehensive Risk Identification Report

### • 4 Risk Assessment Methodologies — 6 classes

- › 4.1 Explore Risk Assessment Frameworks and Their Importance
- › 4.2 Identify Key Components of Risk Assessment Methodologies
- › 4.3 Differentiate Between Qualitative and Quantitative Risk Assessment Techniques
- › 4.4 Apply Risk Assessment Tools to Real-World Scenarios
- › 4.5 Evaluate the Effectiveness of Various Risk Assessment Methodologies
- › 4.6 Develop a Custom Risk Assessment Plan for Your Organization

### • 5 Documentation and Reporting of Risk Assessment Findings — 6 classes

- › 5.1 Analyze Existing Risk Assessment Documentation
- › 5.2 Identify Key Components of Risk Reporting
- › 5.3 Create Effective Risk Assessment Templates
- › 5.4 Draft Comprehensive Risk Assessment Findings
- › 5.5 Integrate Stakeholder Feedback into Reporting
- › 5.6 Present Risk Assessment Findings to Leadership

**• 1 Understanding the Importance of Risk Monitoring** — 6 classes

- › 1.1 Define Key Concepts in Risk Monitoring
- › 1.2 Identify the Role of Risk Monitoring in ISO 27005
- › 1.3 Explore Methods for Effective Risk Monitoring
- › 1.4 Analyze Real-World Examples of Risk Monitoring Success
- › 1.5 Assess Tools and Technologies for Risk Monitoring
- › 1.6 Develop a Personal Action Plan for Enhancing Risk Monitoring Skills

**• 2 Key Principles of Risk Monitoring Frameworks** — 6 classes

- › 2.1 Define Key Components of Risk Monitoring Frameworks
- › 2.2 Identify Stakeholders Involved in Risk Monitoring
- › 2.3 Analyze Effective Tools for Risk Tracking
- › 2.4 Develop Performance Indicators for Risk Assessment
- › 2.5 Implement Continuous Improvement in Risk Review Processes
- › 2.6 Conduct a Case Study on Real-World Risk Monitoring Practices

**• 3 Techniques for Effective Risk Identification and Assessment** — 6 classes

- › 3.1 Explore Common Risk Identification Techniques
- › 3.2 Apply SWOT Analysis for Risk Assessment
- › 3.3 Conduct a Risk Brainstorming Session
- › 3.4 Utilize Risk Assessment Tools and Software
- › 3.5 Develop Risk Scenarios for Evaluation
- › 3.6 Review and Revise Risk Assessment Processes

**• 4 Implementing Continuous Risk Review Processes** — 6 classes

- › 4.1 Identify Key Risk Indicators for Continuous Monitoring
- › 4.2 Develop a Framework for Risk Review Processes
- › 4.3 Establish Roles and Responsibilities in Risk Management
- › 4.4 Implement Tools and Techniques for Risk Tracking
- › 4.5 Conduct Regular Risk Assessment Meetings
- › 4.6 Review and Update Risk Management Strategies Effectively

**• 5 Metrics and Reporting for Risk Monitoring** — 6 classes

- › 5.1 Identify Key Metrics for Risk Monitoring
- › 5.2 Develop Quantitative Risk Rating Systems
- › 5.3 Implement Qualitative Assessment Techniques
- › 5.4 Create Effective Risk Reporting Dashboards
- › 5.5 Analyze Risk Data for Informed Decision Making
- › 5.6 Establish Continuous Improvement Feedback Loops

**• 1 Understanding Risk Treatment Strategies** — 6 classes

- › 1.1 Identify Key Risk Treatment Strategies
- › 1.2 Analyze the Impact of Treatment Options
- › 1.3 Evaluate Cost-Benefit of Risk Mitigation Approaches
- › 1.4 Develop a Comprehensive Risk Treatment Plan
- › 1.5 Implement Effective Monitoring and Review Techniques
- › 1.6 Communicate Risk Treatment Strategies to Stakeholders

**• 2 Developing Risk Treatment Plans** — 6 classes

- › 2.1 Identify Key Risk Areas for Treatment
- › 2.2 Analyze Current Risk Mitigation Strategies
- › 2.3 Define SMART Objectives for Risk Treatment Plans
- › 2.4 Evaluate Treatment Options for Identified Risks
- › 2.5 Create Implementation Roadmap for Risk Treatment
- › 2.6 Monitor and Review Effectiveness of Treatment Plans

**• 3 Implementing Risk Mitigation Measures** — 6 classes

- › 3.1 Identify Key Risk Mitigation Measures
- › 3.2 Evaluate the Effectiveness of Mitigation Strategies
- › 3.3 Develop a Risk Treatment Plan
- › 3.4 Assign Responsibilities for Risk Mitigation
- › 3.5 Monitor and Review Risk Mitigation Actions
- › 3.6 Communicate Mitigation Measures to Stakeholders

**• 4 Monitoring and Reviewing Risk Treatments** — 6 classes

- › 4.1 Identify Key Indicators for Monitoring Risk Treatments
- › 4.2 Evaluate the Effectiveness of Existing Risk Mitigation Strategies
- › 4.3 Implement Continuous Monitoring Techniques for Risk Management
- › 4.4 Analyze Data and Trends in Risk Treatment Outcomes
- › 4.5 Review and Revise Risk Treatment Plans Based on Findings
- › 4.6 Communicate Risk Treatment Review Results to Stakeholders

**• 5 Communication and Reporting in Risk Management** — 6 classes

- › 5.1 Identify Key Stakeholders for Effective Risk Communication
- › 5.2 Develop a Risk Communication Plan Tailored to Stakeholders
- › 5.3 Analyze and Select Appropriate Communication Channels for Risk Reporting
- › 5.4 Design Clear and Concise Risk Reports that Inform Decision-Making
- › 5.5 Implement Feedback Mechanisms to Enhance Risk Communication Effectiveness
- › 5.6 Evaluate and Improve Reporting Practices for Continuous Risk Management

**• 1 Understanding Strategic Risk Communication Frameworks — 6**

classes

- › 1.1 Define Key Concepts in Strategic Risk Communication
- › 1.2 Identify Components of Risk Communication Frameworks
- › 1.3 Analyze the Role of Stakeholders in Risk Communication
- › 1.4 Explore Various Risk Communication Models and Their Applications
- › 1.5 Evaluate the Effectiveness of Different Communication Strategies
- › 1.6 Develop a Strategic Risk Communication Plan

**• 2 Identifying Stakeholders and Communication Channels — 6**

classes

- › 2.1 Identify Key Stakeholders in Information Security Risk Management
- › 2.2 Analyze Stakeholder Needs and Expectations
- › 2.3 Map Communication Channels for Stakeholder Engagement
- › 2.4 Evaluate the Effectiveness of Current Communication Channels
- › 2.5 Develop Tailored Communication Strategies for Different Stakeholders
- › 2.6 Implement and Monitor Communication Plans for Stakeholder Alignment

**• 3 Crafting Effective Risk Messages — 6**

classes

- › 3.1 Identify Key Risk Concepts for Communication
- › 3.2 Analyze Audience Needs and Expectations
- › 3.3 Develop Clear and Concise Risk Messages
- › 3.4 Utilize Visual Aids to Enhance Risk Understanding
- › 3.5 Employ Storytelling Techniques for Effective Messaging
- › 3.6 Evaluate and Refine Risk Communication Strategies

**• 4 Crisis Communication and Risk Perception — 6**

classes

- › 4.1 Define Crisis Communication in Information Security
- › 4.2 Identify Key Elements of Risk Perception
- › 4.3 Analyze Case Studies of Effective Crisis Communication
- › 4.4 Assess Stakeholder Risk Perception During Crises
- › 4.5 Develop a Crisis Communication Strategy for Risk Management
- › 4.6 Evaluate the Impact of Crisis Communication on Stakeholder Trust

**• 5 Evaluating the Impact of Risk Communication Strategies — 6**

classes

- › 5.1 Identify Key Elements of Effective Risk Communication Strategies
- › 5.2 Analyze the Audience for Tailored Communication Approaches
- › 5.3 Evaluate Communication Channels for Maximum Impact
- › 5.4 Measure Success Metrics for Risk Communication Initiatives
- › 5.5 Assess Case Studies on Risk Communication Outcomes
- › 5.6 Develop a Strategic Plan for Future Risk Communication Efforts