

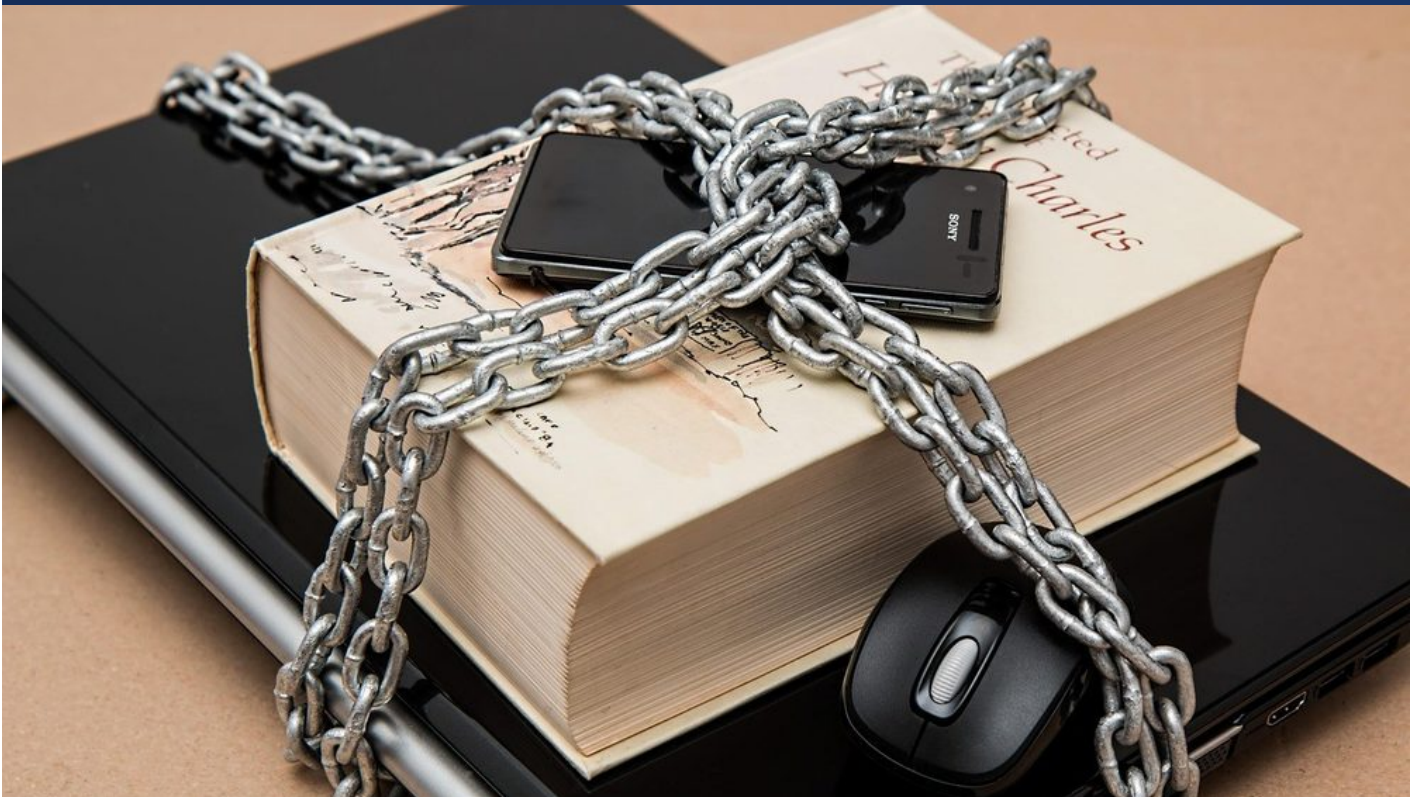
LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001ARS — Information Security in Aerospace

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 TR-ARS-27001ARS • ISO Transport

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	TR-ARS-27001ARS
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 Regulatory Requirements 5 chapters · 30 classes 45 marks	
• 1 Understanding ISO 27001: An Overview for Aerospace — 6 classes › 1.1 Identify the Key Components of ISO 27001 in Aerospace › 1.2 Explore the Importance of Information Security Management Systems (ISMS) › 1.3 Analyze Compliance Requirements for Aerospace Organizations › 1.4 Examine Risk Management Principles in ISO 27001 › 1.5 Discuss Roles and Responsibilities in Implementing ISO 27001 › 1.6 Apply ISO 27001 Principles to Develop a Security Action Plan • 2 Regulatory Frameworks in the Aerospace Industry — 6 classes › 2.1 Identify Key Regulatory Bodies in Aerospace Compliance › 2.2 Analyze International Standards for Aerospace Safety › 2.3 Evaluate National Regulations Impacting the Aerospace Industry › 2.4 Distinguish Between Mandatory and Voluntary Compliance Requirements › 2.5 Assess the Role of ISO Standards in Aerospace Regulatory Compliance › 2.6 Develop a Compliance Action Plan for Aerospace Organizations • 3 Risk Management Principles in Information Security — 6 classes › 3.1 Identify Key Risk Management Concepts in Information Security › 3.2 Analyze Regulatory Frameworks Influencing Risk Management › 3.3 Assess the Impact of Information Security Risks on Aerospace Operations › 3.4 Develop a Risk Assessment Methodology for ISO 27001 Compliance › 3.5 Formulate Risk Mitigation Strategies Tailored to Aerospace Security › 3.6 Evaluate the Effectiveness of Risk Management Practices in Information Security	• 4 Implementing Compliance Measures for ISO 27001 — 6 classes › 4.1 Identify Key Compliance Requirements for ISO 27001 › 4.2 Assess Current Security Practices Against ISO 27001 Standards › 4.3 Develop a Compliance Framework Aligned with ISO 27001 › 4.4 Implement Risk Assessment Procedures for Data Security › 4.5 Monitor and Audit Compliance with ISO 27001 Regulations › 4.6 Evaluate and Update Compliance Measures Regularly • 5 Auditing and Continuous Improvement in Aerospace Compliance — 6 classes › 5.1 Understand the Role of Auditing in Aerospace Compliance › 5.2 Identify Key Compliance Standards and Regulations in Aerospace › 5.3 Develop Effective Auditing Techniques for ISO 27001ARS › 5.4 Analyze Common Compliance Gaps in Aerospace Organizations › 5.5 Implement Continuous Improvement Strategies Post-Audit › 5.6 Evaluate Case Studies of Successful Compliance Enhancements

2

Incident Management and Response

5 chapters · 6 classes

65 marks

• 1 Understanding Incident Management Frameworks in Aerospace

— 6 classes

- › 1.1 Define the Key Components of Incident Management Frameworks
- › 1.2 Explore the Importance of Incident Response in Aerospace
- › 1.3 Identify the Roles and Responsibilities in Incident Management
- › 1.4 Analyze Common Incident Scenarios in the Aerospace Sector
- › 1.5 Evaluate Tools and Techniques for Effective Incident Response
- › 1.6 Develop an Incident Response Plan Tailored for Aerospace Organizations

• 2 Identifying and Classifying Security Incidents

• 3 Developing an Incident Response Plan

• 4 Executing Incident Response Strategies

• 5 Post-Incident Analysis and Continuous Improvement

3

Information Security Frameworks

5 chapters · 30 classes

65 marks

• 1 Understanding Information Security in Aerospace Operations — 6 classes

- › 1.1 Define Key Concepts in Information Security for Aerospace
- › 1.2 Identify Information Security Risks in Aerospace Operations
- › 1.3 Explore ISO 27001 Framework and Its Relevance to Aerospace
- › 1.4 Assess Existing Information Security Policies in Aerospace
- › 1.5 Implement Best Practices for Information Security Management
- › 1.6 Evaluate and Improve Information Security Strategies in Aerospace

• 2 ISO 27001 Overview and Its Applicability to Aerospace — 6 classes

- › 2.1 Define ISO 27001 and Its Purpose in Information Security
- › 2.2 Identify Key Components and Structure of ISO 27001
- › 2.3 Explore the Importance of Information Security in Aerospace
- › 2.4 Compare ISO 27001 with Other Information Security Frameworks
- › 2.5 Assess the Applicability of ISO 27001 in Aerospace Environments
- › 2.6 Implement Initial Steps for ISO 27001 Compliance in Aerospace

• 3 Framework Implementation Strategies for Aerospace Organizations — 6 classes

- › 3.1 Assess Current Information Security Gaps in Aerospace Organizations
- › 3.2 Identify Key Stakeholders for Framework Implementation
- › 3.3 Develop a Tailored Implementation Plan for ISO 27001
- › 3.4 Integrate Information Security Policies with Organizational Strategy
- › 3.5 Monitor and Evaluate Effectiveness of the Security Framework
- › 3.6 Conduct Training and Awareness Programs for Personnel Involved

• 4 Audit and Compliance Processes for ISO 27001 in Aerospace — 6 classes

- › 4.1 Understand the ISO 27001 Framework in Aerospace
- › 4.2 Identify Key Audit Requirements for ISO 27001
- › 4.3 Analyze Compliance Obligations in Aerospace Security
- › 4.4 Develop Audit Checklists for ISO 27001 Standards
- › 4.5 Conduct Mock Audits to Evaluate Compliance
- › 4.6 Implement Continuous Improvement Processes Post-Audit

• 5 Continuous Improvement and Future Trends in Information Security — 6 classes

- › 5.1 Analyze Current Trends in Information Security
- › 5.2 Evaluate Continuous Improvement Models in Information Security
- › 5.3 Implement Effective Metrics for Information Security Performance
- › 5.4 Develop a Continuous Improvement Plan for Security Practices
- › 5.5 Discuss Future Challenges and Innovations in Information Security
- › 5.6 Create a Roadmap for Adopting Emerging Technologies in Security

4

Leadership and Team Dynamics

0 chapters

85 marks

• 1 Fundamentals of Risk Management in Aerospace — 6 classes

- › 1.1 Define and Explain Risk Management Concepts in Aerospace
- › 1.2 Identify Key Risks in Aerospace Operations
- › 1.3 Analyze the Impact of Risks on Aerospace Projects
- › 1.4 Evaluate Risk Mitigation Strategies in Aerospace
- › 1.5 Develop a Risk Management Framework for Aerospace
- › 1.6 Implement Risk Management Practices in Aerospace Leadership

• 2 Identifying Risks in Aerospace Operations — 6 classes

- › 2.1 Understand Key Risk Concepts in Aerospace Operations
- › 2.2 Identify Common Risks in Aerospace Environments
- › 2.3 Analyze Internal and External Risk Factors in Aerospace
- › 2.4 Utilize Risk Assessment Tools for Aerospace Operations
- › 2.5 Evaluate the Impact of Identified Risks on Aerospace Projects
- › 2.6 Develop Mitigation Strategies for Key Aerospace Risks

• 3 Risk Assessment Methodologies for Aerospace — 6 classes

- › 3.1 Identify Key Risk Assessment Methodologies in Aerospace
- › 3.2 Analyze the Impact of Risks on Aerospace Operations
- › 3.3 Evaluate Probability and Severity of Risks in Aerospace Contexts
- › 3.4 Compare and Contrast Qualitative and Quantitative Risk Assessment Techniques
- › 3.5 Develop a Risk Assessment Matrix for Aerospace Applications
- › 3.6 Implement Risk Treatment Strategies in Aerospace Projects

• 4 Risk Mitigation Strategies and Implementation — 6 classes

- › 4.1 Identify Key Risk Mitigation Strategies in Aerospace
- › 4.2 Analyze the Effectiveness of Risk Mitigation Approaches
- › 4.3 Develop a Comprehensive Risk Mitigation Plan
- › 4.4 Implement Risk Mitigation Strategies in Aerospace Operations
- › 4.5 Evaluate the Impact of Risk Mitigation on Aerospace Projects
- › 4.6 Communicate Risk Mitigation Strategies to Stakeholders

• 5 Continuous Monitoring and Improvement of Risk Management — 6 classes

- › 5.1 Identify Key Risk Indicators for Continuous Monitoring
- › 5.2 Establish a Framework for Ongoing Risk Assessment
- › 5.3 Implement Feedback Loops for Risk Management Enhancement
- › 5.4 Analyze Data Trends to Improve Risk Response Strategies
- › 5.5 Develop Training Modules for Continuous Risk Awareness
- › 5.6 Create an Action Plan for Proactive Risk Management Upgrades