

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001AVS — Information Security for Media Companies

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-AVS-27001AVS • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	IIT-AVS-27001AVS
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1

Incident Management and Response

5 chapters · 30 classes 65 marks

• 1 Understanding Incident Management Frameworks in Media Companies — 6 classes

› 1.1 Define Incident Management in the Context of Media Companies

› 1.2 Identify Key Components of Incident Management Frameworks

› 1.3 Explore Legislative and Regulatory Requirements Impacting Incident Management

› 1.4 Analyze Case Studies of Incident Response in Media Companies

› 1.5 Develop a Sample Incident Response Plan for Media Scenarios

› 1.6 Evaluate the Effectiveness of Incident Management Frameworks in Practice

• 2 Identifying and Classifying Incidents in Audio-Visual Environments — 6 classes

› 2.1 Define Key Incident Types in Audio-Visual Systems

› 2.2 Recognize Signs of Potential Security Incidents

› 2.3 Implement Classification Criteria for Incidents

› 2.4 Use Case Studies to Identify Incident Scenarios

› 2.5 Develop Incident Reporting Guidelines for AV Teams

› 2.6 Analyze Incident Impact and Prioritize Response Actions

• 3 Incident Response Planning and Preparation for Media Organizations — 6 classes

› 3.1 Identify Key Components of an Incident Response Plan

› 3.2 Assess Potential Security Threats in Media Organizations

› 3.3 Develop Incident Classification Criteria for Effective Response

› 3.4 Designate Roles and Responsibilities in Incident Response Teams

› 3.5 Create a Communication Strategy for Incident Management

› 3.6 Conduct Tabletop Exercises to Test Incident Response Plans

• 4 Executing Incident Response Protocols: Best Practices — 6 classes

› 4.1 Identify and Classify Security Incidents Effectively

› 4.2 Activate the Incident Response Team for Immediate Action

› 4.3 Communicate Incident Details to Stakeholders Clearly

› 4.4 Contain and Mitigate the Impact of Security Incidents

› 4.5 Analyze and Document Incident Responses for Future Reference

› 4.6 Review and Update Incident Response Protocols Regularly

• 5 Post-Incident Analysis and Continuous Improvement Strategies — 6 classes

› 5.1 Analyze Incident Data to Identify Root Causes

› 5.2 Evaluate Response Effectiveness and Team Performance

› 5.3 Document Findings and Create Post-Incident Reports

› 5.4 Develop Actionable Recommendations for Improvement

› 5.5 Implement Continuous Improvement Frameworks

› 5.6 Conduct Stakeholder Review and Feedback Sessions

• 1 Understanding ISO 27001: Principles and Requirements — 6

classes

- › 1.1 Explore the Fundamentals of ISO 27001
- › 1.2 Identify Key Principles of Information Security Management
- › 1.3 Analyze the Requirements for ISO 27001 Certification
- › 1.4 Understand the Role of Risk Assessment in ISO 27001
- › 1.5 Evaluate the Importance of Continuous Improvement in ISMS
- › 1.6 Implement Best Practices for Adopting ISO 27001 Standards

• 2 Risk Assessment and Treatment in Media Environments — 6

classes

- › 2.1 Identify Risks in Media Operations
- › 2.2 Analyze Vulnerabilities in Media Assets
- › 2.3 Evaluate Potential Threats to Information Security
- › 2.4 Prioritize Risks Based on Impact and Likelihood
- › 2.5 Develop Risk Treatment Plans for Media Environments
- › 2.6 Implement and Monitor Risk Mitigation Strategies

• 3 Implementing Security Controls within Media Companies — 6

classes

- › 3.1 Assessing Current Security Posture in Media Companies
- › 3.2 Identifying Key Security Controls for Media Operations
- › 3.3 Developing a Risk Management Framework for Media Firms
- › 3.4 Integrating Technical and Administrative Controls
- › 3.5 Training Employees on Security Protocols and Best Practices
- › 3.6 Evaluating the Effectiveness of Security Controls in Media Companies

• 4 Managing Compliance and Auditing Processes — 6 classes

- › 4.1 Define Compliance Requirements for Media Companies
- › 4.2 Identify Key Components of an Auditing Framework
- › 4.3 Develop an Internal Audit Plan for Information Security
- › 4.4 Implement Risk Assessment Strategies in Auditing Processes
- › 4.5 Analyze Audit Findings and Develop Corrective Actions
- › 4.6 Communicate Audit Results to Stakeholders Effectively

• 5 Cultivating a Security Culture in Media Organizations — 6 classes

- › 5.1 Define Security Culture and Its Impact on Media Organizations
- › 5.2 Identify Key Elements of a Strong Security Culture
- › 5.3 Assess Current Security Practices and Cultural Gaps in Your Organization
- › 5.4 Develop Strategies for Promoting Information Security Awareness
- › 5.5 Implement Training Programs to Enhance Security Competencies
- › 5.6 Evaluate and Measure the Effectiveness of Security Culture Initiatives

• 1 Understanding Leadership Principles in Information Security**• 2 Developing a Strategic Vision for Information Security Management****• 3 Risk Assessment and Management Strategies in Media Companies****• 4 Fostering a Cybersecurity Culture within Media Organizations****• 5 Evaluating Leadership Effectiveness in Information Security Initiatives**

• 1 Understanding Legal Frameworks in Media Security — 6 classes

- › 1.1 Identify Key Legal Frameworks Affecting Media Security
- › 1.2 Analyze the Importance of Compliance with Data Protection Laws
- › 1.3 Examine Intellectual Property Rights in the Media Industry
- › 1.4 Assess the Impact of GDPR on Media Practices
- › 1.5 Evaluate Industry-Specific Regulations for Media Companies
- › 1.6 Develop a Compliance Action Plan for Media Security Policies

• 2 Compliance Standards for Media Companies — 6 classes

- › 2.1 Identify Key Compliance Standards for Media Companies
- › 2.2 Analyze the Importance of ISO 27001 for Information Security
- › 2.3 Assess Legal Obligations Under Data Protection Regulations
- › 2.4 Evaluate Risks Associated with Non-Compliance
- › 2.5 Develop a Compliance Checklist for Media Operations
- › 2.6 Implement Best Practices for Ongoing Compliance Monitoring

• 3 Risk Assessment and Management in Legal Compliance — 6 classes

- › 3.1 Identify Legal Requirements for Information Security
- › 3.2 Assess Risks Associated with Legal Non-Compliance
- › 3.3 Evaluate The Impact of Data Breaches on Legal Compliance
- › 3.4 Develop a Risk Management Framework for Legal Compliance
- › 3.5 Implement Risk Mitigation Strategies in Media Practices
- › 3.6 Review and Update Legal Compliance Procedures Regularly

• 4 Data Privacy Regulations and Impact on Media Operations — 6 classes

- › 4.1 Explore Key Data Privacy Regulations Affecting Media Companies
- › 4.2 Analyze the Impact of GDPR on Media Operations
- › 4.3 Identify Best Practices for Compliance with Data Privacy Laws
- › 4.4 Evaluate the Role of Data Protection Officers in Media Firms
- › 4.5 Develop a Compliance Checklist for Media Operations
- › 4.6 Create a Data Privacy Impact Assessment for Media Projects

• 5 Auditing and Reporting for Compliance — 6 classes

- › 5.1 Understand the Purpose and Scope of Auditing for Compliance
- › 5.2 Identify Key Legal and Regulatory Frameworks Affecting Media Companies
- › 5.3 Explore the Audit Process: Planning and Preparation
- › 5.4 Conducting Effective Compliance Audits: Best Practices
- › 5.5 Analyze Audit Findings and Their Implications for Compliance
- › 5.6 Develop Reports for Stakeholders: Communicating Audit Results

• 1 Foundations of Risk Assessment in the Media Industry — 6 classes

- › 1.1 Define Key Concepts of Risk in the Media Industry
- › 1.2 Identify Common Risks Facing Media Companies
- › 1.3 Analyze the Impact of Risk on Media Operations
- › 1.4 Explore Risk Assessment Methodologies for Media Contexts
- › 1.5 Develop a Risk Assessment Framework for Media Projects
- › 1.6 Create a Risk Management Plan for Media Initiatives

• 2 Understanding Risk Analysis Methodologies — 6 classes

- › 2.1 Define Key Concepts in Risk Analysis Methodologies
- › 2.2 Identify Different Types of Risks in Media Companies
- › 2.3 Explore Qualitative vs Quantitative Risk Assessment Techniques
- › 2.4 Analyze Risk Assessment Frameworks Relevant to Media
- › 2.5 Evaluate Risk Management Strategies for Effective Decision Making
- › 2.6 Apply Risk Analysis Methodologies to Case Studies in Media

• 3 Evaluating Risks Specific to Media Operations — 6 classes

- › 3.1 Identify Key Risks in Media Operations
- › 3.2 Analyze Vulnerabilities in Media Infrastructure
- › 3.3 Evaluate Impact of Risks on Media Delivery
- › 3.4 Prioritize Risks Based on Severity and Likelihood
- › 3.5 Develop Mitigation Strategies for Media Risks
- › 3.6 Implement a Monitoring Framework for Ongoing Risk Assessment

• 4 Implementing Risk Mitigation Strategies — 6 classes

- › 4.1 Identify Key Risks in Media Operations
- › 4.2 Evaluate Risk Impact and Likelihood
- › 4.3 Develop Risk Mitigation Strategies
- › 4.4 Communicate Risk Mitigation Plans Effectively
- › 4.5 Implement Risk Mitigation Actions
- › 4.6 Review and Adjust Risk Management Strategies

• 5 Monitoring and Reviewing Risk Management Practices — 6 classes

- › 5.1 Analyze Current Risk Management Practices
- › 5.2 Identify Key Performance Indicators for Risk Monitoring
- › 5.3 Implement Effective Monitoring Tools and Techniques
- › 5.4 Evaluate the Effectiveness of Existing Controls
- › 5.5 Conduct Regular Risk Reviews and Assessments
- › 5.6 Create an Action Plan for Continuous Improvement