

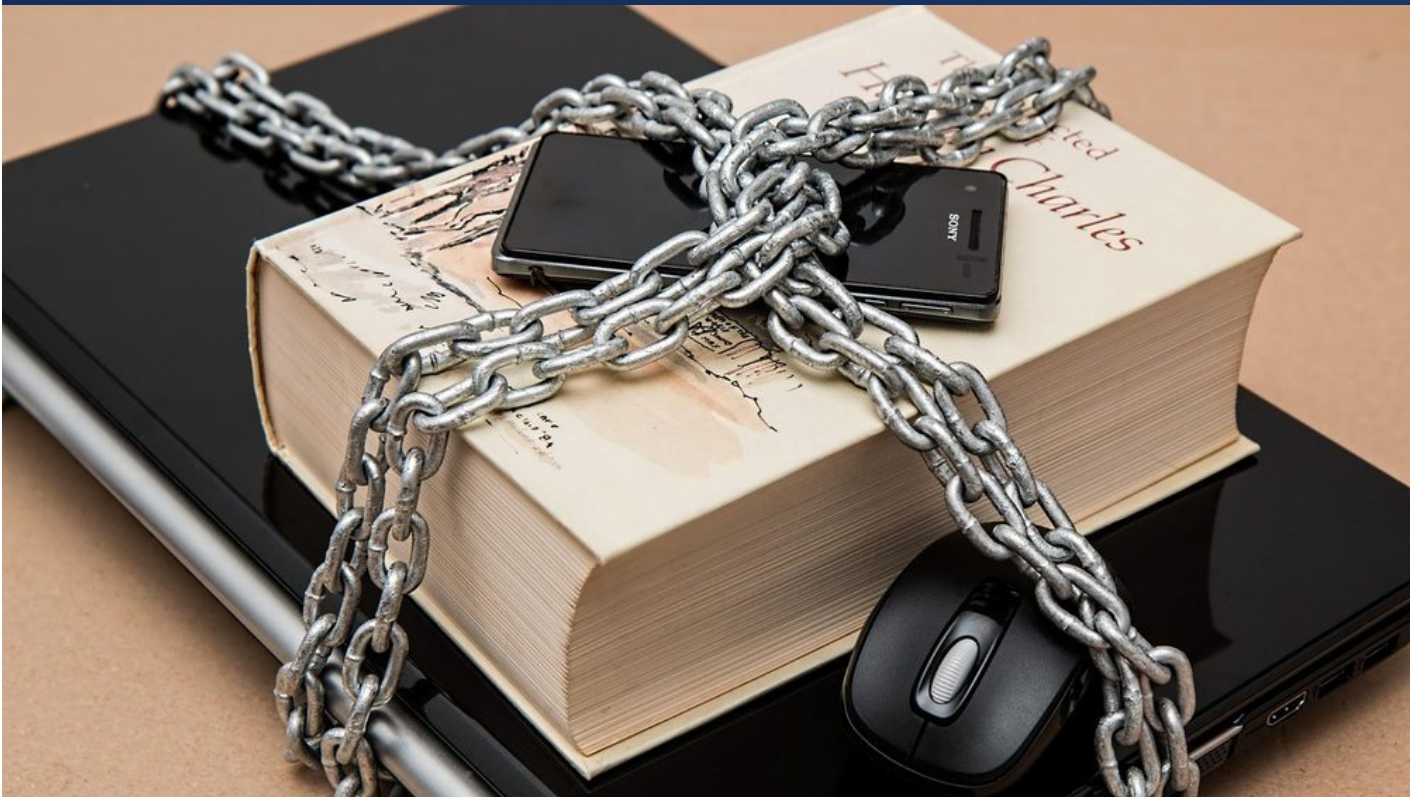
LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001SMV — Information Security in Connected Vehicles

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-SMV-27001SMV • ISO Transport

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

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

CURRICULUM

1 Information Security Principles 5 chapters · 30 classes 85 marks • 1 Fundamentals of Information Security in Connected Vehicles — 6 classes › 1.1 Define Key Concepts of Information Security in Connected Vehicles › 1.2 Identify Common Threats to Information Security in Connected Vehicles › 1.3 Explore the Role of Data Privacy in Connected Vehicle Systems › 1.4 Assess the Importance of Risk Management in Connected Vehicles › 1.5 Develop Security Policies for Connected Vehicle Information Systems › 1.6 Implement Best Practices for Securing Connected Vehicle Data Transmission • 2 Identifying and Assessing Information Security Risks in Smart Systems Vehicles — 6 classes › 2.1 Define Key Information Security Risks in Smart Systems Vehicles › 2.2 Analyze Vulnerabilities in Connected Vehicle Systems › 2.3 Evaluate Threats to Information Security in Smart Vehicles › 2.4 Assess the Impact of Security Breaches in Connected Vehicles › 2.5 Prioritize Risks Based on Likelihood and Impact in Smart Systems › 2.6 Develop a Risk Mitigation Strategy for Information Security in Vehicles • 3 Implementing Security Controls for Connected Vehicle Systems — 6 classes › 3.1 Assess Current Security Vulnerabilities in Connected Vehicles › 3.2 Identify and Select Appropriate Security Controls for Vehicle Systems › 3.3 Develop a Risk Management Plan for Connected Vehicle Security › 3.4 Implement Technical Security Measures in Vehicle Systems › 3.5 Establish Policies and Procedures for Security Maintenance › 3.6 Evaluate the Effectiveness of Security Controls and Improve Them • 4 Developing a Comprehensive Information Security Policy for Connected Vehicles — 6 classes › 4.1 Identify Key Components of an Information Security Policy for Connected Vehicles › 4.2 Analyze Regulatory Requirements Impacting Information Security in Connected Vehicles › 4.3 Assess Risk Management Strategies for Connected Vehicle Security › 4.4 Develop Security Objectives Aligned with Business Goals for Connected Vehicles › 4.5 Implement Best Practices for Creating a Comprehensive Information Security Policy › 4.6 Evaluate and Update the Information Security Policy Regularly for Continuous Improvement • 5 Continuous Improvement and Incident Response in Vehicle Information Security — 6 classes › 5.1 Analyze Continuous Improvement Models for Information Security › 5.2 Identify Key Components of an Effective Incident Response Plan › 5.3 Evaluate Real-World Case Studies of Incident Response in Connected Vehicles › 5.4 Develop a Framework for Continuous Monitoring of Vehicle Information Security › 5.5 Implement Best Practices for Post-Incident Reviews and Lessons Learned › 5.6 Create a Personalized Action Plan for Enhancing Vehicle Cybersecurity
--

• 1 Understanding the Risk Landscape in Connected Vehicles — 6

classes

- › 1.1 Identify Key Risks in Connected Vehicle Systems
- › 1.2 Analyze the Impact of Cyber Threats on Vehicle Security
- › 1.3 Assess Vulnerabilities in Connected Vehicle Infrastructure
- › 1.4 Evaluate Regulatory and Compliance Requirements for Connected Vehicles
- › 1.5 Develop Risk Mitigation Strategies for Connected Vehicles
- › 1.6 Implement a Risk Management Framework for Connected Vehicle Technologies

• 2 Identifying and Assessing Risks in Smart Systems Vehicles — 6

classes

- › 2.1 Define Key Concepts in Risk Management for Connected Vehicles
- › 2.2 Identify Common Risks Associated with Smart Systems Vehicles
- › 2.3 Analyze Vulnerabilities in Connected Vehicle Technologies
- › 2.4 Assess the Impact of Risks on Vehicle Security and Safety
- › 2.5 Evaluate Risk Likelihood Using Case Studies in Smart Vehicles
- › 2.6 Develop a Risk Assessment Framework for Connected Vehicles

• 3 Implementing Risk Mitigation Strategies for Connected Vehicles

— 6 classes

- › 3.1 Identify Key Risks in Connected Vehicle Systems
- › 3.2 Assess the Impact of Cyber Threats on Vehicle Safety
- › 3.3 Develop a Risk Management Framework for Connected Vehicles
- › 3.4 Create Effective Risk Mitigation Strategies for Vulnerabilities
- › 3.5 Implement a Continuous Risk Monitoring Plan for Connected Vehicles
- › 3.6 Evaluate the Effectiveness of Risk Mitigation Measures

• 4 Monitoring and Reviewing Risk Management Processes**• 5 Communicating Risks and Ensuring Stakeholder Engagement in Connected Vehicle Security**