GAQM
Global Association for Quality Management

ISO/IEC 27006-1:2024 - Certified Lead Auditor

www.gaqm.org

ISO/IEC 27006-1:2024 - Certified Lead Auditor - Certification Overview

ISO/IEC 27006-1:2024 Certified Lead Auditor certification is designed for professionals seeking to develop advanced knowledge and expertise in auditing Information Security Management Systems. The standard specifies requirements for organizations and certification bodies that conduct audits and provide ISO/IEC 27001 certification. It complements ISO/IEC 17021-1 and establishes requirements to ensure that ISMS certification activities are performed competently, consistently, and impartially.

This certification equips professionals with the knowledge and skills required to understand ISMS certification requirements, evaluate auditor competence, apply auditing principles, assess information security controls, and understand the certification process. Participants gain insights into audit planning, audit team management, risk assessment, audit evidence evaluation, nonconformity identification, reporting, and follow-up activities. It also develops an understanding of information security, cybersecurity, management system requirements, and the responsibilities involved in leading ISMS certification audits.

The ISO/IEC 27006-1:2024 Certified Lead Auditor qualification is valuable for information security professionals, ISMS auditors, compliance managers, consultants, risk management professionals, and certification body personnel. It demonstrates professional competence in understanding and applying the requirements governing ISMS auditing and certification. This qualification can enhance career opportunities in information security auditing, ISO certification, governance, risk, and compliance (GRC), while supporting professional development in the field of information security management.

Target Audience

Target Audience: The ISO/IEC 27006-1:2024 Certified Lead Auditor course is intended for information security professionals, ISO/IEC 27001 Lead Auditors, ISMS consultants, compliance officers, risk managers, cybersecurity professionals, quality management professionals, and certification body personnel who are involved in or aspire to work in ISMS auditing and certification activities. It is particularly beneficial for individuals seeking to enhance their understanding of ISMS certification requirements, auditor competence, audit management, and the principles of impartiality, consistency, and competence in information security management system certification.

What Modules are covered?

Module 1 - Introduction to ISO/IEC 27006-1:2024

- Introduction to Information Security Management Systems (ISMS)
- Overview and Scope of ISO/IEC 27006-1:2024
- Structure and Key Requirements of the Standard
- Relationship Between ISO/IEC 27001 and ISO/IEC 17021-1
- Principles of ISMS Auditing and Certification
- Roles and Responsibilities of ISMS Lead Auditors

Module 2 - General and Structural Requirements

- Legal and Contractual Requirements
- Management of Impartiality and Conflicts of Interest
- Liability and Financial Requirements
- Structural Requirements for Certification Bodies
- Management and Competence of Certification Personnel
- Confidentiality and Information Security Requirements

Module 3 - Resource and Competence Requirements

- Competence Requirements for ISMS Auditors
- Knowledge and Skills of Information Security Auditors
- Evaluation of Auditor Competence
- Selection and Management of Audit Teams
- Requirements for Technical Experts and External Auditors
- Auditor Performance Monitoring and Professional Development

Module 4 - ISMS Certification Process and Audit Planning

- Application Review and Contract Management
- Determination of ISMS Certification Scope
- Audit Programme Management and Planning
- Determining ISMS Audit Duration
- Multi-Site Certification and Sampling Requirements
- Initial Certification Audits – Stage 1 and Stage 2

Module 5 - Conducting ISMS Audits and Certification Decisions

- Audit Preparation and Opening Meetings
- Audit Evidence Collection and Evaluation
- Assessment of Information Security Risk Management
- Evaluation of ISO/IEC 27001 Information Security Controls
- Identification of Nonconformities and Audit Findings
- Audit Reporting, Certification Review, and Decision-Making

Module 6 - Certification Maintenance and Practical Audit Applications

- Surveillance and Recertification Audits
- Suspension, Withdrawal, and Scope Reduction of Certification
- Handling Complaints and Appeals
- Corrective Actions and Follow-Up Audits
- Practical ISMS Lead Auditor Case Studies and Exercises
- Final Assessment and Certification Examination