GAQM
Global Association for Quality Management

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

www.gaqm.org

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

The ISO/IEC 27006-1:2024 Certified Lead Implementer certification is designed for professionals who wish to develop the knowledge and expertise required to plan, implement, manage, and maintain an Information Security Management System (ISMS) audit and certification framework in accordance with ISO/IEC 27001 requirements and ISO/IEC 27006-1 guidelines. It provides an understanding of the principles, requirements, methodologies, and best practices for establishing effective ISMS certification processes, ensuring consistency, competence, impartiality, and reliability in information security management system certification activities.

The certification training equips participants with insights into certification body requirements, audit planning, auditor competence, certification processes, risk-based assessment, and the management of certification activities. Participants gain familiarity with application reviews, audit team selection, audit duration determination, audit planning, initial certification, surveillance audits, recertification, certification decision-making, and handling confidentiality and impartiality throughout the certification lifecycle.

Target Audience

This certification is intended for information security professionals, ISMS auditors, consultants, certification body personnel, and management system professionals who wish to gain expertise in ISO/IEC 27006-1:2024 requirements and ISMS certification practices. It is particularly suitable for professionals involved in ISO/IEC 27001 audits, certification operations, accreditation, compliance, and information security governance.

- Information Security Managers and Consultants
- ISO/IEC 27001 Lead Auditors and Auditors
- ISMS Implementation Professionals
- Certification Body Auditors and Certification Managers
- Compliance, Risk, and Governance Professionals
- Accreditation and Quality Management Professionals
- IT Security Professionals and Consultants
- Professionals aspiring to work in ISMS certification and auditing

What Modules are covered?

Module 1 - Understanding ISO/IEC 27006-1:2024

- Purpose and scope of the standard
- The role of ISO/IEC 27006-1 in the ISO/IEC 27000 family
- Intended readers and practical applications
- Key terms and concepts

Module 2 - The ISMS Certification Landscape

- The purpose of ISMS Certification
- The relationship between ISO/IEC 27001 and ISO/IEC 27006-1
- Certification bodies and accreditation bodies
- The roles of auditors, technical experts and decision-makers
- Certification impartiality and independence

Module 3 - Requirements for ISMS Certification Bodies

- General requirements and organizational structure
- Management of competence and personnel
- Resource planning and technical capability
- Outsourcing and external resources
- Confidentiality and information security
- Documented information and records

Module 4 - Establishing Competence for ISMS Certification

- Defining the competence needed for certification activities
- Understanding information security management
- Assessing technical and sector-specific knowledge
- Evaluating auditors and technical experts
- Authorization, monitoring and reassessment
- Maintaining competence through continuing development

Module 5 - Managing Impartiality and Conflicts of Interest

- Identifying threats to impartiality
- Assessing and controlling conflicts of interest
- Separating consultancy from certification
- Safeguarding impartiality in audit teams
- Reviewing impartiality arrangements

Module 6 - Application Review and certification Planning

- Receiving and reviewing an application
- Defining the ISMS scope and boundaries
- Determining audit time and resource needs
- Selecting the audit team
- Preparing the audit program
- Managing multi-site and complex organizations

Module 7 - Conducting the Initial Certification Audit

- Stage 1 audit objectives and preparation
- Reviewing documented information and readiness
- Stage 2 audit objectives and evidence gathering
- Evaluating the implementation of the ISMS
- Identifying and recording audit findings
- Communicating results and next steps

Module 8 - Audit Time, Sampling and Risk-Based Planning

- Principles for determining audit duration
- Factors that influence audit time
- Applying sampling to sites, processes and records
- Addressing complexity and information security risk
- Documenting audit-time decisions
- Reviewing adjustments to the audit plan

Module 9 - Evaluating Audit Evidence

- Linking evidence to ISO/IEC 27001 requirements
- Classifying nonconformities
- Assessing corrections and corrective actions
- Managing disputed or unclear findings
- Maintaining consistent audit records

Module 10 - Certification Decisions and Certification Management

- Reviewing audit results before a decision
- Ensuring decision-makers are independent
- Granting or refusing certification
- Issuing certificates and defining their scope
- Suspending, withdrawing or reducing certification
- Managing changes to certified organization

Module 11 - Surveillance and Recertification

- Planning the surveillance cycle
- Selecting surveillance activities
- Evaluating significant changes and incidents
- Preparing for recertification
- Addressing overdue or incomplete audits
- Maintaining continuity of certification

Module 12 - Complaints, Appeals and External Communication

- Receiving and handling complaints
- Managing appeals against certification decisions
- Protecting confidentiality during investigations
- Communicating Certification status accurately
- Managing public information and certificate claims

Chapter 13 - Integrating ISO/IEC 27006-1:2024 into Certification Operations

- Conducting a gap assessment against