CERTIFICATION SYLLABUS

ISO/IEC 27001:2022 Certified Lead Implementer

Exam Code: 27001:2022-CLI™



A complete preparation guide covering exam objectives, core competencies, domain weightage, and topics to prepare.

©2026 Certaining, Inc. All rights reserved.

Table of Contents

1. **Exam Name & Code** 1
2. **Table of Contents** 2
3. **Objective of the Certification** 3
4. **Core Competencies** 4-5
5. **Who Should Take This Certification** 6
6. **Exam Information** 6
7. **Examination Domain & Weightage** 7
8. **Topics to Prepare** 8-10
   - *ISMS Fundamentals & ISO/IEC 27001:2022 Requirements (Advanced)*
   - *Implementation Project Planning & Gap Analysis*
   - *Risk Assessment, Risk Treatment & Statement of Applicability*
   - *Annex A Controls & Operational Implementation*
   - *Leadership, Resources, Competence & Awareness*
   - *Monitoring, Internal Audit & Management Review*
   - *Corrective Action, Certification Readiness & Sustaining the ISMS*

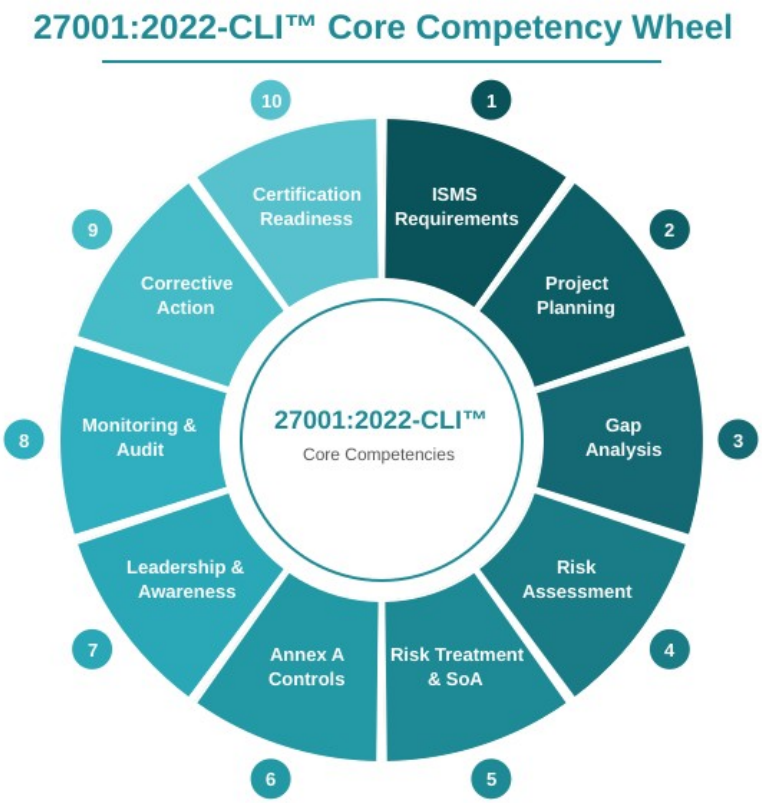
©2026 Certaining, Inc. All rights reserved.

Objective of the Certification

- **Validate lead implementer competence:** the ability to plan, lead, and manage the implementation of an Information Security Management System (ISMS) based on ISO/IEC 27001:2022.
- **Deepen standards expertise:** apply the ISO/IEC 27001:2022 requirements and the Annex A controls, together with ISO/IEC 27002 guidance, with the judgment needed to lead an implementation project.
- **Plan the implementation:** build a business case, define scope and objectives, set up a project team, and prepare a realistic implementation plan.
- **Perform gap analysis:** compare current practices with ISO/IEC 27001:2022 requirements and prioritize actions.
- **Lead risk assessment and treatment:** design a risk assessment method, assess and treat information security risks, and prepare the Statement of Applicability and risk treatment plan.
- **Implement Annex A controls:** select, design, and implement organizational, people, physical, and technological controls in line with the risks.
- **Build leadership, competence, and awareness:** secure top management commitment, assign roles and resources, and develop competence and awareness programs.
- **Measure and review performance:** set up monitoring and measurement, internal audit, and management review of the ISMS.
- **Drive corrective action and improvement:** manage nonconformities, root cause analysis, corrective action, and continual improvement.
- **Prepare for certification and sustain the ISMS:** get ready for stage 1 and stage 2 certification audits and keep the ISMS effective afterwards.

©2026 Certaining, Inc. All rights reserved.

Core Competencies — 27001:2022-CLI™ (ISO/IEC 27001:2022 Certified Lead Implementer)



©2026 Certaining, Inc. All rights reserved.

- **ISMS requirements knowledge:** interpret ISO/IEC 27001:2022 clauses 4 to 10 in depth, including context, leadership, planning, support, operation, performance evaluation, and improvement.
- **Implementation project planning:** define the business case, scope, objectives, team, timeline, and resources for an ISMS implementation.
- **Gap analysis:** assess current practices against the requirements and Annex A controls and prioritize the gaps.
- **Risk assessment:** design and apply a consistent method to identify, analyze, and evaluate information security risks.
- **Risk treatment and Statement of Applicability:** select treatment options and controls, prepare the risk treatment plan, and justify the Statement of Applicability.
- **Annex A control implementation:** implement and tailor the 93 controls across the four themes to the organization's needs.
- **Leadership, competence, and awareness:** obtain management commitment, define roles, and build competence and awareness across the organization.
- **Monitoring and internal audit:** define security metrics, plan internal audits, and prepare management review inputs and outputs.
- **Corrective action and improvement:** manage nonconformities and drive continual improvement of the ISMS.
- **Certification readiness:** understand the stage 1 and stage 2 audits, surveillance, and how to sustain the ISMS after certification.

©2026 Certaining, Inc. All rights reserved.

Who Should Take This Certification

- Information security managers and officers who will lead or manage an ISMS implementation.
- IT managers, CISOs, and security architects responsible for ISO/IEC 27001 readiness.
- Project managers who coordinate information security or compliance programs.
- Risk, compliance, and governance professionals supporting ISO/IEC 27001 certification.
- Consultants who help organizations design and implement an ISMS.
- Professionals who have completed foundation or internal auditor credentials and want to advance.

Exam Information

Exam Name	ISO/IEC 27001:2022 Certified Lead Implementer
Exam Code	27001:2022-CLI™
Exam Format	Multiple Choice Questions (MCQ), including scenario-based questions
Duration	120 minutes
Number of Questions	80
Passing Score	70%
Mode of Exam	Test Center Based Testing / Online Testing
Language	English
Validity	Lifetime
Open Book	No

©2026 Certaining, Inc. All rights reserved.

Examination Domain & Weightage

Domain	Weightage
ISMS Fundamentals & ISO/IEC 27001:2022 Requirements (Advanced)	20%
Implementation Project Planning & Gap Analysis	15%
Risk Assessment, Risk Treatment & Statement of Applicability	15%
Annex A Controls & Operational Implementation	15%
Leadership, Resources, Competence & Awareness	10%
Monitoring, Internal Audit & Management Review	15%
Corrective Action, Certification Readiness & Sustaining the ISMS	10%
Total	**100%**

©2026 Certaining, Inc. All rights reserved.

Topics to Prepare — 27001:2022-CLI™ (ISO/IEC 27001:2022 Certified Lead Implementer)

The topics below represent the core areas candidates should focus on for each domain, reflecting the auditor-level depth expected at the 27001:2022-CLI™ level.

1. ISMS Fundamentals & ISO/IEC 27001:2022 Requirements (Advanced) (20%)

- **Information security principles:** confidentiality, integrity, availability, and the purpose of an ISMS.
- **Standards family:** ISO/IEC 27000, 27001, 27002, 27003, 27004, and 27005, and their roles.
- **Context and scope (clause 4):** issues, interested parties and their requirements, scope, interfaces and dependencies, and the ISMS itself.
- **Leadership (clause 5):** top management commitment, the information security policy, and roles and responsibilities.
- **Planning (clause 6):** risk assessment, risk treatment, information security objectives, and planning of changes.
- **Support (clause 7):** resources, competence, awareness, communication, and documented information.
- **Operation (clause 8):** operational planning and control, risk assessment at planned intervals, and risk treatment.
- **Evaluation and improvement (clauses 9 and 10):** monitoring, internal audit, management review, nonconformity, corrective action, and continual improvement.

2. Implementation Project Planning & Gap Analysis (15%)

- **Project initiation:** top management commitment, business case, scope, and objectives.
- **Legal, regulatory, and contractual requirements:** identifying them and using them as inputs to the ISMS.
- **Gap analysis:** comparing current practices with ISO/IEC 27001 requirements and Annex A, and prioritizing gaps.
- **Implementation plan:** phases, milestones, resources, responsibilities, and schedule.
- **Project team and stakeholders:** cross-functional representation and stakeholder engagement.
- **Project risks:** resistance to change, resource limits, and how to treat them.
- **Integration:** aligning the ISMS with other management systems and existing processes.

3. Risk Assessment, Risk Treatment & Statement of Applicability (15%)

- **Risk assessment method:** risk criteria, risk acceptance criteria, and consistent, valid, and comparable results.

©2026 Certaining, Inc. All rights reserved.

- **Risk identification and analysis:** risk owners, consequences, likelihood, and levels of risk.
- **Risk evaluation:** comparing results with criteria and prioritizing risks.
- **Risk treatment options:** modify, retain, avoid, and share.
- **Control selection:** determining necessary controls and comparing them with Annex A.
- **Statement of Applicability:** necessary controls, justification, implementation status, and justified exclusions.
- **Risk treatment plan:** actions, owners, resources, timelines, and risk owner approval of residual risk.
- **Risk assessment review:** repeating assessments at planned intervals and after significant changes.

4. Annex A Controls & Operational Implementation (15%)

- **Annex A structure:** 93 controls in four themes: organizational, people, physical, and technological.
- **Organizational controls:** policies, asset inventory, classification, access control, supplier relationships, cloud services, and incident management.
- **People controls:** screening, terms of employment, awareness, and remote working.
- **Physical controls:** secure areas, physical entry, equipment security, and clear desk.
- **Technological controls:** endpoint security, access rights, backup, logging, vulnerability management, cryptography, and secure development.
- **Tailoring controls:** selecting and scaling controls to the organization’s risks and size.
- **Operational planning and control:** implementing processes and managing planned changes and outsourced services.

5. Leadership, Resources, Competence & Awareness (10%)

- **Top management role:** accountability, integration into business processes, and support.
- **Roles and authorities:** responsibility for ISMS conformity and reporting on performance.
- **Resources:** people, budget, tools, and time for the ISMS.
- **Competence:** determining needs, training, and evaluating effectiveness.
- **Awareness:** policy, contribution to the ISMS, and consequences of nonconformity.
- **Communication:** what, when, with whom, and how to communicate.

6. Monitoring, Internal Audit & Management Review (15%)

- **Monitoring and measurement:** what to measure, methods, timing, analysis, and evaluation.
- **Metrics:** effectiveness measures in place of simple activity counts, with guidance from ISO/IEC 27004.

©2026 Certaining, Inc. All rights reserved.

- **Internal audit:** audit program, criteria, scope, impartial auditors, and reporting.
- **Management review inputs:** status of actions, changes, performance trends, audit results, and risk treatment status.
- **Management review outputs:** decisions on improvement and changes to the ISMS.
- **Documented information:** records of monitoring, audits, and reviews.

7. Corrective Action, Certification Readiness & Sustaining the ISMS (10%)

- **Nonconformity and corrective action (clause 10.2):** reaction, root cause analysis, action, and effectiveness review.
- **Continual improvement (clause 10.1):** improving suitability, adequacy, and effectiveness.
- **Certification process:** stage 1, stage 2, surveillance, and recertification.
- **Readiness:** evidence the ISMS is operating, internal audit and management review completed.
- **Working with the certification body:** impartiality and independence of consultancy and certification.
- **Sustaining the ISMS:** keeping risks, controls, and documentation current.

©2026 Certaining, Inc. All rights reserved.