Certaining
Be Certain.

CERTIFICATION SYLLABUS



ISO/IEC 27001:
Information Security Lead Implementer

Exam Code: CSLI™

Table of Contents

1. Exam Name & Code.....1
2. Table of Contents.....2
3. Objective of the Certification.....3
4. Core Competencies.....4
5. Who Should Take This Certification.....5
6. Exam Information.....6
7. Examination Domain & Weightage.....7
8. Topics to Prepare.....8

3. Objective of the Certification

The **CSLI™** certification validates a professional's ability to plan, implement, operate and continually improve an Information Security Management System (ISMS) based on ISO/IEC 27001:2022. The certification aims to:

- Validate the ability to lead the end-to-end implementation of an ISMS based on ISO/IEC 27001.
- Build a clear understanding of the ISO/IEC 27001 requirements (Clauses 4–10) and the Annex A controls.
- Prepare professionals to plan implementation projects, including gap analysis, scoping, roadmap and resource planning.
- Develop the skills to carry out information security risk assessment and treatment, and to produce the Statement of Applicability (SoA).
- Enable candidates to select and implement the right Annex A controls for their organization.
- Strengthen the ability to create and manage ISMS documentation, policies and records.
- Promote security awareness, training and communication across the organization.
- Build competence in monitoring, measuring and reviewing ISMS performance through KPIs, internal audits and management reviews.
- Prepare organizations for Stage 1 and Stage 2 certification audits and later surveillance audits.
- Encourage continual improvement of the ISMS using the PDCA cycle.
- Support compliance with legal, regulatory, contractual and customer security requirements.
- Recognize professionals as capable of protecting the confidentiality, integrity and availability of organizational information assets.

4. Core Competencies

CSLI™ (ISO/IEC 27001: Information Security Lead Implementer) certified professionals demonstrate the following competencies:

01	Interpreting the requirements of ISO/IEC 27001:2022 (Clauses 4–10) and the controls of Annex A.
02	Defining the ISMS scope, context, interested parties and information security policy.
03	Conducting information security risk assessment and treatment, and producing the Statement of Applicability (SoA).
04	Selecting and implementing the Annex A controls (organizational, people, physical, technological).
05	Building and managing ISMS documentation, records and document control.
06	Planning implementation projects: gap analysis, roadmap, resources, budget and timelines.
07	Running awareness, training and communication programs.
08	Defining security metrics, monitoring, measurement and management review.
09	Handling internal audits, nonconformities and corrective actions.
10	Preparing the organization for Stage 1 and Stage 2 certification audits and surveillance audits.
11	Driving continual improvement using the PDCA model.

5. Who Should Take This Certification

This certification is designed for professionals who plan, lead or support the implementation of an ISO/IEC 27001 ISMS, including:

- Information security managers, CISOs and security officers
- IT managers, risk and compliance managers, and GRC professionals
- ISMS project managers and implementation team members
- Information security consultants and advisors
- Internal auditors moving into implementation roles
- Data protection, privacy and business continuity professionals
- Professionals who want to build a career in ISO/IEC 27001 implementation

Prerequisites: Basic knowledge of information security concepts. Prior experience in IT, security or management systems is helpful but not mandatory.

6. Exam Information

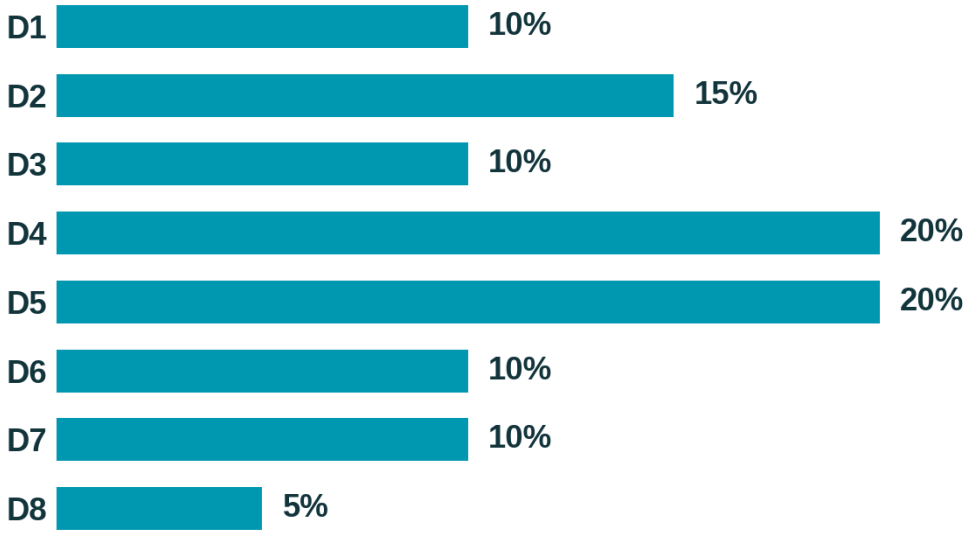
60	90	70%	Lifetime
Questions	Minutes	Passing Score	Validity

Exam Name	ISO/IEC 27001: Information Security Lead Implementer (CSLI™)
Exam Code	CSLI™
Exam Format	Multiple Choice Questions (MCQ)
Duration	90 minutes
Number of Questions	60
Passing Score	70%
Mode of Exam	Test Center Based Testing / Online Testing
Language	English
Validity	Lifetime
Open Book	No

7. Examination Domain & Weightage

No.	Domain	Weightage
D1	Fundamentals of Information Security and ISO/IEC 27001	10%
D2	Initiating the ISMS and Planning the Implementation	15%
D3	Context, Leadership and ISMS Scope	10%
D4	Information Security Risk Assessment and Treatment	20%
D5	Implementation of Annex A Controls	20%
D6	Documentation, Awareness and Operational Management	10%
D7	Monitoring, Internal Audit, Management Review and Improvement	10%
D8	Certification Audit Readiness	5%
	Total	**100%**

Weightage at a Glance



8. Topics to Prepare

CSLI™ (ISO/IEC 27001: Information Security Lead Implementer). Topics map to the exam domains D1–D8; the figure on the right shows each domain's weightage.

D1 Fundamentals 10%

- Confidentiality, integrity and availability (CIA triad)
- Key terms from ISO/IEC 27000
- ISO/IEC 27001 structure, the PDCA model and the ISO family of standards (27002, 27005, 27701)
- Benefits of ISMS certification and legal and regulatory drivers

D2 Initiating and Planning 15%

- Business case and securing management commitment
- Gap analysis, implementation roadmap and project plan
- Roles, responsibilities and resource planning
- Implementation approaches and critical success factors

D3 Context, Leadership and Scope (Clauses 4–5) 10%

- Internal and external issues, interested parties and their requirements
- Defining the ISMS scope and boundaries
- Top management leadership and the information security policy
- Roles, responsibilities and authorities

D4 Risk Assessment and Treatment (Clause 6) 20%

- Risk methodology, criteria and acceptance levels
- Asset identification, threats, vulnerabilities and impact analysis
- Risk treatment options and the risk treatment plan
- Statement of Applicability (SoA)
- Information security objectives and planning of changes

D5 Annex A Controls (2022 edition) 20%

- Organizational controls (37)
- People controls (8)
- Physical controls (14)
- Technological controls (34)
- Control implementation, including access control, cryptography, supplier relationships, incident management, business continuity and secure development

D6 Support and Operation (Clauses 7–8) 10%

- Resources, competence, awareness and communication
- Documented information and document control
- Operational planning and control
- Executing the risk treatment plan

D7 Performance Evaluation and Improvement (Clauses 9–10) 10%

- Monitoring, measurement, analysis and KPIs
- Internal audit programs
- Management review inputs and outputs
- Nonconformity, corrective action and continual improvement

D8 Certification Audit Readiness 5%

- Stage 1 and Stage 2 audit process
- Surveillance and recertification audits
- Choosing a certification body
- Common audit findings and how to prepare for them