CERTIFICATION SYLLABUS

ISO/IEC 27001: Information Security Lead Auditor

Exam Code: CSLA™



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** 8-9
   - *ISMS & ISO/IEC 27001:2022 Requirements (Advanced)*
   - *Annex A Controls & Risk Management for Auditors*
   - *Audit Program Management & Principles*
   - *Audit Planning & Preparation*
   - *Audit Execution, Evidence & Interviewing*
   - *Findings, Nonconformity Grading & Reporting*
   - *Certification Audits, Follow-up & Audit Leadership*

©2026 Certaining, Inc. All rights reserved.

Objective of the Certification

- **Validate lead auditor competence:** the ability to plan, lead, and report audits of an Information Security Management System (ISMS) against ISO/IEC 27001.
- **Deepen standards expertise:** apply the ISO/IEC 27001:2022 requirements and Annex A controls with the judgment needed to lead an audit.
- **Manage audit programs:** establish and manage an audit program, applying ISO 19011 and ISO/IEC 27007.
- **Lead audit teams:** assign roles, guide auditors, and manage team dynamics, conflicts, and time.
- **Conduct first-, second-, and third-party audits:** understand the differences, including certification audit stages, surveillance, and recertification.
- **Evaluate evidence and risk:** reach sound conclusions through interviews, observation, sampling, and review of risk processes.
- **Grade findings and report:** classify nonconformities, write clear findings, and present balanced conclusions.
- **Drive follow-up:** evaluate corrective action plans and verify their effectiveness.
- **Uphold ethics and impartiality:** apply independence, confidentiality, and professional skepticism, and manage conflicts of interest.
- **Create a foundation for senior roles:** prepare for audit program management, certification body, and executive information security responsibilities.

©2026 Certaining, Inc. All rights reserved.

Core Competencies — CSLA™ (ISO/IEC 27001: Information Security Lead Auditor)



©2026 Certaining, Inc. All rights reserved.

- **Advanced ISMS knowledge:** interpret clauses 4–10 in depth and assess how well an ISMS achieves its intended outcomes.
- **Controls and risk assessment:** evaluate the Annex A controls, the Statement of Applicability (SoA), and the risk assessment and treatment process.
- **Audit program management:** define program objectives, manage risks to the program, and monitor and improve it.
- **Audit leadership:** plan the audit, brief the audit team, and manage the audit from opening to closing meeting.
- **Evidence evaluation:** gather, verify, and evaluate objective evidence, and recognize indicators of weak or misleading information.
- **Interviewing and communication:** conduct effective interviews, handle difficult situations, and communicate findings with tact.
- **Findings and reporting:** grade nonconformities, write accurate audit reports, and present results at the closing meeting.
- **Certification audit process:** apply the stages of a certification cycle, including stage 1, stage 2, surveillance, and recertification.
- **Follow-up and closure:** evaluate corrective action plans, verify effectiveness, and support decisions on audit outcomes.
- **Professional conduct:** maintain impartiality, confidentiality, and professional skepticism, and manage conflicts of interest.

©2026 Certaining, Inc. All rights reserved.

Who Should Take This Certification

- Experienced internal auditors who want to lead ISMS audits and audit teams.
- Information security, compliance, and risk professionals moving into audit leadership.
- Auditors who plan to work in third-party certification or supplier audit roles.
- Audit program managers and heads of internal audit or compliance functions.
- ISMS managers and consultants who support organizations through ISO/IEC 27001 certification.
- Professionals who have completed an auditor-level credential such as CSIA™ and want to advance.

Exam Information

Exam Name	ISO/IEC 27001: Information Security Lead Auditor
Exam Code	CSLA™
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 & ISO/IEC 27001:2022 Requirements (Advanced)	20%
Annex A Controls & Risk Management for Auditors	15%
Audit Program Management & Principles	15%
Audit Planning & Preparation	10%
Audit Execution, Evidence & Interviewing	15%
Findings, Nonconformity Grading & Reporting	10%
Certification Audits, Follow-up & Audit Leadership	15%
Total	**100%**

©2026 Certaining, Inc. All rights reserved.

Topics to Prepare — CSLA™ (ISO/IEC 27001: Information Security Lead Auditor)

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

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

- **Clauses 4–10 in depth:** context, leadership, planning, support, operation, performance evaluation, and improvement.
- **ISMS scope and boundaries:** interfaces, dependencies, and outsourced processes.
- **Leadership and policy:** assessing top management commitment and the effectiveness of the information security policy.
- **Objectives and change planning:** how objectives are set, measured, and kept current.
- **Performance evaluation:** monitoring, internal audit, and management review, and how to judge their effectiveness.
- **Improvement:** nonconformity handling, corrective action, and continual improvement.

2. Annex A Controls & Risk Management for Auditors (15%)

- **Control structure:** the 93 controls across organizational, people, physical, and technological themes.
- **Auditing controls:** how to check design and operating effectiveness.
- **Risk assessment and treatment:** methodology, risk owners, residual risk, and risk acceptance.
- **Statement of Applicability (SoA):** testing justifications, inclusions, and exclusions.
- **Link between risks and controls:** consistency of the risk register, treatment plan, and SoA.
- **Related guidance:** ISO/IEC 27002 for controls and ISO/IEC 27005 for risk management.

3. Audit Program Management & Principles (15%)

- **Principles of auditing:** integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach.
- **Audit program:** objectives, scope, risks, resources, procedures, and monitoring.
- **Auditor competence and evaluation:** selecting, evaluating, and developing auditors.
- **Audit types:** first-party, second-party, and third-party audits.
- **Standards for auditing:** ISO 19011 and ISO/IEC 27007.
- **Impartiality and conflicts of interest:** protecting the credibility of audit results.

©2026 Certaining, Inc. All rights reserved.

4. Audit Planning & Preparation (10%)

- **Initiating the audit:** objectives, scope, criteria, and contact with the auditee.
- **Feasibility and resources:** time, team composition, and technical expertise.
- **Document review:** reviewing the ISMS documentation before the audit.
- **Audit plan:** scheduling activities, assigning roles, and sampling plans.
- **Working documents:** checklists, forms, and sampling strategies.

5. Audit Execution, Evidence & Interviewing (15%)

- **Opening meeting:** confirming the plan, communication, and logistics.
- **Collecting evidence:** interviews, observation, and examination of records.
- **Interviewing techniques:** open and closed questions, active listening, and handling resistance.
- **Verifying information:** corroborating statements with objective evidence.
- **Audit team management:** guidance, time management, and handling conflicts.
- **Professional skepticism:** recognizing risks of incomplete or misleading evidence.

6. Findings, Nonconformity Grading & Reporting (10%)

- **Audit findings:** conformity, nonconformity, and opportunities for improvement.
- **Grading nonconformities:** major and minor, and how severity and systemic impact are judged.
- **Writing a finding:** requirement, evidence, and statement of nonconformity.
- **Audit conclusions:** drawing conclusions from the findings against the audit objectives.
- **Closing meeting and report:** presenting results, handling disagreements, and issuing the report.

7. Certification Audits, Follow-up & Audit Leadership (15%)

- **Certification cycle:** stage 1, stage 2, surveillance, and recertification audits.
- **Certification body requirements:** ISO/IEC 17021-1 and ISO/IEC 27006.
- **Special audits:** scope extensions, short-notice audits, and suspended or withdrawn certification.
- **Corrective action plans:** evaluating root cause analysis and the proposed actions.
- **Follow-up and verification:** confirming the implementation and effectiveness of corrective action.
- **Leading with integrity:** decision-making, confidentiality, and professional conduct.

©2026 Certaining, Inc. All rights reserved.