CERTIFICATION SYLLABUS

ISO/IEC 27001: Information Security Internal Auditor

Exam Code: CSIA™



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
   - *Information Security & ISMS Fundamentals*
   - *ISO/IEC 27001:2022 Requirements (Clauses 4–10)*
   - *Annex A Controls & Implementation Guidance*
   - *Information Security Risk Assessment & Treatment*
   - *Audit Principles, Ethics & Auditor Roles*
   - *Audit Planning, Execution & Evidence Gathering*
   - *Audit Reporting, Nonconformities & Follow-up*

©2026 Certaining, Inc. All rights reserved.

Objective of the Certification

- **Validate internal audit competence for ISMS:** the ability to plan and perform internal audits of an Information Security Management System (ISMS) against ISO/IEC 27001.
- **Build knowledge of ISO/IEC 27001:2022:** the requirements in clauses 4–10 and the Annex A controls.
- **Apply audit principles:** use the guidance in ISO 19011 (auditing management systems) and ISO/IEC 27007 (ISMS auditing).
- **Assess risk-based controls:** evaluate how the organization identifies, assesses, and treats information security risks.
- **Gather and evaluate objective evidence:** use interviews, document review, and observation to reach sound audit conclusions.
- **Write clear findings:** raise and classify nonconformities and opportunities for improvement.
- **Verify corrective action:** confirm that the root cause is addressed and that actions are effective.
- **Support certification readiness:** help the organization prepare for external certification and surveillance audits.
- **Uphold professional conduct:** apply objectivity, independence, confidentiality, and integrity.
- **Create a foundation for advanced paths:** a basis for Lead Auditor, Risk Manager, and executive-level information security credentials.

©2026 Certaining, Inc. All rights reserved.

Core Competencies — CSIA™ (ISO/IEC 27001: Information Security Internal Auditor)



©2026 Certaining, Inc. All rights reserved.

- **ISMS understanding:** explain the purpose, scope, and structure of an ISMS and how ISO/IEC 27001 is organized.
- **Requirements interpretation:** interpret clauses 4–10, from context and leadership to performance evaluation and improvement.
- **Controls knowledge:** understand the Annex A control themes (organizational, people, physical, technological) and audit their implementation.
- **Risk-based auditing:** review risk assessment and treatment, the Statement of Applicability (SoA), and risk owners' decisions.
- **Audit planning:** define audit scope, criteria, and objectives, and prepare an audit plan and checklists.
- **Audit execution:** conduct opening and closing meetings, interview auditees, and collect and verify evidence.
- **Findings and reporting:** write accurate findings, classify nonconformities, and prepare a clear audit report.
- **Follow-up:** evaluate corrective actions and verify their effectiveness.
- **Professional ethics:** maintain independence, impartiality, and confidentiality throughout the audit.

©2026 Certaining, Inc. All rights reserved.

Who Should Take This Certification

- Information security, IT, and compliance professionals who will audit an ISMS.
- Internal auditors and quality or risk auditors expanding into information security.
- ISMS coordinators, security officers, and managers responsible for ISO/IEC 27001 compliance.
- Consultants who support organizations preparing for ISO/IEC 27001 certification.
- Governance, risk, and compliance (GRC) professionals, and IT and data protection specialists.
- Graduates and early-career professionals aiming for a career in information security auditing.

Exam Information

Exam Name	ISO/IEC 27001: Information Security Internal Auditor
Exam Code	CSIA™
Exam Format	Multiple Choice Questions (MCQ), including scenario-based questions
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

©2026 Certaining, Inc. All rights reserved.

Examination Domain & Weightage

Domain	Weightage
Information Security & ISMS Fundamentals	15%
ISO/IEC 27001:2022 Requirements (Clauses 4–10)	25%
Annex A Controls & Implementation Guidance	20%
Information Security Risk Assessment & Treatment	10%
Audit Principles, Ethics & Auditor Roles	15%
Audit Planning, Execution & Evidence Gathering	10%
Audit Reporting, Nonconformities & Follow-up	5%
Total	**100%**

©2026 Certaining, Inc. All rights reserved.

Topics to Prepare — CSIA™ (ISO/IEC 27001: Information Security Internal Auditor)

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

1. Information Security & ISMS Fundamentals (15%)

- **Core concepts:** confidentiality, integrity, availability, assets, threats, vulnerabilities, and risk.
- **ISMS purpose and benefits:** a systematic, risk-based approach to protecting information.
- **Standards family:** the ISO/IEC 27000 family, including ISO/IEC 27001 and ISO/IEC 27002.
- **Management system structure:** the common high-level structure and the Plan-Do-Check-Act approach.
- **Key terms:** scope, policy, objectives, interested parties, and documented information.

2. ISO/IEC 27001:2022 Requirements (Clauses 4–10) (25%)

- **Clause 4, Context:** internal and external issues, interested parties, and ISMS scope.
- **Clause 5, Leadership:** commitment, information security policy, and roles and responsibilities.
- **Clause 6, Planning:** risks and opportunities, risk assessment and treatment, objectives, and change planning.
- **Clause 7, Support:** resources, competence, awareness, communication, and documented information.
- **Clause 8, Operation:** operational planning, risk assessment, and risk treatment in practice.
- **Clause 9, Performance evaluation:** monitoring, internal audit, and management review.
- **Clause 10, Improvement:** nonconformity, corrective action, and continual improvement.

3. Annex A Controls & Implementation Guidance (20%)

- **Control structure:** the 93 controls grouped into organizational, people, physical, and technological themes.
- **Organizational controls:** policies, roles, supplier relationships, incident management, and continuity.
- **People controls:** screening, terms of employment, awareness, and remote working.
- **Physical controls:** secure areas, equipment protection, and clear desk and screen.
- **Technological controls:** access control, cryptography, logging, vulnerability management, and secure development.
- **Statement of Applicability (SoA):** justification for including or excluding controls.

©2026 Certaining, Inc. All rights reserved.

- **Auditing controls:** how to verify that a control is implemented and effective.

4. Information Security Risk Assessment & Treatment (10%)

- **Risk methodology:** identification, analysis, and evaluation of information security risks.
- **Risk treatment options:** modify, retain, avoid, and share.
- **Risk acceptance:** acceptance criteria and risk owner approval.
- **Residual risk:** evaluating what remains after treatment.
- **Auditing risk processes:** checking consistency between the risk register, SoA, and treatment plan.

5. Audit Principles, Ethics & Auditor Roles (15%)

- **Audit types:** first-party (internal), second-party, and third-party audits.
- **Audit principles:** integrity, fair presentation, due professional care, confidentiality, independence, and an evidence-based approach.
- **Auditor competence:** knowledge, skills, and ongoing development.
- **Roles and responsibilities:** audit program manager, audit team leader, auditor, and auditee.
- **Related standards:** ISO 19011 and ISO/IEC 27007.

6. Audit Planning, Execution & Evidence Gathering (10%)

- **Audit program and plan:** objectives, scope, criteria, schedule, and resources.
- **Audit preparation:** document review, checklists, and sampling.
- **Opening meeting:** confirming scope, plan, and communication.
- **Evidence gathering:** interviews, observation, and examination of records.
- **Verification:** evaluating audit evidence against criteria to form conclusions.

7. Audit Reporting, Nonconformities & Follow-up (5%)

- **Audit findings:** conformity, nonconformity, and opportunities for improvement.
- **Classifying nonconformities:** major and minor, and how severity is judged.
- **Closing meeting and report:** presenting results and agreeing on next steps.
- **Corrective action:** root cause analysis and effectiveness review.
- **Audit follow-up and closure:** verifying completion and feeding results into management review.

©2026 Certaining, Inc. All rights reserved.