



Global AI
Certification Council



ISO/IEC 27001

LEAD IMPLEMENTER CERTIFICATION

Examination Content Outline
v1.2 | 11 June 2026

Global AI Certification Council
(GAICC)

GAICC-ECO-27001-LI-001

Examination Content Outline

GAICC Certified ISO/IEC 27001 Lead Implementer

Standard: ISO/IEC 27001:2022 (with ISO/IEC 27002/27003/27005 guidance)

Accreditation reference: ISO/IEC 17024:2026 (Third Edition) · IAS AC474 (June 2024) · IAF MD25

Contents

1 Purpose of this Examination Content Outline	3
2 Target candidate and competence	3
3 Eligibility and formal training	3
4 Domains and weightings	4
5 Domains, tasks and enablers	4
Domain I — ISMS Governance, Context and Leadership (25%)	4
Domain II — ISMS Implementation and Operational Control (40%)	5
Domain III — Performance Evaluation, Audit Readiness and Continual Improvement (20%)	5
Domain IV — Information Security Culture, Third-Party Risk and AI-Era ISMS (15%)	5
6 Examination structure	6
7 Benchmark note	6
8 Fees & Pricing	6

This Examination Content Outline is the authority for item writing, blueprinting and the modified-Angoff standard-setting study for the GAICC ISO/IEC 27001 Lead Implementer examination, and is read with the Structural Reference & Control Map (GAICC-REF-27001-001).

1 Purpose of this Examination Content Outline

This ECO defines what the GAICC ISO/IEC 27001 Lead Implementer examination assesses: the competence to lead an ISMS implementation programme to ISO/IEC 27001:2022. It refines version 1.0 against the standard, the ISO/IEC 27002/27003/27005 guidance and comparable benchmark schemes, and is read with the Structural Reference & Control Map (GAICC-REF-27001-001).

This document is an original GAICC reference compiled from publicly available information and verified for accuracy against GAICC's licensed copy of the standard. It lists clause and control references and titles only; it does not reproduce the normative text of ISO/IEC 27001:2022, which must be obtained from ISO or an authorised reseller.

2 Target candidate and competence

The candidate can plan, build and operate an ISMS: scoping, risk assessment and treatment, the Statement of Applicability, Annex A control implementation, operational procedures, performance evaluation and audit readiness — at lead-implementer level.

3 Eligibility and formal training

GAICC certifications are developed in alignment with ISO/IEC 17024. Candidates for the GAICC ISO/IEC 27001 Lead Implementer certification must meet the formal-training requirement below. Training contact hours are counted as Continuing Professional Development (CPD) hours.

Educational background	Professional experience	Formal training requirement
Open entry. Prior ISO/IEC 27001 Foundation knowledge is recommended.	Relevant experience recommended but not mandatory.	Completion of at least 32 contact hours of structured ISO/IEC 27001 implementation training delivered by GAICC-authorised providers or equivalent recognised institutions. Students can also fulfil this requirement by completing GAICC self-paced courses.

Training may be delivered online or in person and must be evidenced by a certificate of completion stating the provider, programme title, duration (contact hours) and completion date. Applications may be selected for audit to verify training documentation.

4 Domains and weightings

#	Domain	Weight	Items (of 60)
I	ISMS Governance, Context and Leadership	25%	15
II	ISMS Implementation and Operational Control	40%	24
III	Performance Evaluation, Audit Readiness and Continual Improvement	20%	12
IV	Information Security Culture, Third-Party Risk and AI-Era ISMS	15%	9
Total		100%	60

5 Domains, tasks and enablers

Each domain below sets out the tasks a Lead Implementer candidate is expected to perform and the illustrative enablers from which examination items are drawn. Enablers are indicative, not exhaustive.

Domain I ISMS Governance, Context and Leadership

25%

Task	Illustrative enablers / examples
Establish context and ISMS scope (Clause 4).	Internal / external issues including climate relevance; interested parties; boundaries and interfaces; scope statement.
Secure leadership and define the policy (Clause 5).	Top-management commitment; information security policy; roles, responsibilities and authorities.
Set objectives and plan the programme (Clause 6.2, 6.3).	Measurable security objectives; implementation plan; planning of changes; resourcing.
Establish governance and documented information (Clause 7).	Competence and awareness; communication plan; document and records control.

Domain II ISMS Implementation and Operational Control

40%

Task	Illustrative enablers / examples
Conduct the information security risk assessment (Clause 6.1.2, 8.2).	Risk criteria; asset / threat / vulnerability or scenario approach; risk owners; ISO/IEC 27005 alignment.
Design and execute risk treatment (Clause 6.1.3, 8.3).	Treatment options; control selection from Annex A; residual risk acceptance; risk treatment plan.
Produce and maintain the Statement of Applicability.	Inclusion / exclusion justification; mapping to the 93 Annex A controls; review on change.
Implement Annex A controls across the four themes.	Organizational, People, Physical and Technological controls; evidence patterns for each.
Operate the ISMS (Clause 8.1).	Operational procedures; change control; supplier and cloud security operations.

Domain III Performance Evaluation, Audit Readiness and Continual Improvement

20%

Task	Illustrative enablers / examples
Monitor, measure, analyse and evaluate (Clause 9.1).	Metrics and KPIs; effectiveness of controls; ISO/IEC 27004 alignment.
Run the internal audit programme (Clause 9.2).	Programme, scope, auditor competence and independence; findings.
Conduct management review (Clause 9.3).	Inputs, outputs, decisions, resources.
Drive improvement (Clause 10).	Nonconformity and corrective action; continual improvement; readiness for certification audit.

Domain IV Information Security Culture, Third-Party Risk and AI-Era ISMS

15%

Task	Illustrative enablers / examples
Build security culture and awareness.	Training, behaviour, security event reporting (A.6.x); culture beyond compliance.
Manage third-party, cloud and supply-chain risk.	Supplier relationships and agreements (A.5.19–A.5.23); ICT supply chain; cloud services.
Integrate privacy and adjacent regimes.	PII protection (A.5.34); legal / regulatory requirements; integration with ISO/IEC 27701 and 9001.
Address the AI-era ISMS and the 27001–	AI-related information-security risks; integrating the ISMS

6 Examination structure

Attribute	Detail
Number of items	60 scored items (45 single-answer MCQ + 15 multi-answer)
Format	MCQ (4 options A–D); multi-answer (5 options A–E, select all that apply, no partial credit)
Duration	90 minutes
Delivery	Online AI-proctored or test-centre; closed book; randomised
Pass mark	70% scaled (provisional; to be confirmed by a modified-Angoff study)
Cognitive level	Predominantly Apply / Analyse / Evaluate; scenario-based

7 Benchmark note

Comparable Lead Implementer schemes organise the same body of knowledge into seven domains — fundamentals, ISMS requirements, planning, implementation, monitoring, continual improvement and certification-audit preparation. GAICC consolidates these into four domains weighted 25/40/20/15, aligned with the nine-module GAICC course and the GAICC ISO/IEC 42001 family, and adds explicit coverage of security culture, third-party / cloud risk and the AI-era ISMS.

8 Fees & Pricing

Examination, membership and renewal fees are published in the applicable GAICC Candidate Handbook and on the GAICC website (www.gaicc.org). To maintain a single source of truth, fee amounts are not reproduced in this Examination Content Outline.

About the Global AI Certification Council

The Global AI Certification Council (GAICC) develops vendor-neutral, role-anchored professional credentials, developed in alignment with ISO/IEC 17024 and maintained through transparent psychometric and continuing-education processes.

gaicc.org · support@gaicc.org



Global AI
Certification Council

ISO/IEC 27001

LEAD IMPLEMENTER CERTIFICATION

Competence to plan, build and operate an information security management system to ISO/IEC 27001:2022 — at lead-implementer level.

gaicc.org · support@gaicc.org