Global AI Certification Council

ISO/IEC 27001 Foundation — Examination Content Outline

GAICC Certified ISO/IEC 27001 Foundation

Field	Detail
Document code	GAICC-ECO-27001-F-001
Version	v1.1 DRAFT
Issued	11 June 2026
Standard	ISO/IEC 27001:2022 (with ISO/IEC 27000 vocabulary and ISO/IEC 27002:2022 controls)
Accreditation reference	ISO/IEC 17024:2026 (Third Edition) · IAS AC474 (June 2024) · IAF MD25

GAICC · Global AI Certification Council Limited · NZ Company 9371200 · Auckland, New Zealand
Directors: Dr Faiz Rasool · Latha Karthigaa Murugesan

CONFIDENTIAL — prepared for IAS accreditation submission

Document control

Field	Detail
Document title	ISO/IEC 27001 Foundation — Examination Content Outline
Document code	GAICC-ECO-27001-F-001
Version	v1.1 DRAFT
Status	First draft — for IAS submission
Issue date	11 June 2026
Author	Dr Faiz Rasool, CEO and Co-Director
Owner	GAICC Quality Manager (acting: Dr Faiz Rasool)
Approver	GAICC Board of Directors
Classification	Confidential — IAS accreditation submission
Next review	Annually or upon material change
Accreditation reference	ISO/IEC 17024:2026 · IAS AC474 (June 2024) · IAF MD25

Version history

Version	Date	Author	Summary of change
v1.0 DRAFT	11 June 2026	F. Rasool	Initial draft for IAS submission.
v1.1 DRAFT	18 June 2026	F. Rasool	Added Section 3 (Eligibility and formal training): 16 contact-hours training requirement. Subsequent sections renumbered.

Approval

Role	Name	Signature	Date
Prepared by	Dr Faiz Rasool, CEO and Co-Director		11 June 2026
Reviewed by	SME Panel Chair		
Approved by	GAICC Board		

Contents

1 Purpose of this Examination Content Outline

This Examination Content Outline (ECO) defines what the GAICC ISO/IEC 27001 Foundation examination assesses. It is the authority for item writing, blueprinting and the modified-Angoff standard-setting study, 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 Foundation certification confirms awareness-level competence: understanding the purpose, structure and core concepts of ISO/IEC 27001 and an ISMS. It suits newcomers to information security governance and is a stepping stone to the Lead Implementer and Lead Auditor pathways. It does not assess the ability to implement or audit an ISMS.

3 Eligibility and formal training

GAICC certifications are developed in alignment with ISO/IEC 17024. Candidates for the GAICC ISO/IEC 27001 Foundation 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 — no specific prerequisite.	Not required.	Completion of at least 16 contact hours of structured ISO/IEC 27001 Foundation 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 40)
I	Information Security & ISMS Fundamentals	40%	16
II	ISMS Requirements — Clauses 4 to 10	40%	16
III	Annex A Controls & Certification Awareness	20%	8
	Total	100%	40

5 Domains, tasks and enablers

Domain I — Information Security & ISMS Fundamentals (40%)

Task	Illustrative enablers / examples
Explain core information-security concepts.	Confidentiality, integrity, availability (CIA); authenticity, non-repudiation; assets, threats, vulnerabilities, risk, controls.
Describe what an ISMS is and why organisations adopt it.	Risk-based management system; drivers and benefits; interested parties.
Outline the purpose, scope and structure of ISO/IEC 27001.	Clauses 1–3 vs 4–10; Annex SL high-level structure; Annex A.
Recognise the ISO/IEC 27000 family and key relationships.	27000 vocabulary; 27002 controls guidance; 27003, 27005; relationship to ISO 9001 and ISO/IEC 42001.
Explain the management-system and PDCA model.	Plan–Do–Check–Act; continual improvement; certification vs accreditation at awareness level.

Domain II — ISMS Requirements: Clauses 4 to 10 (40%)

Task	Illustrative enablers / examples
Describe context and scope (Clause 4).	Internal/external issues (incl. climate-change relevance); interested parties; ISMS scope.
Describe leadership and policy (Clause 5).	Top-management commitment; information security policy; roles, responsibilities and authorities.
Explain planning and risk (Clause 6).	Risk assessment and treatment; Statement of Applicability; security objectives; planning of changes.
Identify support requirements (Clause 7).	Resources, competence, awareness, communication, documented information.

Task	Illustrative enablers / examples
Describe operation (Clause 8).	Operational planning and control; performing risk assessment and treatment.
Describe performance evaluation (Clause 9).	Monitoring and measurement; internal audit; management review.
Describe improvement (Clause 10).	Continual improvement; nonconformity and corrective action.

Domain III — Annex A Controls & Certification Awareness (20%)

Task	Illustrative enablers / examples
Identify the four Annex A control themes.	Organizational (A.5), People (A.6), Physical (A.7), Technological (A.8); 93 controls in total.
Recognise common controls and their purpose.	Examples such as access control, classification, supplier and cloud security, incident management, backup, cryptography.
Explain the Statement of Applicability.	Selection, justification of inclusion/exclusion, link to risk treatment.
Outline the certification lifecycle at awareness level.	Stage 1 and Stage 2 audits, surveillance, recertification; roles in an ISMS.

6 Examination structure

Attribute	Detail
Number of items	40 scored items
Format	Single-answer multiple choice (4 options A–D)
Duration	60 minutes
Delivery	Online proctored or test-centre; closed book
Pass mark	70% (provisional; to be confirmed by a modified-Angoff study)
Cognitive level	Predominantly Remember / Understand, with some Apply

7 Benchmark note

The Foundation scope aligns with comparable Foundation certifications (e.g. PECB and APMG ISO/IEC 27001 Foundation), which test information-security and ISMS concepts, the structure of the standard, the risk and PDCA model, and Annex A awareness. GAICC consolidates these into three domains weighted 40/40/20, consistent with the GAICC ISO/IEC 42001 Foundation.