Global AI Certification Council

GAICC

CERTIFIED AI LAW & COMPLIANCE PROFESSIONAL CERTIFICATION

Examination Content Outline – March 2026

Global AI Certification Council **(GAICC)**

Examination Content Outline

March 2026

Published by: Global AI Certification Council (GAICC)

3900 Westerre Pkwy, Richmond,
VA 23233, USA

Level 2, 697 Collins Street, Melbourne
VIC 3008, Australia

Level 3, 21 Putney Way Manukau,
Auckland, New Zealand 2104

Contents

Introduction

The Global AI Certification Council (GAICC) offers a professional certification for legal and compliance professionals known as the **GAICC Certified AI Law & Compliance Professional (GAICC-CAILCP)**.

This credential validates practitioner-level competence in AI governance, multi-jurisdictional regulatory compliance, technical risk assessment, and the practical application of AI tools within legal and compliance practice. The certification is designed for lawyers, compliance officers, data protection officers, legal operations professionals, GRC professionals, and in-house counsel operating in a global regulatory landscape — including emerging AGI risk.

GAICC's certification development process follows globally recognised best practices for professional credentialing, including those defined in the ISO/IEC 17024: Conformity Assessment – General Requirements for Bodies Operating Certification of Persons.
A key feature of ISO/IEC 17024 compliance is the use of a competency-based and criterion-referenced approach to exam development. GAICC conducts global practice analyses and job-task studies to ensure the CAILCP examination reflects real-world roles and responsibilities of legal and compliance professionals governing AI systems across diverse industries and jurisdictions.

This Examination Content Outline (ECO) defines:

- The domains of competence required of a certified AI Law & Compliance Professional,
- The tasks and enablers within each domain that demonstrate capability, and
- The relative weight of each domain in the overall assessment.

The CAILCP exam evaluates knowledge, skills, and abilities across the full spectrum of AI law and compliance — covering global regulatory frameworks, technical risk architecture, risk classification, practical legal AI skills, liability and enforcement, governance structures, emerging AGI governance, and ethics, bias, and fairness.
All questions are scenario-based, requiring the application of knowledge to realistic, multi-dimensional situations rather than definition recall. Questions are developed and validated by experienced subject-matter experts drawn from legal practice, government, academia, and industry to ensure relevance, fairness, and psychometric validity.

This document therefore serves as both a blueprint for the CAILCP examination and a professional development guide for individuals and organisations seeking to strengthen competence in AI law, governance, and compliance.

Exam Content Outline

The **GAICC Certified AI Law & Compliance Professional (GAICC-CAILCP)** examination measures the candidate's ability to apply AI law, governance, and compliance principles across realistic, multi-jurisdictional scenarios spanning regulatory analysis, technical risk assessment, liability mapping, practical legal AI skills, and ethical governance.

The outline below identifies the major domains of competence and the relative percentage of questions that appear on the examination. Each domain encompasses a set of tasks and enablers that reflect how AI law and compliance responsibilities are performed in practice.

Domains and Weightings

Domain	Description	Approximate Weight on Exam
I. Global AI Regulatory Landscape	Multi-jurisdictional regulatory analysis, extraterritorial exposure mapping, and cross-border compliance.	18%
II. Governance-Technical AI Risk	Translating AI technical failure modes into legal exposure categories and governance risk frameworks.	18%
III. Risk Classification & Compliance	Applying risk classification across multiple frameworks and designing proportional governance controls.	15%

IV. AI for Lawyers Practical Skills	Using AI tools for legal practice, drafting AI policies and clauses, and conducting AI risk assessments.	14%
V. Liability & Enforcement	Analysing AI liability theories, executive accountability, insurance, and enforcement trends.	10%
VI. Policy & Governance Structures	Designing AI governance frameworks, risk registers, vendor oversight, and crisis incident response.	10%
VII. AGI & Future Governance	Evaluating governance frameworks for advanced AI, alignment risk, and strategic executive advisory.	10%
VIII. Ethics, Bias & Fairness	Applying fairness frameworks, bias auditing, and operationalising ethical AI governance.	5%
Total		100%

Domain, Task and Enablers

In the GAICC-CAILCP framework, a domain represents a major area of professional competence required to govern AI systems from a legal and compliance perspective.

Each domain contains a set of tasks — the key responsibilities of the professional — and enablers — illustrative examples that demonstrate how these responsibilities are carried out in practice. Enablers are not exhaustive; they simply highlight typical evidence or actions that reflect the expected level of capability.

Domain I – Global AI Regulatory Landscape (≈ 18%)

Purpose:
To conduct multi-jurisdictional AI regulatory analysis, map extraterritorial exposure, and identify compliance priorities across global frameworks.

Task	Illustrative Enablers / Examples
1. Conduct extraterritorial exposure mapping for multinational AI deployments.	Jurisdiction identification matrices, regulatory overlap analyses, and compliance priority assessments across EU, US, UK, APAC, Middle East, and China frameworks.
2. Analyse and apply the EU AI Act risk classification system including boundary cases.	Risk tier determinations, prohibited practice assessments, high-risk obligation checklists, and GPAI compliance analyses.

3. Evaluate jurisdiction-specific enforcement risks and regulatory priorities.	FTC enforcement doctrine analysis, SEC/FINRA AI guidance application, EEOC algorithmic scrutiny assessments, and state-level compliance mapping (Colorado AI Act, NYC Local Law 144).
4. Identify regulatory conflicts and harmonisation opportunities across jurisdictions.	Cross-border conflict analyses, framework alignment charts, and regulatory harmonisation reports.
5. Apply sector-specific and regional AI governance frameworks.	UK pro-innovation model assessments, Singapore Model AI Governance mapping, China regulatory measure analyses, and ISO/IEC 42001/ NIST AI RMF integration plans.

Domain II – Governance-Technical AI Risk (≈ 18%)

Purpose:
To translate AI technical failure modes into concrete legal exposure categories and apply a structured technical-legal risk mapping framework.

Task	Illustrative Enablers / Examples
1. Translate AI technical failure modes into legal exposure categories.	Technical-legal risk mapping matrices covering product liability, consumer protection, anti-discrimination, data protection, professional negligence, IP, and securities exposure.
2. Assess foundation model architecture decisions for governance risk implications.	Architecture risk assessments, training data audits, model lifecycle compliance reviews, and RAG system governance evaluations.
3. Evaluate AI vendor technical claims against governance requirements.	Vendor due diligence frameworks, API dependency assessments, model versioning risk analyses, and supply chain provenance reviews.
4. Apply red teaming and safety testing concepts to governance oversight.	Adversarial testing evaluations, jailbreaking risk assessments, prompt injection governance implications, and safety benchmark analyses.
5. Assess agentic AI systems for delegation accountability and autonomous decision risk.	Autonomous decision chain analyses, tool-use risk mappings, delegation authority frameworks, and human oversight gap assessments.

Domain III – Risk Classification & Compliance (≈ 15%)

Purpose:
To apply risk classification frameworks across multiple jurisdictions and design proportional governance controls that scale with risk level.

Task	Illustrative Enablers / Examples
1. Apply EU AI Act high-risk classification to real-world AI systems including edge cases.	Conformity assessment plans, technical documentation templates, quality management frameworks, and post-market monitoring procedures.
2. Map AI systems to compliance obligations across multiple jurisdictions simultaneously.	Multi-jurisdictional compliance matrices, global equivalence mapping charts, and cross-framework obligation analyses.
3. Design proportional governance controls that scale with risk level.	Risk-proportionate control frameworks, compliance-by-design methodologies, and AI impact assessment templates (FRIA, AIA, sector-specific).
4. Prepare risk documentation to regulatory standards.	Risk documentation packages, regulatory submission templates, and evidence portfolios meeting EU, US, UK, and APAC expectations.

Domain IV – AI for Lawyers Practical Skills (≈ 14%)

Purpose:
To use AI tools effectively for legal practice while maintaining professional standards, and to draft enforceable AI governance policies and contractual clauses.

Task	Illustrative Enablers / Examples
1. Use AI tools effectively for legal research, drafting, and review while maintaining professional standards.	Prompt engineering for legal tasks, legal drafting augmentation workflows, AI contract review processes, and hallucination control verification protocols.
2. Implement confidentiality and privilege protections when using AI tools.	Data sanitisation procedures, privilege preservation frameworks, vendor contractual clauses, and enterprise vs consumer AI risk policies.
3. Draft enforceable AI governance policies and contractual clauses.	AI acceptable use policies, vendor due diligence clauses, governance charters, model documentation requirements, incident response clauses, and AI representations and warranties.
4. Conduct comprehensive AI risk assessments following structured methodology.	Risk assessment summary memos, legal exposure vector identification, framework-specific risk classification, and proportional control recommendations.

Domain V – Liability & Enforcement (≈ 10%)

Purpose:
To analyse evolving AI liability theories, assess executive accountability exposure, and evaluate enforcement trends across jurisdictions.

Task	Illustrative Enablers / Examples
1. Analyse AI liability theories and their application to different AI system types.	Civil liability model assessments (negligence, strict liability, product liability), EU AI Liability Directive analysis, and algorithmic negligence standard of care evaluations.
2. Assess executive and officer liability exposure for AI governance failures.	D&O exposure assessments, personal liability analyses, officer due diligence checklists, and board accountability frameworks.
3. Evaluate insurance and risk transfer options for AI-related liabilities.	Cyber policy gap analyses, professional indemnity reviews, AI-specific coverage assessments, and risk transfer strategy documents.
4. Analyse enforcement case trends across regulatory jurisdictions.	FTC action analyses, ICO enforcement reviews, EU AI Office signal assessments, and cross-jurisdictional enforcement comparison reports.

Domain VI – Policy & Governance Structures (≈ 10%)

Purpose:
To design AI governance frameworks, build risk registers, structure vendor oversight, and execute crisis incident response.

Task	Illustrative Enablers / Examples
1. Design AI governance frameworks appropriate to organisational size, sector, and risk profile.	Governance committee charters, RACI matrices, three lines of defence models, and AI policy architecture documents.
2. Build AI risk registers and incident escalation protocols.	Risk register templates, scoring methodologies, escalation trigger definitions, severity classification frameworks, and regulatory reporting procedures.
3. Structure AI vendor oversight programmes.	Due diligence checklists, ongoing monitoring frameworks, contractual control templates, and exit strategy plans.
4. Execute structured AI incident response and crisis governance.	Incident response playbooks, containment and disclosure protocols, regulatory notification procedures, litigation risk mitigation plans, and post-incident review processes.

Domain VII – AGI & Future Governance (≈ 10%)

Purpose:
To evaluate governance frameworks for increasingly autonomous AI systems, analyse alignment risk, and advise boards and executives on strategic AI governance.

Task	Illustrative Enablers / Examples
1. Evaluate governance frameworks for increasingly autonomous AI systems.	Agent autonomy spectrum analyses, containment vs control framework assessments, and governance gap analyses for advanced AI capabilities.
2. Analyse the alignment problem and its governance implications.	Alignment risk briefings, legal preparedness gap analyses, liability shift assessments, and AI rights and personhood risk-based framings.
3. Advise boards and executives on AI governance as a strategic function.	AI risk dashboards, governance maturity assessments, regulatory readiness scorecards, risk appetite definitions, and board reporting templates.
4. Assess international governance coordination for advanced AI systems.	Treaty framework analyses, compute governance assessments, safety standard comparisons, and dual-use AI policy evaluations.

Domain VIII – Ethics, Bias & Fairness (≈ 5%)

Purpose:
To apply fairness frameworks to AI system evaluation, assess bias risk across the AI lifecycle, and operationalise ethical AI governance.

Task	Illustrative Enablers / Examples
1. Apply fairness frameworks to AI system evaluation and governance.	Fairness definition analyses (demographic parity, equalised odds, individual fairness), tension mapping between competing fairness metrics, and fairness testing protocols.
2. Assess bias risk across the AI lifecycle.	Lifecycle bias audits (data collection, labelling, training, evaluation, deployment, monitoring), comparative regulatory analyses of algorithmic fairness approaches, and bias audit methodology reviews.
3. Operationalise ethical AI governance frameworks.	Ethics-to-governance translation plans, transparency and explainability obligation assessments, and responsible AI principle implementation roadmaps.

Cognitive Depth and Assessment Approach

The CAILCP examination evaluates three progressive cognitive levels across all domains:

- **Understanding:** Knowledge of global AI regulatory frameworks, technical risk concepts, and governance principles.
- **Application:** Practical use of regulatory analysis, risk mapping, policy drafting, and AI tools in real-world legal and compliance contexts.
- **Analysis and Evaluation:** Critical assessment of complex, multi-jurisdictional scenarios requiring legal judgement, ethical reasoning, and systemic governance thinking.

All 60 questions are scenario-based, requiring application of knowledge to realistic situations rather than definition recall. Scenarios test multi-domain competency: a single question may span regulatory, technical, and governance dimensions. The 90-minute duration allows approximately 90 seconds per question, enabling deeper analysis than standard multiple-choice examinations.

GAICC Eligibility Requirements

To qualify for the GAICC Certified AI Law & Compliance Professional (GAICC-CAILCP) certification, candidates must demonstrate appropriate education, professional experience, and structured training aligned with the competencies required for AI law and compliance practice.

All relevant AI governance, legal, or compliance experience must have been gained within the last eight (8) consecutive years before submitting the application.

Educational Background	Recommended Professional Experience	Formal Training Requirement
Secondary qualification (high school diploma, associate degree, or global equivalent)	Five years / 60 months of professional experience in legal practice, compliance, data protection, AI governance, or GRC.	Completion of the GAICC-CAILCP programme (24–26 contact hours) or equivalent GAICC-approved training.
Bachelor's degree (or global equivalent)	Three years / 36 months of experience in AI governance, legal technology, compliance, or data protection.	Completion of the GAICC-CAILCP programme (24–26 contact hours) or equivalent GAICC-approved training.

GAIIC Examination Information

Exam Structure

Component	Description
Total Questions	60
Format	Scenario-based multiple-choice questions delivered through the GAICC online testing platform.
Allotted Time	90 minutes.
Pass Mark	70%
Negative Marking	No
Question Style	All questions are scenario-based, requiring application of knowledge to multi-dimensional AI law and compliance situations.

Exam Delivery

The CAILCP examination is offered as online AI-proctored testing. All questions are randomly presented, and candidates cannot return to earlier sections once submitted. The exam platform includes a built-in timer, navigation panel, and flag-for-review feature.

Scoring and Results

- Each scored question is worth one mark.
- Examination results are reported immediately upon completion.
- Feedback is provided by domain (Global Regulatory, Governance-Technical Risk, Risk Classification, Practical Skills, Liability, Policy & Governance, AGI, Ethics).
- A minimum scaled score of 70% is required to pass.
- All scores are verified through GAICC's psychometric calibration process to maintain fairness and comparability across testing sessions.

Retake Policy

Each candidate is granted **one(1) free retake.** Paid retakes are permitted without limit, subject to payment of the applicable resit fee for each attempt.

GAICC-CAILCP Examination Fees

Membership Fees

Membership fee is 99 USD.

Examination Fees

Exam Fee – Member (USD)	Exam Fee – Non-Member (USD)
399	525

Notes:

- All fees are quoted in **USD** and may be subject to local taxes or bank-processing charges.
- **Membership is optional**, but members benefit from discounted exam fees and GAICC-exclusive resources.
- Payments may be made via **credit card** or **international bank transfer** through the **GAICC Certification Portal.**
- Renewal and re-examination fees are published annually on the GAICC official website ***(www.gaicc.org)***.

GAICC Certification Maintenance and Renewal Requirements

Certification Validity

The GAICC-CAILCP certification is valid for a period of three (3) years from the date of initial certification. To maintain active status, certified professionals must demonstrate ongoing learning and practical engagement in the fields of AI law, governance, and compliance.

Continuing Professional Development (CPD) Requirements

During each three-year certification cycle, candidates must earn and record a minimum of 60 Continuing Professional Development (CPD) hours, distributed across the following categories:

CPD Category	Description	Minimum Hours
1. Professional Learning	Participation in GAICC-recognised training, conferences, webinars, or workshops related to AI law, governance, ethics, or compliance.	20
2. Practical Application	Direct involvement in advising on AI governance, conducting AI risk assessments, drafting AI policies, or leading AI compliance projects.	20
3. Contribution & Knowledge Sharing	Activities such as publishing articles, mentoring, research, or contributing to AI governance initiatives, policy papers, or standards development.	10
4. Elective Activities	Additional learning or engagement activities supporting continuous professional growth.	10
Total	Minimum required.	60 CPDs

GAICC Code of Conduct and Ethics Statement

Purpose

The Global AI Certification Council (GAICC) upholds the highest standards of integrity, accountability, and professional behaviour in the certification and practice of AI law and compliance professionals. All GAICC-certified individuals must demonstrate ethical leadership and responsible stewardship in the governance of AI systems.

Commitment to Ethical Practice

By applying for and maintaining GAICC certification, candidates agree to:

1. **Act with Integrity and Fairness** – Conduct all professional activities honestly, without bias, conflict of interest, or misrepresentation of competence or credentials.
2. **Protect Human Rights and Wellbeing** – Ensure that AI systems under their influence respect human dignity, fairness, privacy, and non-discrimination.
3. **Ensure Transparency and Accountability** – Promote explainable and auditable AI outcomes; disclose limitations, risks, and decision criteria in plain language.
4. **Safeguard Data and Information** – Uphold confidentiality and data-protection principles consistent with ISO/IEC 42001, ISO/IEC 27701, and applicable laws.
5. **Exercise Professional Competence** – Maintain up-to-date knowledge through continual learning, professional development, and adherence to recognised standards and best practices.
6. **Report and Mitigate Misuse** – Take appropriate action when encountering unethical AI practices or violations of applicable regulations or standards.
7. **Respect Intellectual Property and Diversity of Perspectives** – Value collaboration, cultural sensitivity, and inclusiveness across disciplines and communities.

Frequently Asked Questions (FAQ)

GAICC Certified AI Law & Compliance Professional (GAICC-CAILCP)
Examination Content Outline – February 2026
Global AI Certification Council (GAICC)

1. What is the GAICC Certified AI Law & Compliance Professional (GAICC-CAILCP)?

It is a practitioner-level, internationally recognised credential that validates the competence of legal and compliance professionals in AI governance, multi-jurisdictional regulatory compliance, technical risk assessment, and practical AI application in legal practice.

2. Who should apply for this certification?

This certification is ideal for lawyers, compliance officers, data protection officers, legal operations professionals, GRC professionals, and in-house counsel who advise on or govern AI systems.

3. What are the eligibility requirements?

Applicants must meet education, professional experience, and formal training criteria. Education: Secondary, bachelor's, or master's qualification. Experience: 36–60 months of relevant legal, compliance, or AI governance work. Training: Completion of the GAICC-CAILCP programme (24–26 hours) or equivalent approved training.

4. How many questions are in the exam and how long does it take?

The examination consists of 60 scenario-based questions. Candidates have 90 minutes to complete the exam.

5. What is the passing score?

A minimum scaled score of 70% is required to pass.

6. How often can I take the exam?

Each candidate is granted **one(1) free retake.** Paid retakes are permitted without limit, subject to payment of the applicable resit fee for each attempt.

7. What is the certification validity period?

The Foundation certification is valid for **three (3) years** from the date of issue.

8. How do I maintain or renew my certification?

Certified professionals must complete a minimum of 60 CPD hours within each three-year cycle and submit a renewal application with the required fee.

9. What does the exam cover?

The exam assesses competence across eight domains: Global AI Regulatory Landscape, Governance-Technical AI Risk, Risk Classification & Compliance, AI for Lawyers Practical Skills, Liability & Enforcement, Policy & Governance Structures, AGI & Future Governance, and Ethics, Bias & Fairness.

10. What is the exam format?

The exam includes scenario-based multiple-choice questions. It is delivered through the GAICC Online AI-Proctored Testing Platform, ensuring secure and flexible access worldwide.

11. Does GAICC provide digital credentials?

Yes. Upon certification, you receive a digital badge and certificate that can be shared on LinkedIn, résumés, and professional profiles.

12. How can I contact GAICC for support?

Global AI Certification Council (GAICC)
Level 3, 21 Putney Way, Manukau, Auckland 2104, New Zealand
✉️ Email: **support@gaicc.org**
🌐 Website: ***www.gaicc.org***
📱Phone: ***+61 492 061 339/+64 21 103 6356***