Global AI Certification Council

# GAICC
# CERTIFIED PROFESSIONAL IN AI GOVERNANCE

**Examination Content Outline – 1st Edition | 2026**

Global AI Certification Council **(GAICC)**

## Examination Content Outline

1st Edition | 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 **GAICC Certified Professional in AI Governance (GAICC CPAIG)** is a practitioner-level, internationally recognised credential validating competence in AI governance across technical, regulatory, ethical, and strategic dimensions.

The GAICC CPAIG is built from a genuinely global perspective - providing equal weight to Asia-Pacific, Middle East, African, and Latin American regulatory environments alongside Western frameworks. The credential goes deeper into agentic AI, generative AI governance, and the emerging challenges of increasingly autonomous AI systems than any comparable certification currently available.

**This Examination Content Outline defines:**
> The eight domains of competence required of a GAICC CPAIG holder
> The competencies and performance indicators within each domain
> The relative weight of each domain in the overall examination
> The cognitive depth and assessment approach applied across all domains

**Assessment Philosophy**
All 80 questions are scenario-based, requiring application of knowledge to realistic multi-jurisdictional AI governance situations. Questions test Application (45%) and Analysis/Evaluation (30%) cognitive levels. Only 25% operate at Understanding level. No question tests definition recall alone.

## How GAICC CPAIG Differentiates

| Feature | GAICC CPAIG | IAPP AIGP (Benchmark) |
|---|---|---|
| Global Regulatory Coverage | EU + US + UK + APAC + Middle East + Africa + LATAM | EU AI Act + US primary focus |
| Agentic AI Governance | Dedicated domain - full autonomous system governance | Limited coverage embedded in broader topics |
| Generative AI Governance | Dedicated domain - RAG, fine-tuning, multi-agent, GPAI | Briefly embedded within broader content |

| Feature | GAICC CPAIG | IAPP AIGP (Benchmark) |
|---|---|---|
| Technical-Legal Bridge | Dedicated module translating failure modes to obligations | General technical literacy overview |
| Human Rights Integration | Dedicated competency using UN Guiding Principles | Not covered |
| Strategic Board Advisory | Dedicated module with practical dashboard tools | Brief mention |
| Questions | 80 questions (2 hours) | 100 questions (2 hours) |
| Passing Mark | 70% | 60% (300/500 scaled) |
| Validity | 3 years | 2 years |

# Examination Structure

| Component | Details |
|---|---|
| Total Questions | 80 questions (70 scored + 10 unscored pilot) |
| Format | Scenario-based multiple-choice - single best answer per question |
| Duration | 2 hours (no optional break) |
| Pass Mark | 70% (minimum 49 of 70 scored questions correct) |
| Scaled Score | 100-500 scale; 350 is the passing threshold |
| Negative Marking | None - candidates should answer all questions |
| Delivery | GAICC Online AI-Proctored Platform - global browser access, 24/7 scheduling |
| Results | Immediate upon completion with domain-level performance feedback |
| Retake Policy | One complimentary retake within 12-month eligibility window |
| Cognitive Split | Understanding 25% \| Application 45% \| Analysis & Evaluation 30% |

## Domain Weightings

| Domain | Weight | Questions |
|---|---|---|
| I. Global AI Governance Landscape | 20% | ~14 questions |
| II. Technical AI Risk & Governance Architecture | 18% | ~13 questions |
| III. AI Lifecycle Governance | 16% | ~11 questions |
| IV. Laws, Standards & Multi-Jurisdictional Compliance | 15% | ~11 questions |
| V. Agentic & Generative AI Governance | 12% | ~9 questions |
| VI. Governance Strategy & Organisational Design | 10% | ~7 questions |
| VII. Ethics, Bias, Fairness & Human Rights | 5% | ~4 questions |
| VIII. Future AI & Emerging Governance Frontiers | 4% | ~3 questions |
| TOTAL | 100% | 80 Questions |

# Domains, Competencies & Performance Indicators

## Domain I – Global AI Governance Landscape (≈ 20%)

**Purpose:**
Conduct multi-jurisdictional AI governance analysis, map extraterritorial exposure, and identify compliance priorities across the full global regulatory landscape including APAC, Middle East, Africa, and Latin America alongside EU/US/UK.

| Competency | Performance Indicators |
|---|---|
| I.A Understand what AI governance is and why it matters globally | Know accepted definitions and types of AI systems; Identify risks and harms to individuals, groups, organisations, and society; Understand unique characteristics requiring governance (opacity, autonomy, scale, data dependency); Apply core responsible AI principles (fairness, safety, privacy, transparency, accountability, human-centricity) |
| I.B Map extraterritorial regulatory exposure for multinational deployments | Conduct jurisdiction identification across EU, US, UK, APAC, Middle East, Africa, and Latin America; Analyse regulatory overlap and compliance priority conflicts; Build extraterritorial exposure matrices; Identify where multiple frameworks apply simultaneously to a single AI system or deployment |
| I.C Analyse and apply the EU AI Act risk classification system | Apply risk tier determinations (prohibited, high-risk, limited-risk, minimal-risk); Assess boundary cases and grey zones; Map GPAI obligations and conformity assessment requirements; Understand enforcement framework, transition timelines, and proportional penalties by role (provider, deployer, importer) |

| Competency | Performance Indicators |
|---|---|
| I.D Evaluate Asia-Pacific, Middle East, and African AI governance frameworks | Apply Singapore Model AI Governance Framework; Assess Japan, South Korea, and Australia approaches; Evaluate UAE AI Strategy and Saudi NDMO guidelines; Identify African Union and national AI frameworks; Compare prescriptive vs principles-based regulatory models across jurisdictions |
| I.E Assess US federal and state-level AI regulatory environments | Apply FTC enforcement doctrine to AI systems; Analyse SEC/FINRA, EEOC, FDA, and CFPB AI guidance; Map state-level AI laws including Colorado, Illinois, Texas, and NYC Local Law 144; Identify sector-specific compliance obligations and enforcement priorities |
| I.F Identify regulatory conflicts and harmonisation opportunities | Build cross-border conflict analysis frameworks; Identify where frameworks align (OECD principles, ISO 42001 base) and where they clash; Develop harmonisation strategies; Advise on pragmatic compliance sequencing across competing jurisdictional obligations |

## Domain II – Technical AI Risk & Governance Architecture (≈ 18%)

**Purpose:**
Translate AI technical failure modes into governance obligations; assess foundation model architecture decisions for compliance risk; evaluate vendor technical claims; and apply structured technical-legal risk mapping - giving governance professionals genuine technical literacy.

| Competency | Performance Indicators |
|---|---|
| II.A Translate AI technical failure modes into governance obligations | Map model drift, hallucination, bias amplification, brittleness, and data poisoning to specific governance risks and legal exposure categories (product liability, consumer protection, anti-discrimination, data protection, professional negligence); Apply probability/severity harms matrix; Develop technical-legal risk registers |
| II.B Assess foundation model architecture for governance risk | Evaluate pre-training, fine-tuning, and RLHF decisions for compliance implications; Assess RAG architecture risk for accuracy and IP obligations; Conduct training data audits for IP, consent, and bias; Evaluate model versioning obligations for ongoing compliance |
| II.C Evaluate AI vendor technical claims against governance requirements | Conduct vendor due diligence on model safety and accuracy claims; Assess API dependency and third-party model supply chain risks; Evaluate model documentation and provenance audit trails; Identify red flags in vendor representations, warranties, and benchmark claims |

| Competency | Performance Indicators |
| --- | --- |
| II.D Apply red teaming and safety testing to governance oversight | Understand adversarial testing methodologies (red teaming, jailbreaking, prompt injection); Interpret safety benchmark results for governance purposes; Commission and review independent bias audits; Apply safety testing findings to ongoing governance obligations and regulatory submissions |
| II.E Govern multimodal and large language model deployments | Identify governance differences between language, vision, audio, and multimodal models; Apply GPAI-specific governance requirements under EU AI Act; Assess open-source model governance risks and limitations; Evaluate edge vs cloud deployment governance and jurisdictional implications |

## Domain III – AI Lifecycle Governance (≈ 16%)

**Purpose:**
Apply governance responsibilities across the complete AI lifecycle - from design and data collection through development, testing, deployment, monitoring, and decommissioning - ensuring continuous accountability at every stage.

| Competency | Performance Indicators |
|---|---|
| III.A Govern the design and use-case definition phase | Define and document the business context and use-case justification; Conduct pre-deployment impact assessments (FRIA, AIA, sector-specific); Apply ethics-by-design and privacy-by-design principles; Identify human oversight requirements at design stage; Engage cross-functional stakeholders in governance review |
| III.B Govern data collection, processing, and training data governance | Establish lawful basis and consent frameworks for training data; Assess data quality, integrity, bias risk, and fitness-for-purpose; Document data lineage and provenance; Apply data minimisation to AI development; Govern use of synthetic, third-party, scraped, and personal data in training pipelines |
| III.C Govern model development and testing processes | Apply governance controls to model training, validation, and testing; Commission bias and fairness testing protocols; Oversee unit, integration, performance, security, and interpretability testing; Manage and document risks identified during development; Apply model cards and technical documentation requirements |

| Competency | Performance Indicators |
|---|---|
| III.D Govern model release and deployment readiness | Assess deployment readiness against conformity assessment requirements; Prepare model cards, system cards, and regulatory submission packages; Establish change management and version control governance; Apply sector-specific deployment authorisation requirements (medical device, financial services, critical infrastructure) |
| III.E Govern continuous monitoring and maintenance | Design and implement continuous monitoring programmes; Establish model retraining triggers and schedules; Conduct periodic audits (performance, safety, bias, security); Manage model drift and data distribution shift; Apply post-market monitoring obligations across EU, US, UK, and APAC jurisdictions |
| III.F Govern decommissioning and system retirement | Design AI system decommissioning protocols; Manage data retention and deletion obligations at system retirement; Document decommissioning decisions and evidence trails; Assess liability exposure during transition and wind-down periods; Notify affected parties and regulators as required |

## Domain IV – Laws, Standards & Multi-Jurisdictional Compliance (≈ 15%)

**Purpose:**
Understand how global laws - data privacy, anti-discrimination, consumer protection, sector-specific regulation, and AI-specific legislation - apply to AI systems, and integrate international standards into governance programmes.

| Competency | Performance Indicators |
|---|---|
| IV.A Apply data privacy laws to AI systems globally | Apply GDPR, CCPA/CPRA, PDPA, PIPL, and LGPD to AI development and deployment; Apply automated decision-making rights and human review obligations across jurisdictions; Manage cross-border data transfer obligations for AI training and inference |
| IV.B Apply anti-discrimination and consumer protection laws to AI | Apply nondiscrimination obligations in employment, credit, lending, housing, insurance, and healthcare; Understand consumer protection prohibitions on unfair, deceptive, and manipulative AI practices; Apply product liability frameworks to AI system failures; Map EEOC, CFPB, FCA, and equivalent enforcement risks |
| IV.C Understand and apply AI-specific legislation | Apply EU AI Act risk classification and full compliance obligations; Understand South Korean AI Basic Law and Asia-Pacific AI legislation; Apply sector-specific AI laws (health, finance, employment, critical infrastructure); Understand GPAI model compliance requirements and foundation model obligations |

| Competency | Performance Indicators |
|---|---|
| IV.D Integrate international AI standards into governance programmes | Apply ISO/IEC 42001 AI Management System certification requirements; Implement NIST AI RMF (Govern, Map, Measure, Manage) in organisational context; Apply OECD AI Principles to governance design; Integrate ISO 22989 and ISO 42005 standards; Develop standards-based evidence portfolios for regulatory demonstration |
| IV.E Build multi-jurisdictional compliance programmes | Design compliance matrices mapping AI systems to obligations across jurisdictions; Develop regulatory equivalence mapping for global operations; Prioritise compliance sequencing under resource constraints; Build regulatory change monitoring and adaptation processes |

## Domain V – Agentic & Generative AI Governance (≈ 12%)

**Purpose:**
Govern the unique risks posed by agentic AI systems (autonomous agents, multi-agent architectures, AI in automated decision chains) and generative AI deployments - the fastest-growing and least-governed frontier of AI risk.

| Competency | Performance Indicators |
|---|---|
| V.A Assess agentic AI systems for delegation and accountability risk | Analyse autonomous decision chains and tool-use risk; Map delegation authority across human-AI systems; Identify human oversight gaps in agentic workflows; Assess multi-agent system governance challenges; Apply containment vs autonomy framework decisions and document governance rationale |
| V.B Govern generative AI deployments and content risks | Apply governance controls to LLM-generated content in commercial and regulated contexts; Assess hallucination risk and implement verification workflows; Govern synthetic media and deepfake exposure; Apply IP and copyright obligations to training data and AI-generated outputs; Manage professional standards when AI assists in regulated advice |
| V.C Assess and govern RAG and fine-tuned model deployments | Evaluate governance implications of RAG architecture choices; Assess knowledge base integrity, currency, and provenance risks; Govern fine-tuning data selection, consent, and compliance obligations; Manage version control and audit trails for customised model deployments |

| Competency | Performance Indicators |
|---|---|
| V.D Apply governance frameworks to AI agent autonomy levels | Apply autonomy spectrum (human-in-the-loop to fully autonomous) to governance design; Assess legal accountability allocation across different autonomy levels; Design override, intervention, and emergency stop governance requirements; Apply EU AI Act human oversight requirements to agentic deployment contexts |
| V.E Govern multi-agent systems and AI pipelines | Assess accountability in multi-agent AI architectures and orchestration frameworks; Apply governance controls to AI pipeline design and operation; Identify liability distribution across interconnected agent networks; Govern prompt chaining and cascading decision risks; Assess supply chain risks in AI agent ecosystems |

## Domain VI – Governance Strategy & Organisational Design (≈ 10%)

**Purpose:**
Design AI governance programmes appropriate to organisational size, sector, and risk profile; build risk registers and incident response capability; structure vendor oversight; and advise boards and executives on AI governance as a strategic function.

| Competency | Performance Indicators |
|---|---|
| VI.A Design AI governance frameworks for organisations | Build governance committee charters and RACI matrices; Apply three lines of defence model to AI governance; Design AI policy architecture (acceptable use, procurement, development, deployment, monitoring); Tailor governance structures to company size, sector, maturity, and risk tolerance |
| VI.B Build AI risk registers and incident escalation protocols | Design AI risk register templates and scoring methodologies; Define escalation triggers, severity classifications, and accountability chains; Build regulatory reporting procedures and notification timelines; Develop post-incident review and governance improvement processes |
| VI.C Structure AI vendor and third-party oversight programmes | Design vendor due diligence frameworks for AI procurement; Build ongoing monitoring programmes for AI vendors; Draft contractual control requirements, audit rights, and governance obligations; Manage model supply chain risk; Develop vendor exit strategy and continuity governance |

| Competency | Performance Indicators |
|---|---|
| VI.D Execute AI incident response and crisis governance | Apply incident response playbooks to AI failure scenarios; Sequence containment, disclosure, regulatory notification, and litigation risk management; Coordinate legal, technical, communications, and executive response to AI crises; Manage post-incident remediation and governance enhancement |
| VI.E Advise boards and executives on AI governance strategy | Build AI risk dashboards and metrics frameworks for board reporting; Conduct AI governance maturity assessments; Define AI risk appetite and integrate with enterprise risk management; Present regulatory readiness scorecards; Advise on AI governance investment and the business case for proactive compliance |

## Domain VII – Ethics, Bias, Fairness & Human Rights (≈ 5%)

**Purpose:**
Apply fairness frameworks to AI system evaluation; assess bias risk across the AI lifecycle; operationalise ethical governance; and integrate human rights due diligence obligations into AI governance design.

| Competency | Performance Indicators |
|---|---|
| VII.A Apply fairness frameworks to AI governance | Apply competing fairness definitions (demographic parity, equalised odds, individual fairness, counterfactual fairness); Map tensions between fairness metrics and navigate regulatory expectations; Commission and interpret fairness testing results; Apply regulatory approaches to algorithmic fairness across EU, US, and APAC jurisdictions |
| VII.B Assess bias risk across the full AI lifecycle | Identify bias introduction risks at each lifecycle stage (data collection, labelling, model training, evaluation, deployment, monitoring); Commission and evaluate independent bias audits; Apply algorithmic impact assessment methodologies; Manage bias-related regulatory enforcement and litigation risk; Apply proportional remediation controls |
| VII.C Operationalise ethical AI governance frameworks | Translate ethical AI principles into enforceable governance controls; Apply transparency and explainability obligations across regulatory contexts; Implement responsible AI programme structures with clear accountability; Integrate ethics review into governance decision-making and procurement processes |

| Competency | Performance Indicators |
| --- | --- |
| VII.D Integrate human rights due diligence into AI governance | Apply UN Guiding Principles on Business and Human Rights to AI deployment; Assess AI system human rights impact (privacy, expression, non-discrimination, due process); Design human rights impact assessments for high-risk AI systems; Integrate human rights obligations into vendor governance and contractual frameworks |

## Domain VIII – Future AI & Emerging Governance Frontiers (≈ 4%)

**Purpose:**
Evaluate governance challenges posed by increasingly capable and autonomous AI systems, frontier AI risk, and international governance coordination - ensuring governance professionals are prepared for AI systems beyond current regulatory design.

| Competency | Performance Indicators |
|---|---|
| VIII.A Evaluate governance frameworks for increasingly autonomous AI | Assess agent autonomy spectrum and governance implications at each level; Apply containment vs control framework approaches; Identify current governance gaps for advanced AI capabilities; Evaluate sufficiency of existing regulatory frameworks for near-future AI systems including frontier models |
| VIII.B Assess frontier and advanced AI governance challenges | Understand alignment problem concepts and their practical governance implications; Assess governance preparedness gap analyses for advanced AI; Evaluate liability shift implications as AI autonomy increases; Apply precautionary governance principles to uncertain and potentially catastrophic risk profiles |
| VIII.C Assess international AI governance coordination | Evaluate treaty, multilateral agreement, and international governance forum frameworks for AI; Assess compute governance approaches and hardware-level safety control implications; Compare safety standards across major AI-developing nations (US, EU, China, UK, Japan); Evaluate dual-use AI policy and technology export control implications |

# 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 | Professional Experience | Training Requirement |
|---|---|---|
| Secondary Qualification (high school diploma, associate degree, or global equivalent) | 5 years (60 months) of professional experience in AI governance, risk, compliance, policy, or related field | Completion of GAICC CPAIG programme (28-30 hours) or GAICC-approved equivalent training |
| Bachelor's Degree (or global equivalent) | 3 years (36 months) of experience in AI governance, data, compliance, technology, or related discipline | Completion of GAICC CPAIG programme or GAICC-approved equivalent training |
| Master's Degree or Professional Qualification | 2 years (24 months) of relevant experience in AI governance, law, risk, or related field | Completion of GAICC CPAIG programme or GAICC-approved equivalent training |

## Experience Recency

All relevant experience must have been gained within the last eight (8) consecutive years before submitting the GAICC CPAIG application. Experience from diverse sectors, jurisdictions, and organisational sizes is recognised and encouraged.

# Certification Maintenance & CPD Requirements

The GAICC CPAIG certification is valid for three (3) years. During each cycle, certified professionals must earn a minimum of 60 CPD hours:

| CPD Category | Description | Minimum Hours |
|---|---|---|
| 1. Professional Learning | GAICC-recognised training, conferences, webinars, or workshops in AI governance, law, ethics, regulation, or compliance | 20 hours |
| 2. Practical Application | Direct involvement in AI governance advisory, risk assessments, policy drafting, or leading AI compliance programmes | 20 hours |
| 3. Contribution & Knowledge Sharing | Publishing articles, mentoring, research, contributing to AI governance standards, policy papers, or community initiatives | 10 hours |
| 4. Elective Activities | Additional learning or engagement activities supporting continuous professional growth in AI-adjacent disciplines | 10 hours |
| TOTAL | Minimum required across all categories in each 3-year certification cycle | 60 CPD Hours |

# Examination Fees

| Item | Details | Fee (USD) |
|---|---|---|
| Annual Membership | Access to GAICC resources, CPD tracking platform, member community, discounts | $99 |
| Exam Fee (Members) | Includes one exam attempt. Resit fee applies for any additional attempt. | $449 |
| Exam Fee (Non-Members) | Includes one exam attempt. Resit fee applies for any additional attempt. | $595 |
| Certification Renewal (Members) | Per 3-year renewal cycle - CPD portfolio submission required | $199 |
| Certification Renewal (Non-Members) | Per 3-year renewal cycle - CPD portfolio submission required | $299 |

# GAICC Code of Professional Conduct

| Principle | Obligation |
|---|---|
| 1. Integrity and Fairness | Act honestly in all professional activities without bias, conflict of interest, or misrepresentation of competence. Disclose potential conflicts proactively. |
| 2. Human Rights and Wellbeing | Ensure AI systems under governance influence respect human dignity, fairness, privacy, and non-discrimination across all affected populations. |
| 3. Transparency and Accountability | Promote explainable and auditable AI outcomes. Disclose limitations, risks, and decision criteria in plain language accessible to affected parties. |
| 4. Data Protection and Privacy | Uphold confidentiality and data-protection principles consistent with applicable laws and international standards. |
| 5. Professional Competence | Maintain up-to-date knowledge through continuous learning, professional development, and active engagement with evolving AI governance standards. |
| 6. Reporting and Mitigation of Misuse | Take appropriate action when encountering unethical AI practices or violations of applicable regulations or professional standards. |
| 7. Global Responsibility | Recognise that AI governance has global implications. Apply governance standards that protect individuals regardless of jurisdiction. |

# Frequently Asked Questions (FAQ)

**GAICC Certified Professional in AI Governance (GAICC CPAIG)**
**Examination Content Outline – 1st Edition | 2026**
**Global AI Certification Council (GAICC)**

## 1. What is the GAICC CPAIG?

A practitioner-level, globally recognised AI governance credential validating competence across technical, regulatory, ethical, and strategic dimensions - built from a genuinely global perspective.

## 2. Who should pursue CPAIG?

AI governance professionals, risk and compliance managers, policy advisors, DPOs, technology executives, legal professionals, GRC practitioners, and anyone responsible for governing AI systems.

## 3. How does CPAIG differ from IAPP AIGP?

CPAIG provides deeper global coverage (APAC, Middle East, Africa, LATAM), dedicated agentic and generative AI governance domains, technical-legal bridge module, human rights integration, and strategic board advisory content.

## 4. What are the eligibility requirements?

Education (secondary to postgraduate), 2-5 years relevant experience (depending on education level), and completion of the GAICC CPAIG programme (28-30 hours) or approved equivalent.

## 5. What is the exam format?

80 scenario-based MCQs in 2 hours via GAICC Online AI-Proctored Platform. Pass mark is 70%.

## 6. How long is the certification valid?

3 years. Renewal requires 60 CPD hours per cycle plus a renewal application and fee.

## 7. What digital credentials are provided?

Digital badge and verifiable certificate for LinkedIn, resumes, and professional profiles plus listing in the GAICC global credentials register.

## 8. 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***