Global AI Certification Council

GAICC CPAIG

CERTIFIED PROFESSIONAL IN AI GOVERNANCE

Examination Content Outline
1st Edition | 2026

Global AI Certification Council
(GAICC)

Examination Content Outline

1st Edition | 2026

Global AI Certification Council

The Credential at a Glance

80 MCQs	70%	60 CPDs
2 hours · Examination	Pass mark · scenario-based	Every 3 years · Renewal

Credential	GAICC Certified Professional in AI Governance (GAICC CPAIG)
Issued by	Global AI Certification Council (GAICC)
Standard	ISO/IEC 17024 Conformity Assessment for Certification Bodies
Examination	80 scenario-based MCQs | 2 hours | 70% pass mark
Validity	3 years | 60 CPD hours per cycle
Contact	certify@gaicc.org | www.gaicc.org

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

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 examination, and the cognitive depth applied across all domains.

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:

01 The eight domains of competence required of a GAICC CPAIG holder

02 The competencies and performance indicators within each domain

03 The relative weight of each domain in the overall examination

04 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	Benchmark credential
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
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 hrs)	100 questions (3 hrs)
Pass 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
II. Technical AI Risk & Governance Architecture	18%	~13
III. AI Lifecycle Governance	16%	~11
IV. Laws, Standards & Multi-Jurisdictional Compliance	15%	~11
V. Agentic & Generative AI Governance	12%	~9
VI. Governance Strategy & Organisational Design	10%	~7
VII. Ethics, Bias, Fairness & Human Rights	5%	~4
VIII. Future AI & Emerging Governance Frontiers	4%	~3
TOTAL	**100%**	**80 questions**

Cognitive Split

25% Understanding **45%** Application **30%** Analysis & Evaluation

Domains, Competencies & Performance Indicators

The eight domains that follow set out, for each area of competence, the purpose of the domain, its examination weight, and the performance indicators against which candidates are assessed.

DOMAIN

I

Global AI Governance Landscape

20% | ~14 questions

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 the enforcement framework, transition timelines, and proportional penalties by role (provider, deployer, importer).
I.D Evaluate Asia-Pacific, Middle East, and African AI governance frameworks	Apply the 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 versus 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

18% | ~13 questions

Technical AI Risk & Governance Architecture

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 a 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.
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 the EU AI Act; assess open-source model governance risks and limitations; evaluate edge versus cloud deployment governance and jurisdictional implications.

DOMAIN

III

AI Lifecycle Governance

16% | ~11 questions

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.
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% | ~11 questions

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 the 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.
IV.D Integrate international AI standards into governance programmes	Apply ISO/IEC 42001 AI Management System certification requirements; implement the NIST AI RMF (Govern, Map, Measure, Manage) in organisational context; apply OECD AI Principles to governance design; integrate ISO 22989 and ISO 42005; 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% | ~9 questions

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 versus 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.
V.D Apply governance frameworks to AI agent autonomy levels	Apply the 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% | ~7 questions

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 the 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.
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% | ~4 questions

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.
VII.D Integrate human rights due diligence into AI governance	Apply the 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

4% | ~3 questions

Future AI & Emerging Governance Frontiers

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 the agent autonomy spectrum and governance implications at each level; apply containment versus control framework approaches; identify current governance gaps for advanced AI capabilities; evaluate the 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 CPAIG certification, candidates must demonstrate the educational background, professional experience, and structured training set out below.

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 at least 28–30 contact hours of structured CPAIG training delivered by GAICC-authorised providers or equivalent recognised institutions. Students can also fulfil this requirement by completing GAICC self-paced courses.
Bachelor's Degree (or global equivalent)	3 years (36 months) of experience in AI governance, data, compliance, technology, or related discipline	Completion of at least 28–30 contact hours of structured CPAIG training delivered by GAICC-authorised providers or equivalent recognised institutions. Students can also fulfil this requirement by completing GAICC self-paced courses.
Master's Degree or Professional Qualification	2 years (24 months) of relevant experience in AI governance, law, risk, or related field	Completion of at least 28–30 contact hours of structured CPAIG training delivered by GAICC-authorised providers or equivalent recognised institutions. Students can also fulfil this requirement by completing GAICC self-paced courses.

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
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 hours**

Examination Fees

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.

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

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.

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.

How does CPAIG differ from comparable credentials?

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

What are the eligibility requirements?

Education (secondary to postgraduate), 2–5 years relevant experience depending on education level, and completion of at least 28–30 contact hours of structured CPAIG training delivered by GAICC-authorised providers or equivalent recognised institutions. Students can also fulfil this requirement by completing GAICC self-paced courses.

What is the exam format?

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

How long is the certification valid?

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

What digital credentials are provided?

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

certify@gaicc.org | support@gaicc.org | www.gaicc.org

Global AI
Certification Council

GAICC CPAIG

CERTIFIED PROFESSIONAL IN AI GOVERNANCE

The global standard for professionals who govern AI systems with authority, depth, and genuine international competency.

www.gaicc.org | certify@gaicc.org | support@gaicc.org

Examination Content Outline | 1st Edition | 2026 ·