Global AI
Certification Council

GAICC RAIGP

ROBOTIC AI GOVERNANCE PROFESSIONAL

Examination Content Outline
1st Edition | 2026

Global AI Certification Council
(GAICC)

Examination Content Outline

1st Edition | 2026 · GAICC-ECO-RAIGP-001

Global AI Certification Council

The Credential at a Glance

100 MCQs	70%	60 CPDs
2 h 30 min · Examination	Pass mark · scenario-based	Every 3 years · Renewal

Credential	GAICC Robotic AI Governance Professional (GAICC RAIGP)
Issued by	Global AI Certification Council (GAICC)
Standard	Developed in accordance with ISO/IEC 17024 (Conformity assessment. General requirements for bodies operating certification of persons)
Document code	GAICC-ECO-RAIGP-001 | v1.0 | Issued 13 September 2026
Training requirement	32 hours of RAIGP training by any of three recognised routes
Examination	100 scenario-based MCQs | 2 hours 30 minutes | 70% pass mark
Validity	3 years | 60 CPD hours per cycle
Recommended background	GAICC CPAIG or GAICC AAIGP, or an equivalent AI governance credential, strongly recommended; not a prerequisite
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 RAIGP holder, the forty competencies and performance indicators within each domain, the relative weight of each domain in the examination, the cognitive depth applied across all domains, the eligibility requirements, and the Code of Professional Conduct and maintenance requirements that apply to holders.

Introduction

The GAICC Robotic AI Governance Professional (GAICC RAIGP) is an advanced practitioner credential for professionals who authorise, oversee, assure and stop AI systems that move through the physical world: industrial and collaborative robots, mobile robots and fleets, service and humanoid robots, medical robots, agricultural machines, autonomous vehicles and uncrewed aircraft. It is the first GAICC credential written for systems whose failures are measured in kinetic energy.

Conventional AI governance asks whether a system's output is accurate, fair and lawful. Agentic governance asks what a system is permitted to do and on whose authority. Robotic AI governance asks a harder question still: what is this system permitted to do with mass, force and speed, among people who did not choose to be near it, and what evidence proves it will stop when it must. RAIGP is built around that question.

RAIGP sits where two mature disciplines meet and have not yet been joined. The safety of machinery discipline (ISO 12100, ISO 10218, ISO 13849-1, IEC 61508, the EU Machinery Regulation) governs robots as machines but assumes deterministic control. AI governance (ISO/IEC 42001, ISO/IEC 42005, the EU AI Act, NIST AI RMF) governs learning systems but assumes their failures are informational. Learned control policies, robot foundation models, fleet learning and teleoperation break both assumptions at once. RAIGP holders are the professionals who can read a functional safety claim and an AI impact assessment in the same meeting, and know which one is missing.

RAIGP extends the GAICC AI Governance Framework, Maturity Model and Implementation Roadmap into embodied operation. It assumes the governance fundamentals taught in CPAIG and the authority and control concepts taught in AAIGP, and examines the physical safety, assurance, security, liability and regulatory problems created by autonomy with a body.

This Examination Content Outline defines:

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

02 The forty competencies and the 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

05 The eligibility requirements that apply before a candidate may sit the examination

06 The Code of Professional Conduct and the certification maintenance requirements that apply to holders

Assessment Philosophy

All 100 questions are scenario-based. Every item places the candidate in a decision seat: accept or refuse residual risk, authorise or withhold deployment, stop or continue, notify or hold, promote or demote autonomy, sign or decline the declaration. Questions test Application (45%) and Analysis and Evaluation (40%) cognitive levels. Only 15% operate at Understanding level.

No question tests definition recall alone, no question requires engineering calculation, and no question can be answered from vendor terminology. Candidates are expected to reason from first principles where standards and regulation are silent, because for learned control of physical systems they frequently are.

Standards and regulation in this field move quickly. Items are written against the position stated in the current edition of this outline. Where an obligation has a future application date, items test the candidate's ability to sequence governance work ahead of it, not to guess whether the date will move. GAICC reviews this outline at least annually and after any material change in the standards and regulation named in the performance indicators.

How GAICC RAIGP Differentiates

Dimension	GAICC RAIGP	GAICC AAIGP	GAICC CPAIG	Functional safety credentials	General AI governance credentials
Governance question	What may this system do with mass, force and speed, among people, and what proves it will stop	What may this system do, on whose authority, and how is it stopped	Is this AI system lawful, fair and well governed	Does this machine meet the required performance level or safety integrity level	Is this AI system lawful and well documented
Physical safety and the machinery regime	Full domain: ISO 12100, ISO 10218:2025, ISO 13482, ISO 3691-4, functional safety claims, Machinery Regulation, workplace safety law	Not addressed	Not addressed	Core content, engineering depth, no AI or learning	Not addressed
Learned control and robot foundation models	Full domain: learned policies, vision-language-action models, ISO/IEC TR 5469 configurations, deployer fine-tuning, fleet learning	Agent architectures and orchestration for software agents	Introductory coverage within technical foundations	Rarely addressed; assumes deterministic control	Rarely addressed
Human oversight	Full domain: stop and fallback, minimal risk condition, teleoperation, collaborative operation, human factors, public and care settings	Approval gates, circuit breakers, kill switches for software agents	Human oversight requirements and override principles	Emergency stop and safeguarding design	Human in the loop stated as a principle
Assurance and safety case	Full domain: UL 4600, GSN, AMLAS and SACE, scenario-based testing, simulation credibility, independent assessment, safety performance indicators	Trajectory evaluation, agentic red teaming, assurance cases	Commissioning and interpreting model safety testing	Verification against safety standards; safety case in UL 4600 programmes only	Limited

How GAICC RAIGP Differentiates (continued)

Dimension	GAICC RAIGP	GAICC AAIGP	GAICC CPAIG	Functional safety credentials	General AI governance credentials
Cybersecurity, data and supply chain	Full domain: IEC 62443, Cyber Resilience Act, robot attack surfaces, sensor and teleoperation data, provenance and import controls	Non-human identity, tool grants, exfiltration through action	Data protection and third-party governance at principle level	Cybersecurity as a machinery requirement, limited depth	Privacy focus
Incident, liability and insurance	Full domain: physical incident response, recalls, workplace and product regulators, Product Liability Directive 2024/2853, insurance prerequisites	Agentic incident response, notification, supply chain liability	Incident and notification obligations	Accident investigation at engineering level	Documentation obligations
Regulation	AI Act applied through the machinery, medical, vehicle and aviation regimes; sector regimes; United States, China, Korea, Japan and other jurisdictions	AI Act, GPAI and automated decision-making rights applied to agents	Global AI law landscape	Machinery and product safety law	AI law landscape
Training requirement for eligibility	32 hours	32 hours	28 to 30 hours	Typically 4 to 5 days of training	Varies
Examination	100 scenario items, 2.5 hours, 70% pass	100 scenario items, 2.5 hours, 70% pass	80 scenario items, 2 hours, 70% pass	Typically 2 to 6 hours, engineering calculation, 80% pass in some schemes	Typically 100 items, 3 hours, scaled pass

Examination Structure

Component	Details
Total Questions	100 questions (88 scored + 12 unscored pilot)
Format	Scenario-based multiple-choice, single best answer per question, four options A to D
Duration	2 hours 30 minutes (150 minutes), no optional break
Pass Mark	70% of scored questions (62 of 88), reported on a 100–500 scale where 350 is the passing threshold; the cut score is confirmed through modified-Angoff standard setting
Scaled Score	100–500 scale; 350 is the passing threshold
Negative Marking	None. Candidates should answer all questions
Delivery	AI-proctored on the GAICC hub (hub.gaicc.org), global browser access
Results	Provisional result displayed on screen on completion, with domain-level performance feedback
Certification decision	The Certification Decision Authority reviews the provisional result and confirms the decision within 72 hours
Cognitive Split	Understanding 15% | Application 45% | Analysis and Evaluation 40%
Reference Material	Closed book. No external reference material permitted. No calculation is required

Domain Weightings

Dom	Domain Title	Weight	Scored Questions
I	Embodied AI Systems and Robot Architecture Literacy	12%	~11
II	Physical Safety Governance and the Machinery and Product Regime	15%	~13
III	Risk, Hazard and Impact Assessment for Embodied AI	14%	~12
IV	Human Oversight, Control and Human-Robot Interaction	13%	~11
V	Assurance, Safety Cases, Verification and Validation	13%	~11
VI	Cybersecurity, Data and Supply Chain Governance for Robots	11%	~10
VII	Operations, Incident Response, Liability and Insurance	11%	~10
VIII	Regulatory Landscape, Sector Regimes and Enterprise Scaling	11%	~10
TOTAL		**100%**	**88 + 12 pilot**

Examination Development and Maintenance

Items are written by subject matter experts against the performance indicators published in this outline, reviewed by a second expert who did not write the item, and edited for language, cultural neutrality and single-best-answer defensibility. Every item records the competency it tests. New items enter a live form as unscored pilot items before they are scored, and item performance is reviewed after each form.

The cut score is confirmed through modified-Angoff standard setting by a panel independent of the item writers. Domain weightings are reviewed against practice at each revision of this outline. This outline is reviewed at least annually, and whenever a material change in the standards or regulation named in the performance indicators changes what competent practice requires. An item affected by such a change is withdrawn or rewritten before the next form is published.

Examination content is confidential. No training provider, including GAICC, has access to the live item pool, and no

DOMAIN

I

Embodied AI Systems and Robot Architecture Literacy

12% | ~11 questions

Purpose

Read and interrogate a robot system design well enough to govern it. Understand the sensing, perception, planning, control and actuation stack, the safety layer, learned control policies, operating environments and fleet architectures at the level of detail a governance decision actually requires, without becoming an engineer.

Competency	Performance Indicators
I.A Classify robots and autonomous systems for governance	Apply ISO 8373 vocabulary for robot, industrial robot, service robot, collaborative application and autonomy; distinguish industrial, collaborative, mobile (AGV and AMR), service, humanoid, medical, agricultural, autonomous vehicle and uncrewed aircraft classes and the regulatory regime each attracts; classify degree of autonomy and operating environment: segregated, shared, collaborative, public and domestic; identify the point at which an automated machine becomes an AI-driven autonomous system for registry and tiering purposes; register every robot and fleet in the AI system inventory with owner, risk tier, autonomy level, operational design domain and oversight mode, as required by Phase 3 of the GAICC Implementation Roadmap.
I.B Interpret the robot stack and the safety layer	Read the sense, perceive, plan, control and actuate pipeline and identify where AI decides and where deterministic control decides; distinguish a safety-rated function from a performance function; identify the safety layer (safety controller, monitored standstill, speed and separation monitoring, power and force limiting, safe torque off) and assess whether it is independent of the AI; treat kinetic energy, reach, payload, speed and failure modes as governance variables; interrogate a design document to surface undeclared autonomy, learning or remote control.
I.C Govern learned control policies and robot foundation models	Distinguish modular classical control from end-to-end learned policies and vision-language-action models; assess non-determinism, distribution shift and unknown unsafe behaviour in learned policies; govern deployer fine-tuning, demonstration data and on-device adaptation as changes to behaviour; assess when a robot foundation model meets the general-purpose AI model criteria for regulatory purposes; apply the three ISO/IEC TR 5469 configurations: AI inside a safety function, non-AI safety mechanisms around AI, and AI used to develop safety functions.
I.D Govern the operating environment and operational design domain	Specify an operational design domain using ISO 34503 and PAS 1883 style taxonomies: environment, people present, tasks, speeds, lighting, weather and connectivity; distinguish segregated, shared, collaborative and public operating environments and the assurance each demands; identify environmental assumptions that become safety case claims and require monitoring; govern operational design domain expansion as a change-control event; apply the operational design domain concept to robots and sites that were not designed with one.
I.E Assess fleets, connectivity and teleoperation architectures	Distinguish standalone, fleet-managed, cloud-dependent and edge-only architectures; assess dependence on connectivity, latency and remote compute for safety-relevant functions; identify teleoperation, remote assistance and human data collection loops within the architecture; assess multi-robot coordination, interoperability and emergent interaction risk in fleets; map architecture choice to accountability allocation across manufacturer, integrator, operator, cloud and teleoperation providers.

DOMAIN

II

Physical Safety Governance and the Machinery and Product Regime

15% | ~13 questions

Purpose

Govern the robot as a machine and as a product. Apply the safety of machinery discipline, conformity assessment and workplace safety law that robots already attract, and integrate AI governance into that regime rather than beside it. This is the domain that separates robotic AI governance from all prior AI governance practice.

Competency	Performance Indicators
II.A Apply the machinery risk assessment discipline	Apply ISO 12100 hazard identification, risk estimation and the three-step risk reduction method; distinguish inherently safe design, safeguarding and complementary measures, and information for use; read and challenge a robot application risk assessment, including task-based assessment; own residual risk acceptance as a documented governance decision with a named accountable person; require reassessment when task, tooling, layout, speed, software, personnel or operating environment changes.
II.B Govern robot safety standards compliance	Apply ISO 10218-1 and ISO 10218-2:2025: robot classes, collaborative applications, functional safety and cybersecurity as a safety precondition; apply ISO 3691-4 and ANSI/A3 R15.08 to automated guided vehicles, autonomous mobile robots and fleets; apply ISO 13482 and its service robot revision to robots operating around the public; track ISO 25785-1 for dynamically stable and humanoid robots and IEC 80601-2-77 and 80601-2-78 for medical robots; identify which standard applies, where all standards are silent, and what a claim of conformity actually evidences.
II.C Read and challenge functional safety claims	Read performance level and safety integrity level claims (ISO 13849-1, IEC 62061, IEC 61508) for each safety function; distinguish IEC 60204-1 stop categories 0, 1 and 2 and what each means for a person near the robot; verify that safety functions are implemented independently of learned components; identify when a safety function with self-evolving behaviour falls outside existing functional safety standards; require evidence rather than assertion for every safety function claimed by a supplier or integrator.
II.D Govern conformity assessment and market placement	Apply the EU Machinery Regulation 2023/1230 from 20 January 2027, including Annex I Part A machinery with safety components that have self-evolving behaviour; distinguish manufacturer, integrator, importer, distributor and user obligations, including when an integrator or deployer becomes the manufacturer of the application; govern CE marking, technical documentation, declaration of conformity, notified body involvement and substantial modification; apply equivalent regimes outside the EU, including OSHA and ANSI/A3 in the United States, UL 3300 and UL 3100 certification, and AS/NZS 4024; track the harmonised standards status under the Machinery Regulation and the AI Act and its effect on presumption of conformity.
II.E Integrate workplace health and safety obligations	Apply workplace safety duties (OSHA General Duty Clause and lockout-tagout, UK and New Zealand health and safety at work duties, EU Framework Directive) to robot deployment; govern maintenance, testing, commissioning and teach modes as the highest-risk states of a robot; apply ISO 45001 and worker consultation, including the AI Act deployer duty to inform workers and their representatives; set competence, training and authorisation requirements for anyone working with, near or on a robot; measure and report injury, near miss and psychosocial indicators with integrity.

DOMAIN

III

Risk, Hazard and Impact Assessment for Embodied AI

14% | ~12 questions

Purpose

Identify, analyse and treat the risks that only exist when AI moves mass through the physical world: hazards from performance insufficiency, learned behaviour, human factors and the environment, alongside conventional AI risk.

Competency	Performance Indicators
III.A Apply an embodied AI risk taxonomy	Classify perception failure, planning and policy failure, control failure, human oversight failure, cyber compromise and organisational failure; classify hazards by kinetic energy, reversibility, detectability and time to harm; distinguish fault-based hazards addressed by functional safety from performance insufficiency hazards addressed by ISO 21448; distinguish robotic risk from model-output risk and route each to the correct control and owner; classify cascading and correlated failure across fleets, shared spaces and supply chains.
III.B Commission hazard analysis for autonomy	Commission and challenge STPA for human and robot systems, including unsafe control actions by software and by people; use HAZOP, FMEA, FTA and HARA outputs as inputs to governance decisions; build and maintain a triggering-condition inventory for perception-driven robots; require hazard analysis to be revisited for every operational design domain expansion and behaviour-changing update; identify hazard analysis that is asserted rather than performed.
III.C Assess learned-policy and foundation-model risk	Assess distribution shift, edge cases, reward misspecification and unknown unsafe scenarios in learned physical behaviour; assess prompt injection and adversarial input paths into language-directed robots; assess risk from fleet learning, over-the-air updates and deployer fine-tuning; apply the ISO/IEC 42001 and ISO/IEC 23894 risk process to learned physical behaviour; set an explicit risk appetite for physical autonomy by robot class and operating environment.
III.D Conduct embodied AI impact assessment	Extend ISO/IEC 42005 style impact assessment to physical harm, property damage, workplace and public impact; assess impact on people who never chose to interact with the robot: bystanders, children, older people, people with disabilities; assess psychosocial, ergonomic, privacy and surveillance impacts of robots in shared spaces; apply proportionality between autonomy granted and assurance required; produce records that satisfy the Impact Assessment control domain and workplace data protection and fundamental rights impact assessment requirements.
III.E Integrate robotic risk into enterprise risk management	Extend the AI risk register to robot and fleet risk types and scoring; map robotic risk onto operational, health and safety, cyber, product liability and third-party risk taxonomies; define severity classification and escalation triggers for physical incidents and near misses; aggregate portfolio-level robot risk for board reporting; apply the Risk, Impact and Trustworthiness dimension of the GAICC Maturity Model.

DOMAIN

IV

13% | ~11 questions

Human Oversight, Control and Human-Robot Interaction

Purpose

Design oversight that is meaningful when a system moves at machine speed in a physical space: control authority, intervention, stop and fallback, teleoperation, and the human operating model and human factors around them.

Competency	Performance Indicators
IV.A Design meaningful human oversight for physical autonomy	Distinguish human in the loop, on the loop and out of the loop for robots and fleets; apply EU AI Act Article 14 principles and ISO/IEC TS 8200 controllability to embodied systems; match oversight mode to kinetic energy, reversibility, operating environment and volume; identify oversight that is nominal: a person present but unable to intervene in time; assess supervisor capacity, reaction time and automation bias.
IV.B Govern stop, fallback and containment	Specify emergency stop, protective stop and safe state design, reachability and testing; define minimal risk condition and minimal risk manoeuvre for mobile and public-facing robots; define geofencing, speed limiting and safety envelopes enforced by runtime monitoring; specify who may halt a robot or a fleet, by what mechanism and within what time; test stop and fallback under realistic conditions and after every behaviour-changing update.
IV.C Govern teleoperation and remote assistance	Distinguish direct teleoperation, remote assistance, supervision and fleet monitoring; set operator-to-robot ratios, latency limits, handover and authority rules; govern operator competence, fatigue, rostering and location, including cross-border operation; govern human data collected through teleoperation and its reuse as training data; disclose the human in the loop honestly to users, workers and the public.
IV.D Govern human-robot interaction and collaborative work	Treat the choice of collaborative operation method (monitored standstill, hand guiding, speed and separation monitoring, power and force limiting) as a governance decision; address deskilling, over-trust, vigilance decay and mode confusion in supervising teams; govern robot-set work pace, ergonomic and psychosocial hazards; apply the People, Functions and Capability layer of the GAICC AI Governance Framework; set competence requirements for operators, supervisors and maintainers of autonomous systems.
IV.E Govern robots in public, domestic and care settings	Assess interaction with children, older people, people with disabilities and animals; govern anthropomorphism, deception and expectation setting, including disclosure that a human may be piloting; govern robots that observe, record or identify people in public and private spaces; apply consent, dignity and autonomy principles in care and companionship deployments; set autonomy promotion and demotion criteria for robots operating among the public.

DOMAIN

V

Assurance, Safety Cases, Verification and Validation

13% | ~11 questions

Purpose

Commission, interpret and act on evidence that a robot is acceptably safe and behaves acceptably, before authorisation and continuously through its operating life.

Competency	Performance Indicators
V.A Build and challenge the safety case	Apply UL 4600 and structured argument notations (GSN, CAE) to autonomous products; apply AMLAS and SACE style arguments to machine-learnt components and autonomy; identify the claim with no evidence, the assumption with no monitor and the argument that is asserted rather than demonstrated; link the safety case to the AI management system, the nine GAICC control domains and the tenth, Agentic and Autonomous AI; treat the safety case as dynamic: re-open it for new sites, embodiments, operating environments and behaviour updates.
V.B Commission verification and validation	Define acceptance criteria for behaviour in the physical world, not only for model accuracy; apply scenario-based testing, simulation, digital twins and physical testing in proportion to risk; govern simulation credibility: assumptions, fidelity, coverage and the sim-to-real gap; require verification and validation coverage across the full operational design domain, including vulnerable road users and edge cases; assess vendor evidence and specify what the vendor can be held to.
V.C Direct evaluation and red teaming of physical AI	Commission semantic safety and refusal evaluation for language-directed robots, including constitution-style benchmarks; scope red team engagements for adversarial input, prompt injection, sensor spoofing and unsafe action; set rules of engagement and physical safety controls for testing near people; interpret findings, set remediation thresholds and require re-testing before autonomy promotion; distinguish model evaluation from system evaluation from field evaluation.
V.D Govern change: updates, fleet learning and regression	Govern over-the-air software and policy updates as safety-relevant change control; require independent verification before a fix is declared closed; maintain regression suites over behaviour, not only model accuracy; govern vendor model version changes, deprecation and forced updates; retain evaluation evidence for assurance, audit, regulators and insurers.
V.E Obtain and use independent assessment and certification	Distinguish self-declaration, second-party assessment, third-party certification and notified body assessment; commission independent safety case assessment against ISO/IEC 15026-2 and recognised industry practice; read type and product certification marks for what they do and do not cover; define safety performance indicators and use them as leading indicators; prepare robotic systems for internal audit and external certification, including ISO/IEC 42001.

DOMAIN

VI

11% | ~10 questions

Cybersecurity, Data and Supply Chain Governance for Robots

Purpose

Treat cybersecurity, data and supply chain provenance as physical safety controls, because a compromised or poorly sourced robot is a hazard, not an IT incident.

Competency	Performance Indicators
VI.A Govern robot cybersecurity as a safety precondition	Apply IEC 62443 zones, conduits, security levels and the role split between asset owner, integrator, product supplier and service provider; apply the ISO 10218:2025 safety-related cybersecurity requirement and ISO/SAE 21434 style threat analysis and risk assessment; threat-model robot-specific attack surfaces: wireless provisioning, middleware, teleoperation links, cloud services and physical ports; require secure update, authentication, telemetry egress control and vulnerability handling from suppliers; apply the EU Cyber Resilience Act: vulnerability and incident reporting from 11 September 2026 and full obligations from 11 December 2027.
VI.B Govern the robot data lifecycle	Inventory sensor, camera, audio, location, biometric and telemetry data collected by robots; govern training, validation and test datasets, including humanoid datasets and teleoperation recordings; apply data protection law to robots that record people: video device guidance, biometrics and data protection impact assessment; set retention, access and cross-border transfer rules for robot data and logs; govern consent and labour conditions across the human data supply chain of teleoperators and annotators.
VI.C Govern logging, traceability and evidence integrity	Specify minimum event data: sensor snapshots, state, commands, interventions, stops, updates and operator actions; protect log integrity against tampering, loss and vendor lock-in; align retention with limitation periods, regulator and insurer requirements; ensure logging spans the fleet, the cloud and the teleoperation layer; balance evidence completeness against privacy and data minimisation.
VI.D Govern supply chain, provenance and third parties	Conduct due diligence on manufacturers, integrators, component suppliers, model providers and cloud and teleoperation vendors; require software bills of materials, hardware provenance and import and export compliance, including restrictions such as the FCC Covered List; assess foreign-jurisdiction data flows and remote access embedded in products; set contractual requirements for security updates, disclosure timelines, audit rights and continuity; monitor third-party behaviour in production rather than relying on attestation.
VI.E Govern physical security, tampering and misuse	Control physical access to robots, controllers, teach pendants, debug ports and charging infrastructure; detect and respond to tampering with sensors, safety devices, configuration and firmware; apply the Responsible Use control domain to prevent weaponisation, harassment and unlawful surveillance using general-purpose robots; govern insider misuse and unauthorised repurposing of robots and fleets; require tamper-evident logging of physical and configuration changes.

DOMAIN

VII

11% | ~10 questions

Operations, Incident Response, Liability and Insurance

Purpose

Run robots safely at scale, respond when a robot harms a person or property, and allocate responsibility across the robot supply chain before that happens rather than after.

Competency	Performance Indicators
VII.A Operate the robot and fleet governance model	Define the fleet operating model, roles, rosters and escalation paths; monitor safety performance indicators, anomalies, near misses and intervention rates; govern site commissioning, layout change and re-commissioning; run drills for stop, evacuation and remote handover; feed monitoring output into the Improve stage of the Direct, Assess, Operate, Improve loop.
VII.B Execute incident response for physical events	Sequence scene safety, medical response, isolation of the robot, evidence preservation, fleet-wide containment, remediation and disclosure; preserve logs, video and physical evidence before remediation destroys them; determine whether the same behaviour is live elsewhere in the fleet and act on it; coordinate operations, safety, legal, communications and executive response under time pressure; support workers and affected people after an incident.
VII.C Manage regulatory notification, recalls and investigations	Apply reporting obligations to workplace regulators, product safety authorities, AI Act serious incident reporting as applied through the machinery regime, Cyber Resilience Act reporting, medical device vigilance and vehicle and aviation crash reporting; manage software recalls and field corrective actions across a fleet; cooperate with and support independent investigation; document and justify decisions not to notify; manage notification across multiple jurisdictions simultaneously.
VII.D Allocate liability and manage insurance	Distinguish the responsibilities of manufacturer, component and model provider, integrator, importer, deployer and operator; apply the EU Product Liability Directive 2024/2853 from 9 December 2026: software and AI as products, presumptions of defect, disclosure of evidence and substantial modification through updates or learning; apply negligence, workers' compensation and product liability theories in common law jurisdictions, including lessons from recent autonomous vehicle verdicts; draft contractual allocation, warranties, update obligations, audit rights and indemnities; assess insurance cover, exclusions and underwriting prerequisites such as standards conformity and logging.
VII.E Learn from incidents and near misses	Conduct post-incident review focused on the control structure and oversight design rather than operator blame; feed findings into the risk register, safety case, control set and autonomy levels; share learning across the fleet and with the supply chain; track corrective and preventive action to closure; report systemic findings to the board and governing body.

DOMAIN

VIII

11% | ~10 questions

Regulatory Landscape, Sector Regimes and Enterprise Scaling

Purpose

Apply law and standards written separately for machines and for AI to systems that are both, sector by sector and jurisdiction by jurisdiction, and scale robotic AI governance from a single pilot to an enterprise portfolio.

Competency	Performance Indicators
VIII.A Apply AI regulation to robots	Apply EU AI Act Article 6 classification to robots: Annex I Section A products (medical devices, vehicles, aviation), Annex I Section B machinery governed through Machinery Regulation delegated acts, and Annex III use cases; apply the timeline as amended by Regulation (EU) 2026/1744: Annex III obligations from 2 December 2027 and Annex I product obligations from 2 August 2028; apply general-purpose AI model obligations to robot foundation models; apply deployer obligations including human oversight, logging, monitoring and worker information; identify clearly where existing regulation is silent on embodied autonomy and advise a defensible position.
VIII.B Apply sector regimes	Medical and surgical robots: EU Medical Device Regulation, FDA predetermined change control plans, AI-enabled device guidance and degree of autonomy classification; autonomous vehicles: UNECE global automated driving systems regulation, NHTSA automated vehicle framework and Standing General Order, UK Automated Vehicles Act 2024; uncrewed aircraft: ISO 21384-3 operational procedures and national beyond visual line of sight rules; agriculture: ISO 18497 autonomous operating zones and supervisory requirements; defence and security robots: the CCW process on lethal autonomous weapons and the principle that responsibility cannot be transferred to a machine, at awareness level.
VIII.C Apply jurisdictional regimes beyond the EU	United States: federal posture and pre-emption debate, state AI laws, OSHA, NHTSA, FAA, FDA and the FCC Covered List for foreign-produced robotic devices; China: the Humanoid Robots and Embodied Intelligence Standards System (2026 edition), Cybersecurity Law AI provisions and generative AI measures; Korea AI Basic Act high-impact AI duties; Japan AI Promotion Act and the AISI guide to safety evaluation of AI robotics; Singapore, United Kingdom, Australia and New Zealand approaches and where they rely on existing safety and privacy law; international instruments: OECD AI Principles, Council of Europe Framework Convention, UN Global Dialogue on AI Governance.
VIII.D Apply management system standards to robotic operation	Map ISO/IEC 42001 clauses and Annex A controls onto the robot lifecycle from concept to decommissioning; apply the nine GAICC control domains and the tenth, Agentic and Autonomous AI, to a robot portfolio; integrate the AI management system with ISO 45001, ISO 9001, ISO/IEC 27001 and IEC 62443 programmes; apply the NIST AI RMF Govern, Map, Measure and Manage functions to robotic risk; extend an existing AI management system scope to cover robots without rebuilding it.
VIII.E Scale robot governance and advise the board	Operate a robot and fleet registry with autonomy, operating environment and risk tiers, and apply tiered governance proportionate to risk; apply the GAICC Maturity Model dimensions and the seven phases of the GAICC Implementation Roadmap, including Phase 7, Adapt and extend, where frontier autonomous credentials sit; track and anticipate standards and regulatory development (ISO 25785-1, ISO/IEC TS 22440, humanoid standards, harmonised standards) and act before obligations bind; report portfolio risk, incident trend and autonomy distribution to the board and define board-level risk appetite for physical autonomy; escalate clearly where authority granted exceeds assurance held, and present the business case for robot governance investment.

Eligibility Requirements

GAICC RAIGP is an advanced credential. The one hard requirement is training: 32 hours of structured RAIGP training completed by any of the three recognised routes before the examination.

Recommended background

- The GAICC Certified Professional in AI Governance (CPAIG) or the GAICC Agentic AI Governance Professional (AAIGP), or an equivalent AI governance credential. RAIGP assumes working knowledge of AI governance fundamentals and does not re-teach them.
- Professional experience in one or more of: robotics or autonomous systems delivery, machinery or functional safety, health and safety, AI governance, risk, compliance, audit, security, product compliance, insurance or law. Experience is advisory. It supports readiness and is not a barrier to access.
- Candidates from a machinery or functional safety background (for example holders of CMSE, TÜV Functional Safety Engineer, CFSE or CFSP, or UL-CASP) will find Domain II familiar and should expect Domains I, III, V and VIII to carry the AI governance content they have not met. Candidates from an AI governance background should expect the reverse.
- No engineering qualification is required. The examination requires the candidate to read and challenge engineering evidence, not to produce it.

Training requirement and routes

The 32-hour training requirement may be met by any one of three routes. All three are equivalent for eligibility purposes and no route, including GAICC's own, confers any advantage in the examination.

Route	Description
1. GAICC self-paced course	The 32-hour RAIGP course completed in the candidate's own time on the GAICC hub.
2. GAICC-authorised Certified Instructor or Authorised Training Partner	Instructor-led delivery of the 32-hour programme by an authorised partner or an authorised GAICC Certified Instructor.
3. A GAICC-recognised institution	32 hours of RAIGP training delivered by an institution recognised by GAICC for this purpose.

Who it is for

AI governance leads, robotics and automation programme leaders, health and safety and functional safety managers, risk and compliance managers, internal and external auditors, product compliance and regulatory affairs professionals, security and OT security architects, fleet and operations managers for autonomous systems, insurers and claims professionals, legal and privacy professionals, and consultants advising on robot and autonomous system deployment.

Certification Maintenance & CPD Requirements

The GAICC RAIGP certification is valid for three (3) years. During each cycle, certified professionals earn a minimum of 60 CPD hours, allocated across the three competencies of the GAICC AI Competence Triangle:

Competence	Focus	Minimum
Technology	Robot and autonomous system authorisation, risk and hazard assessment, evaluation, assurance and security work	27 hours
Humanity	Human oversight, human-robot interaction, ethics, worker and public impact, and responsible-use practice	12 hours
Strategy	Portfolio governance, board advisory, standards and policy contribution, and recognised learning	21 hours
TOTAL	**Minimum required in each 3-year certification cycle**	**60 CPD Hours**

Hours may be earned through robot and autonomous system authorisation, risk and hazard assessment, oversight and safety case work, evaluation, audit, incident response, standards and policy contribution, and recognised learning. The renewal period, CPD allocation and renewal fee are stated in the GAICC RAIGP Candidate Handbook, which is the authority.

Examination Fees

Examination, membership and renewal fees are published in the GAICC RAIGP Candidate Handbook and on the GAICC certification body website (certifications.gaicc.org/fees). 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, including commercial interests in a robot, integrator or platform under review.
2. Proportionate Autonomy	Never recommend or approve a level of physical autonomy that exceeds the assurance evidence held, and never allow a safety function to depend on a component whose behaviour has not been verified. Where authority and evidence diverge, say so in writing.
3. Human Life, Health and Wellbeing	Treat the safety of workers, users and bystanders, including people who never chose to be near the robot, as the first obligation. Physical harm is irreversible; commercial pressure never justifies a disabled safeguard or an untested update.
4. Transparency and Accountability	Promote reconstructable robot behaviour. Ensure a named human remains accountable for every autonomous action, and disclose honestly when a human is piloting or assisting a robot that appears autonomous.
5. Data Protection and Privacy	Uphold confidentiality and data protection principles across sensor data, recordings of people, teleoperation footage, training data and logs, consistent with applicable laws and international standards.
6. Professional Competence	Maintain current knowledge across both machinery safety and AI governance in a field changing faster than its standards. Know the limits of one's competence and involve functional safety, security and legal specialists where the decision requires them.
7. Reporting and Mitigation of Misuse	Take appropriate action when encountering unsafe deployments, disabled or bypassed safety functions, suppressed or falsified incident and injury data, robots repurposed for harm, or violations of applicable regulation or professional standards.
8. Global Responsibility	Recognise that a robot may be manufactured in one jurisdiction, trained in a second and operated in a third. Apply governance standards that protect individuals regardless of where the robot was made or where the person stands.

Frequently Asked Questions

What is the GAICC RAIGP?

An advanced practitioner credential for professionals who authorise, oversee, assure and stop AI systems that move through the physical world. It governs autonomy with a body: robots, fleets, humanoids, autonomous vehicles and uncrewed aircraft.

Who should pursue RAIGP?

AI governance leads, robotics and automation programme leaders, health and safety and functional safety managers, risk and compliance managers, internal and external auditors, product compliance and regulatory affairs professionals, security and OT security architects, fleet and operations managers for autonomous systems, insurers and claims professionals, legal and privacy professionals, and consultants advising on robot and autonomous system deployment.

Do I need CPAIG or AAIGP first?

CPAIG or AAIGP, or an equivalent AI governance credential, is strongly recommended but not required. RAIGP assumes working knowledge of AI governance fundamentals and does not re-teach them.

Do I need to be an engineer?

No. RAIGP requires you to read, challenge and act on engineering evidence such as risk assessments, functional safety claims and safety cases. It does not require you to produce them or to perform calculations.

How does RAIGP differ from AAIGP?

AAIGP governs software agents that act on digital systems: authority, identity, delegation, containment and evidence. RAIGP governs systems that act on the physical world, where the machinery safety regime, kinetic hazards, workplace safety law, product liability and physical incident response apply. The two credentials share the GAICC framework and the same examination format and are designed to be held together.

How does RAIGP differ from a functional safety credential?

Functional safety credentials certify engineering competence in deterministic safety functions to a performance or integrity level. RAIGP certifies governance competence across the whole system: learned behaviour, human oversight, assurance, security, liability and regulation, and how they integrate with functional safety. RAIGP holders work alongside functional safety engineers; they do not replace them.

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

Frequently Asked Questions (continued)

Does RAIGP cover autonomous vehicles and drones?

Yes, at governance level. Autonomous vehicles and uncrewed aircraft are embodied AI systems with their own sector regimes, and Domain VIII applies those regimes. RAIGP does not certify vehicle homologation or remote pilot competence.

Does RAIGP cover military robots?

Only at awareness level. Domain VIII covers the international process on lethal autonomous weapons and the principle that responsibility cannot be transferred to a machine. RAIGP does not train the design or deployment of weapons.

What is the exam format?

100 scenario-based multiple-choice questions in 2 hours 30 minutes, AI-proctored on the GAICC hub at hub.gaicc.org. Pass mark is 70% of scored questions.

When do I know if I have passed?

A provisional result is displayed on screen on completion, with domain-level feedback. The Certification Decision Authority reviews it and confirms the certification decision within 72 hours.

How long is the certification valid?

3 years. Renewal requires 60 CPD hours per cycle, allocated across the GAICC AI Competence Triangle, plus a renewal application and fee as stated in the Candidate Handbook.

What digital credentials are provided?

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

How does RAIGP relate to the GAICC Framework?

RAIGP operationalises the GAICC AI Governance Framework for hybrid human and autonomous machine teams. It maps to the Autonomy and Human Oversight trustworthiness characteristic, the Agentic and Autonomous AI control domain, the Maturity Model dimensions, and Phase 7, Adapt and extend, of the Implementation Roadmap.

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

Global AI
Certification Council

GAICC RAIGP

ROBOTIC AI GOVERNANCE PROFESSIONAL

For professionals who authorise, oversee and are accountable for AI systems that move through the physical world.

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

Examination Content Outline | GAICC-ECO-RAIGP-001 | 1st Edition | 2026