Global AI Certification Council

GAICC TRAINING · COURSE CURRICULUM

[EAIGP]

Engineering AI Governance Professional

32-Hour Course Curriculum

1st Edition | 2026 | v1.0

Course	Engineering AI Governance Professional (EAIGP) certification course
Document code	GAICC-CUR-EAIGP-001
Version	1.0 · 23 October 2026
Duration	4 days · 32 contact hours · 32 CPD hours
Prepares for	GAICC Engineering AI Governance Professional (GAICC-EAIGP)

1. Course overview

The four-day, 32-contact-hour course moves from accountability and regulation to safety engineering, lifecycle control, assurance, security, oversight and the governance of generative, agentic and physical AI. Each module is built around engineering cases drawn from automotive, aerospace, machinery and robotics, process industries, utilities, infrastructure, semiconductors and telecom, and from the digital engineering services firms that build and validate AI for them. Learners produce working artefacts, including classification decisions, hazard analyses, safety case fragments, AIBOMs, V&V plans and agent control matrices, which they take back to their organisations. A horizon-scanning segment closes each day so that learners can track standards in drafting and rules with later application dates.

Duration **4 days · 32 contact hours**	**CPD** **32 CPD hours on completion**	**Modules** **19 modules plus capstone**
Delivery **In person, live online, or GAICC self-paced**	**Class size** **Recommended maximum of 24 learners**	**Leads to** **GAICC Engineering AI Governance Professional (GAICC-EAIGP)**

Course learning outcomes

By the end of the course, learners will be able to:

1. Map engineering AI use cases to regulatory routes, conformity assessment and liability exposure across markets.
2. Integrate machine learning into IEC 61508, ISO 26262, SOTIF and ISO/PAS 8800 safety lifecycles.
3. Build safety cases and confidence arguments that hold for learned components within defined ODDs.
4. Govern datasets, models and AIBOMs under configuration control across OTA updates and long asset lives.
5. Plan verification and validation using simulation, digital twins, robustness testing and run-time monitors.
6. Secure AI in operational technology and meet Cyber Resilience Act vulnerability reporting duties.
7. Set autonomy limits, approval gates and evidence for AI coding agents and agentic engineering workflows.
8. Design human oversight, field monitoring and incident reporting that protect workers, users and communities.

Who should attend

- Functional safety and systems safety engineers
- Chartered and professional engineers signing off designs
- Product compliance and homologation leads
- Verification, validation and test engineers
- ML engineers and MLOps leads in products
- OT, ICS and product cybersecurity specialists
- Quality and integrated management system managers

- Digital engineering and IT services delivery leads

2. Course at a glance

Module	Title	Domains	Hours
Day 1	**Accountability and Product Regulation**	Domains I, II	**8.0 h**
M01	Engineering AI landscape and professional duty	I	1.5 h
M02	Governance roles, AI inventory and liability exposure	I	1.5 h
M03	EU AI Act classification after the Omnibus	II	2.0 h
M04	Machinery Regulation, Cyber Resilience Act and liability	II	1.5 h
M05	Type-approval, aviation and export controls	II	1.5 h
Day 2	**Safety Engineering and Lifecycle**	Domains III, IV	**8.0 h**
M06	Hazard analysis and operational design domain	III	2.0 h
M07	ML in functional safety and SOTIF lifecycles	III	2.0 h
M08	Safety cases and confidence arguments	III	1.0 h
M09	Data, provenance and AI bills of materials	IV	1.5 h
M10	Model change, OTA updates and self-evolution	IV	1.5 h
Day 3	**Assurance and Cyber Resilience**	Domains V, VIII, VI	**8.0 h**
M11	V&V planning, simulation and digital twins	V	2.0 h
M12	Robustness, uncertainty and run-time monitors	V	1.5 h
M13	Validating AI-generated code and tests	V, VIII	1.0 h
M14	Securing AI in operational technology	VI	2.0 h
M15	CRA reporting and AI supply chain security	VI	1.5 h
Day 4	**Oversight, Agents and Capstone**	Domains VII, VIII, I, II, III, IV, V, VI	**8.0 h**
M16	Human oversight, ethics and societal impact	VII	2.0 h
M17	Generative and agentic AI in engineering workflows	VIII	2.0 h
M18	Physical AI, integrated systems and field monitoring	VIII	2.0 h
M19	Capstone and exam readiness	I, II, III, IV, V, VI, VII, VIII	2.0 h
Total			**32.0 h**

3. Detailed curriculum

DAY 1

Accountability and Product Regulation

Establish who is accountable for engineering AI and which product, AI, cybersecurity and liability rules apply, in which order and from when.

M01 Engineering AI landscape and professional duty · 1.5 hours

Domains I · Competencies EAIGP-1.1, EAIGP-1.2

Learning outcomes	• Map AI use cases across design, production, operation and maintenance • Rate use cases for safety relevance and irreversibility of harm • Apply professional body guidance on AI-assisted work and sign-off
Topics	Generative design, simulation surrogates and digital twins · Perception, autonomy, robotics and process control · Predictive maintenance and inspection · AI-generated code and tests · Engineering NZ, Engineering Council and RAEng, Engineers Europe and NSPE guidance · Recording AI use in engineering records
Activity	A chartered structural engineer is asked to sign off a generative design for a pedestrian bridge; learners decide what independent checks, records and limitations must exist before signature.

M02 Governance roles, AI inventory and liability exposure · 1.5 hours

Domains I · Competencies EAIGP-1.3, EAIGP-1.4, EAIGP-1.5

Learning outcomes	• Define decision rights for AI model release and change • Build an AI inventory that links to hazard logs and AIBOMs • Identify professional indemnity and contractual gaps for AI deliverables
Topics	Design authority and safety manager roles · Independent assessment and competence · AI inventory attributes and unrecorded AI · Insurer AI exclusions and disclosure · Warranties and limitation clauses
Activity	Learners build an inventory entry and decision-rights matrix for a predictive maintenance model at a utility, then review a supply contract for AI liability gaps.

M03 EU AI Act classification after the Omnibus · 2.0 hours

Domains II · Competencies EAIGP-2.1, EAIGP-2.5

Learning outcomes	• Classify AI-enabled systems under Article 6 using the narrowed safety component test • Distinguish Annex I Section A, Section B and Annex III routes and dates • Explain the role of EN 18286 and pending harmonised standards
Topics	Regulation (EU) 2026/1744 and revised dates · Narrowed safety component definition · Section A versus Section B products · Registration of non-high-risk assessments · EN 18286 and presumption of conformity · GB and South Korea approaches
Activity	Learners classify six systems, including a lift monitoring function, an AI quality inspection camera, a grid balancing optimiser and a dosing controller, and justify each route and date.

M04 Machinery Regulation, Cyber Resilience Act and liability · 1.5 hours

Domains II · Competencies EAIGP-2.2, EAIGP-2.3

Learning outcomes	• Identify self-evolving safety functions requiring third-party assessment • Apply essential requirements 1.1.9 and 1.2.1 to AI control systems • Plan CRA and PLD obligations for AI-enabled products
Topics	Annex I Part A points 5 and 6 · Protection against corruption and control system limits · Application from 20 January 2027 · CRA essential requirements and support periods · PLD software, updates and disclosure
Activity	Learners prepare the conformity plan for a collaborative robot cell with AI vision placed on the EU market in 2027, including notified body engagement and CRA support period.

M05 Type-approval, aviation and export controls · 1.5 hours

Domains II · Competencies EAIGP-2.4, EAIGP-2.5, EAIGP-2.6

Learning outcomes	• Relate UNECE and EASA regimes to AI Act Section B • Screen chips, compute and model weights for export control status
Topics	UN R155, R156 and R185 · EASA Concept Paper and NPA 2025-07 · Learned versus learning AI · US advanced chip controls and model weight status · Horizon scan: Day 1 regulation watch list
Activity	Learners assess whether an offshore delivery team may access an advanced chip training cluster and aerospace technical data for a client, and record the decision.

DAY 2

Safety Engineering and Lifecycle

Bring machine learning inside functional safety and SOTIF practice, and keep datasets and models under engineering configuration control.

M06 Hazard analysis and operational design domain · 2.0 hours

Domains III · Competencies EAIGP-3.1, EAIGP-3.2

Learning outcomes	• Apply STPA and HAZOP to systems with learned components • Specify an ODD and define behaviour on ODD exit • Link ODD attributes to data and test coverage
Topics	STPA unsafe control actions · HAZOP guidewords for perception outputs · ML failure modes and long tail · ODD taxonomies · Minimal risk conditions and fallback
Activity	Learners run an STPA on an autonomous mobile robot in a semiconductor fab and specify its ODD, including lighting, floor and crowding conditions.

M07 ML in functional safety and SOTIF lifecycles · 2.0 hours

Domains III · Competencies EAIGP-3.3, EAIGP-3.4, EAIGP-3.6

Learning outcomes	• Integrate ML activities into IEC 61508 and ISO 26262 lifecycles • Identify triggering conditions using SOTIF and ISO/PAS 8800 • Allocate integrity levels and architectural mitigations around ML
Topics	ISO/IEC TR 5469 classes and usage levels · ISO/IEC TS 22440 and ISO 26262 edition 3 direction · SOTIF scenario areas · ISO/PAS 8800 safety requirements · SIL, ASIL and DAL allocation · ED-324/ARP6983 ML constituent · Rail software and EN 50716
Activity	Learners decompose a pedestrian detection function into an ML channel and an independent monitor, allocate ASILs and list SOTIF triggering conditions.

M08 Safety cases and confidence arguments · 1.0 hours

Domains III · Competencies EAIGP-3.5

Learning outcomes	• Build a safety case fragment with an explicit confidence argument • Identify defeaters and assurance deficits
Topics	Goal Structuring Notation · UL 4600 and ISO/TS 5083 · Safety performance indicators · Maintaining the case through life
Activity	Learners draft and peer-challenge a safety case fragment for a predictive maintenance model after a false negative on a critical pump.

M09 Data, provenance and AI bills of materials · 1.5 hours

Domains IV · Competencies EAIGP-4.1, EAIGP-4.2, EAIGP-4.3

Learning outcomes	• Specify datasets linked to ODD and safety requirements • Produce an AIBOM meeting G7 minimum elements • Align MLOps controls with configuration management
Topics	ISO/IEC 5338 lifecycle processes · Dataset specification and labelling quality · Synthetic and simulated data · SPDX 3.0 and CycloneDX ML-BOM · Reproducibility records
Activity	Learners write a dataset specification and AIBOM for a weld inspection model trained partly on synthetic images.

M10 Model change, OTA updates and self-evolution · 1.5 hours

Domains IV · Competencies EAIGP-4.4, EAIGP-4.5

Learning outcomes	• Run change impact analysis for a retrained model • Set bounds for continuously learning systems • Write supplier flow-down requirements for model evidence
Topics	UN R156 and RXSWIN · Staged rollout and rollback · Learned versus learning systems · Long asset life and obsolescence · Horizon scan: Day 2 standards in drafting
Activity	Learners decide whether an OTA update of a perception model under R156 needs approval extension, and what the safety case must show before release.

DAY 3

Assurance and Cyber Resilience

Produce verification evidence that holds up, including for AI-generated code and digital twins, and secure AI in operational technology.

M11 V&V planning, simulation and digital twins · 2.0 hours

Domains V · Competencies EAIGP-5.1, EAIGP-5.2, EAIGP-5.6

Learning outcomes	• Write a V&V plan with acceptance criteria and independence • Justify sim-to-real transfer with correlation evidence • Judge digital twin fidelity before using twin results as evidence
Topics	Requirements-based and data-based evidence · Scenario-based testing · SIL and HIL configurations · Simulator qualification · ISO 23247 and digital thread · Twin validity envelope
Activity	Learners review a V&V plan for a plant control surrogate model and identify where digital twin evidence exceeds its validated range.

M12 Robustness, uncertainty and run-time monitors · 1.5 hours

Domains V · Competencies EAIGP-5.3, EAIGP-5.4

Learning outcomes	• Select robustness and uncertainty methods for a perception model • Specify an independent run-time monitor and safety envelope
Topics	ISO/IEC 24029-2 formal methods · ISO/IEC 25059 quality characteristics · Calibration and out-of-distribution detection · Safety envelopes and simplex architectures
Activity	Learners design a run-time monitor that places an AI-guided crane into a safe state when model uncertainty or ODD conditions breach limits.

M13 Validating AI-generated code and tests · 1.0 hours

Domains V, VIII · Competencies EAIGP-5.5, EAIGP-8.1

Learning outcomes	• Assess AI-generated tests for oracle correctness and traceability • Classify AI coding tools for tool confidence
Topics	MISRA and CERT conformance · Tool qualification · The oracle problem · Limits of coverage arguments
Activity	An AI coding agent writes regression tests for chip validation against a digital twin; learners sample the tests, find oracles that mirror the twin, and set acceptance conditions.

M14 Securing AI in operational technology · 2.0 hours

Domains VI · Competencies EAIGP-6.1, EAIGP-6.2, EAIGP-6.3

Learning outcomes	• Place AI components in IEC 62443 zones and conduits • Threat model an AI-enabled system using MITRE ATLAS • Specify integrity controls against poisoning and corruption
Topics	IEC 62443 security levels · AI in OT principles · Adversarial patches and evasion · Prompt injection into engineering assistants · Model signing and secure update
Activity	Learners threat model a cloud-trained anomaly detection model feeding setpoint advice to a water treatment SCADA system and redesign its conduits.

M15 CRA reporting and AI supply chain security · 1.5 hours

Domains VI · Competencies EAIGP-6.4, EAIGP-6.5

Learning outcomes	• Run a CRA 24-hour and 72-hour reporting exercise • Assess third-party model and dataset security • Apply ISO 10218:2025 cybersecurity provisions to robot cells
Topics	Single reporting platform · Coordinated vulnerability disclosure · CRA, NIS2 and sector reporting · Pretrained model supply chain risks · Horizon scan: Day 3 security watch list
Activity	In a timed exercise, learners prepare the early warning and notification for an actively exploited model poisoning vulnerability in an industrial gateway.

DAY 4

Oversight, Agents and Capstone

Design oversight that works in process time, govern generative, agentic and physical AI, and integrate everything into a defensible governance case.

M16 Human oversight, ethics and societal impact · 2.0 hours

Domains VII · Competencies EAIGP-7.1, EAIGP-7.2, EAIGP-7.3, EAIGP-7.4, EAIGP-7.5

Learning outcomes	• Design oversight and takeover within process safety time • Identify automation bias risks in HMI and review processes • Assess workforce, environmental and community impact including iwi and hapū engagement
Topics	ISO/IEC TS 8200 controllability · Automation bias and skill fade · IEEE 7000 and IEEE 7009 · Worker consultation and cobots · Energy use of AI · Te Tiriti o Waitangi and infrastructure engagement
Activity	Learners assess an AI-assisted flood gate control scheme for oversight timing, operator interface, fail-safe behaviour and engagement with mana whenua.

M17 Generative and agentic AI in engineering workflows · 2.0 hours

Domains VIII · Competencies EAIGP-8.1, EAIGP-8.2

Learning outcomes	• Set verification levels for AI-generated artefacts by integrity level • Design approval gates, least privilege and reversibility for engineering agents • Specify an agent registry and audit trail
Topics	AI coding agents and generative design · IP, open source and standards licence terms · Joint agency agentic AI guidance · OWASP Agentic Top 10 · Kill switches and rollback · Agents touching PLC and SCADA
Activity	Learners build a control matrix for an agent that proposes PLC logic changes and releases design packages, deciding which actions need human approval.

M18 Physical AI, integrated systems and field monitoring · 2.0 hours

Domains VIII · Competencies EAIGP-8.3, EAIGP-8.4, EAIGP-8.5, EAIGP-8.6

Learning outcomes	• Assess robot foundation models and humanoids against current standards • Map ISO/IEC 42001 and EN 18286 into existing management systems • Define services-provider roles, evidence packs and field monitoring duties
Topics	ISO 10218:2025 and ISO 25785-1 · Vision-language-action models · Integrated management systems · Article 25 and substantial modification · R185 in-service reporting and post-market monitoring · Horizon scan: Day 4 future watch
Activity	Learners prepare the client evidence pack and field monitoring plan a services firm owes after delivering an AI vision function for a collaborative robot cell.

M19 Capstone and exam readiness · 2.0 hours

Domains I, II, III, IV, V, VI, VII, VIII · Competencies EAIGP-1.2, EAIGP-2.1, EAIGP-3.5, EAIGP-4.4, EAIGP-5.6, EAIGP-6.4, EAIGP-7.1, EAIGP-8.2, EAIGP-8.5

Learning outcomes	• Integrate classification, safety, assurance and security decisions into one governance case • Defend the case before a panel acting as regulator, client and signing engineer • Practise scenario items across all eight domains
Topics	Capstone case work · Panel challenge · Exam blueprint walk-through · Timed practice items
Activity	Teams present a governance case for an AI-enabled inspection robot and respond to challenge from a panel acting as notified body, client and chartered engineer.

4. Capstone and exam readiness

Teams act for a digital engineering services firm that has delivered an autonomous inspection robot for a water treatment plant, with perception models retrained monthly and control software partly written by an AI coding agent and validated against a digital twin. They must classify the system, present the hazard analysis, ODD and safety case, show configuration and AIBOM control, defend the V&V and security evidence, and set oversight and agent controls. A panel acting as notified body, client and chartered engineer challenges the case.

Assessment for learning

- A short knowledge check at the end of each module, mapped to competency codes, with feedback.
- A daily scenario review in which teams defend their decisions to the instructor.
- A full timed mock examination of 80 questions in 120 minutes, available on the GAICC learning platform after Day 4, with feedback by domain.
- Course completion requires attendance of all 32 contact hours (or completion of all self-paced modules) and submission of the capstone.

5. Learner toolkit

Learners leave with practical templates they can use at work from day one:

- Engineering AI use case and regulatory route mapper
- AI Act and Machinery Regulation classification decision tree
- ML-adapted STPA and HAZOP worksheet
- Operational design domain specification template
- Safety case pattern library for learned components
- Dataset specification and provenance record
- AI bill of materials template (SPDX 3.0 and CycloneDX)
- Model change impact analysis checklist for OTA and field updates
- V&V plan template for AI-enabled systems
- AI coding agent and agentic workflow control matrix
- CRA vulnerability reporting playbook
- Services-provider client evidence pack template

6. Future watch

A recurring horizon-scanning segment keeps the course current. It covers emerging technology, regulation and practice in engineering, manufacturing, mobility, infrastructure and industrial technology, and is refreshed at every curriculum review:

- ISO 26262 edition 3, IEC 61508 edition 3 and ISO/IEC TS 22440
- Machinery Regulation delegated acts on AI due by 2 August 2028
- Final Article 6 guidelines and further AI Act harmonised standards (EN 18228, EN 18229, EN 18284)
- EASA Concept Paper Issue 03, ED-324/ARP6983 and assurance of learning AI
- Humanoid and legged robots under ISO 25785-1

- Vision-language-action and robot foundation models in control loops
- Continuously learning systems and predetermined change limits
- Sovereign models, compute export controls and model weight security

7. Delivery requirements

Requirement	Standard
Instructor	GAICC Certified Instructor holding the EAIGP (or, during launch, a GAICC-approved subject matter expert) with at least five years of AI governance, risk, assurance or regulatory experience in engineering, manufacturing, mobility, infrastructure and industrial technology.
Materials	Current GAICC courseware only: slides, learner workbook, activity book, case packs and toolkit templates.
Live online	Camera-on participation, breakout rooms for team activities, and sessions of no more than four hours without a substantial break.
Self-paced	Equivalent content and activities, with completion tracked per module and contact hours verified by the platform.
Enterprise delivery	Case studies may be tailored to an organisation's own AI portfolio, delivery model and client obligations, provided all modules and competencies are covered in full.
Impartiality	Instructors have no access to live examination items and do not examine or certify their own learners.

8. Competency coverage matrix

Every task in the Examination Content Outline is taught in at least one module.

Code	Task	Modules
EAIGP-1.1	Map AI use cases across the engineering lifecycle, from generative design and simulation surrogates to perception, process control and inspection, and rate each for safety relevance.	M01
EAIGP-1.2	Apply professional duty of care to AI-assisted engineering work so that a competent engineer verifies, owns and signs off every safety-related output and records AI use.	M01, M19
EAIGP-1.3	Define engineering AI governance roles, decision rights and escalation paths linking design authority, functional safety, cybersecurity, quality and responsible AI functions.	M02
EAIGP-1.4	Establish and maintain an AI inventory covering embedded, enterprise and engineering-tool AI, recording owner, intended purpose, regulatory route and integrity level.	M02
EAIGP-1.5	Assess contractual, liability and professional indemnity exposure from AI use, including insurer AI exclusions, client warranties and allocation of responsibility in supply contracts.	M02
EAIGP-2.1	Classify AI-enabled systems under EU AI Act Article 6, applying the narrowed safety component test and distinguishing Annex I Section A, Section B and Annex III routes.	M03, M19
EAIGP-2.2	Plan Machinery Regulation conformity for AI-enabled machinery, including third-party assessment of self-evolving safety functions and essential requirements on corruption and control systems.	M04
EAIGP-2.3	Determine Cyber Resilience Act and Product Liability Directive obligations for AI-enabled products with digital elements, including updates, support periods and disclosure risk.	M04
EAIGP-2.4	Interpret sector type-approval and certification regimes for AI in vehicles and aviation, including UNECE R155, R156 and R185 and EASA trustworthy AI guidance.	M05
EAIGP-2.5	Use harmonised standards and international regimes, including EN 18286, GB machinery and UKCA rules and the South Korea AI Basic Act, to plan multi-market compliance.	M03, M05
EAIGP-2.6	Screen AI hardware, compute, model weights and engineering data transfers for export control, sanctions and technology security obligations in global delivery models.	M05
EAIGP-3.1	Conduct hazard analysis for AI-enabled systems using STPA, HAZOP and FMEA adapted for ML failure modes, functional insufficiencies and unsafe control actions.	M06
EAIGP-3.2	Specify the operational design domain and its monitoring, covering environmental, behavioural and data conditions, and define system behaviour on ODD exit.	M06
EAIGP-3.3	Integrate ML development into IEC 61508 and ISO 26262 safety lifecycles using ISO/IEC TR 5469, while tracking ISO/IEC TS 22440 and ISO 26262 edition 3.	M07
EAIGP-3.4	Apply ISO 21448 SOTIF and ISO/PAS 8800 to identify and reduce functional insufficiencies and triggering conditions in AI perception and decision functions.	M07
EAIGP-3.5	Construct safety cases with explicit confidence arguments for learned components, using UL 4600, ISO/TS 5083 and goal structuring methods, and maintain them through life.	M08, M19

Code	Task	Modules
EAIGP-3.6	Allocate SIL, ASIL or DAL where ML sits, using architectural mitigations such as monitors, diversity and safety envelopes, and the ED-324/ARP6983 ML constituent approach.	M07
EAIGP-4.1	Implement ISO/IEC 5338 AI lifecycle processes and MLOps controls aligned with engineering configuration management, systems engineering and quality systems.	M09
EAIGP-4.2	Specify dataset requirements and quality criteria, and establish provenance and lineage for training, validation and test data, including synthetic and simulated data.	M09
EAIGP-4.3	Produce and maintain AI bills of materials using SPDX 3.0 or CycloneDX ML-BOM, meeting G7 minimum elements and supporting customer and regulator requests.	M09
EAIGP-4.4	Control model versions and change impact across over-the-air and field updates, linking each release to safety case, type-approval and RXSWIN records.	M10, M19
EAIGP-4.5	Bound self-evolving and continuously learning systems, manage long asset life against fast model change, and flow governance requirements down to suppliers.	M10
EAIGP-5.1	Develop V&V plans for AI-enabled systems that define acceptance criteria, independence, test environments and evidence linked to safety and regulatory requirements.	M11
EAIGP-5.2	Apply scenario-based, simulation, software-in-the-loop and hardware-in-the-loop testing, and justify sim-to-real transfer with correlation evidence.	M11
EAIGP-5.3	Assess model robustness, quality and uncertainty using ISO/IEC 24029, ISO/IEC 25059 and uncertainty quantification methods.	M12
EAIGP-5.4	Specify run-time monitors and safety envelopes that detect anomalous AI behaviour and enforce safe states independently of the learned component.	M12
EAIGP-5.5	Validate AI-generated code, tests and designs against coding standards, requirements traceability and test oracles, and qualify the AI tools used.	M13
EAIGP-5.6	Assess digital twin fidelity, validity range and digital thread integrity before twin results are used as verification or certification evidence.	M11, M19
EAIGP-6.1	Architect AI deployments in OT using IEC 62443 zones, conduits and security levels, applying the joint agency principles for secure AI integration in OT.	M14
EAIGP-6.2	Threat model AI-enabled systems for adversarial ML, including evasion, physical adversarial patches, model extraction and prompt injection, using MITRE ATLAS.	M14
EAIGP-6.3	Protect training data, models and update channels against poisoning and corruption, meeting Machinery Regulation 1.1.9 and AI Act accuracy, robustness and cybersecurity expectations.	M14
EAIGP-6.4	Operate vulnerability handling and incident reporting under the Cyber Resilience Act, including 24-hour early warnings and 72-hour notifications for actively exploited vulnerabilities and severe incidents.	M15, M19
EAIGP-6.5	Secure the AI supply chain and robotic systems, covering third-party models, datasets and toolchains and the ISO 10218:2025 cybersecurity requirements for industrial robots.	M15
EAIGP-7.1	Design human oversight and controllability that operate within process safety time, using ISO/IEC TS 8200 and defined intervention, override and takeover modes.	M16, M19

Code	Task	Modules
EAIGP-7.2	Assess HMI design for automation bias, mode confusion and skill fade, and build a safety culture in which people challenge AI outputs.	M16
EAIGP-7.3	Apply IEEE 7000 value-based engineering and IEEE 7009 fail-safe design to embed ethical requirements and safe failure behaviour in autonomous systems.	M16
EAIGP-7.4	Evaluate worker safety and workforce impact of AI and automation, including consultation, competence and psychosocial risk, under health and safety duties.	M16
EAIGP-7.5	Assess the environmental, energy and community impact of engineering AI, including meaningful engagement with iwi, hapū and affected communities on infrastructure projects.	M16
EAIGP-8.1	Govern AI coding agents and generative design tools that produce safety-critical artefacts, covering verification, traceability, intellectual property and licence terms of standards and data.	M13, M17
EAIGP-8.2	Set controls for agentic engineering workflows that touch PLC, SCADA or design release, including least privilege, approval gates, reversibility, sandboxing and an agent registry.	M17, M19
EAIGP-8.3	Assess physical AI, collaborative and mobile robots and humanoids, applying ISO 10218:2025, tracking ISO 25785-1, and integrating foundation models into robot control safely.	M18
EAIGP-8.4	Design integrated management systems combining ISO/IEC 42001, EN 18286, ISO 9001, IATF 16949 or AS9100, functional safety management and a cybersecurity management system.	M18
EAIGP-8.5	Determine services-provider obligations under the AI Act, including provider versus supplier roles, substantial modification and validation evidence packs for clients.	M18, M19
EAIGP-8.6	Operate field monitoring and incident reporting for AI-enabled products, meeting R185 in-service reporting, CRA, PLD and post-market monitoring expectations.	M18

9. CPD and progression

Completing the course earns 32 CPD hours, recorded on the certificate of completion. The course meets the training requirement for the EAIGP examination. For existing GAICC holders, the hours can count towards renewal of other GAICC certifications under the Technology, Humanity and Strategy split, as recorded in the GAICC renewal register.

Document control

Document	32-Hour Course Curriculum: Engineering AI Governance Professional (EAIGP)
Document code	GAICC-CUR-EAIGP-001
Version	1.0
Issued	23 October 2026
Status	Issued for courseware development

Owner	Global AI Certification Council Limited (GAICC), Certification Scheme Committee
Review cycle	At least annually, and whenever a material regulatory or standards change occurs in the sector