Global AI Certification Council

GAICC CERTIFICATION · SCHEME DOCUMENT

[EAIGP]

Engineering AI Governance Professional

Certification Scheme Document

1st Edition | 2026 | v1.2



Certification	GAICC Engineering AI Governance Professional (GAICC-EAIGP)
Document code	GAICC-SCH-EAIGP-001
Version	1.2 · 30 October 2026
Status	Approved
Designed to align with	ISO/IEC 17024:2026

Document control

Document	Certification Scheme Document: Engineering AI Governance Professional (EAIGP)
Document code	GAICC-SCH-EAIGP-001
Version	1.2
Issued	30 October 2026
Status	Approved
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

Version history

Version	Date	Change
1.0	23 October 2026	First issue of the scheme for SME Panel review.
1.1	30 October 2026	Appeals contact added: appeal within 30 days by writing to support@gaicc.org.
1.2	30 October 2026	All 80 examination items are scored. Item counts restated for 80 items. Reviewed by the SME Panel and approved by the GAICC Board.

Approval

Role	Name	Date
Prepared by	GAICC Certification Scheme Team	23 October 2026
Reviewed by	GAICC Subject Matter Expert Panel	30 October 2026
Approved by	GAICC Board	30 October 2026

1. Purpose and scope

This document defines the certification scheme for the GAICC Engineering AI Governance Professional (GAICC-EAIGP). It sets out the scope of certification, the competence requirements, the prerequisites, the assessment method, and the rules for awarding, maintaining, suspending and withdrawing the credential.

The scheme is designed to align with ISO/IEC 17024:2026, Conformity assessment: General requirements for bodies operating certification of persons. It is owned and operated by GAICC, which is independent of any training provider and of any employer of candidates.

1.1 Scope of certification

The EAIGP certifies that a person has the knowledge and the applied judgement to govern artificial intelligence across its lifecycle in engineering, manufacturing, mobility, infrastructure and industrial technology: to interpret sector regulation and standards, assess and treat AI risk, design and operate controls, provide assurance evidence and advise decision-makers. It covers predictive, generative and agentic AI, whether built in-house, procured or delivered by third parties.

1.2 Purpose of the certification

AI now sits inside machines, vehicles, robots, process plants, networks and the tools engineers use to design and verify them. Generative design proposes structures, surrogate models replace simulations, perception models decide when a robot slows down, and AI coding agents write the regression tests that sign off silicon against a digital twin. Failures in these systems can cause physical, often irreversible, harm. Established engineering assurance was built for deterministic, specified behaviour, and it struggles with data-driven insufficiencies, distribution shift, self-evolving behaviour, rapid model updates over decades-long asset lives, and AI-generated artefacts that reviewers are inclined to trust. Professional bodies are clear that AI cannot sign off work: the engineer remains accountable, and some professional indemnity insurers are adding AI exclusions.

An Engineering AI Governance Professional connects AI governance to the disciplines engineering organisations already run: functional safety, safety of the intended functionality, systems engineering, configuration management, verification and validation, OT cybersecurity and quality management. Holders classify AI-enabled products under product, AI, cybersecurity and liability law; integrate machine learning into IEC 61508, ISO 26262, ISO 21448 and ISO/PAS 8800 lifecycles; build safety cases with explicit confidence arguments; keep datasets, models and AI bills of materials under configuration control through over-the-air updates; plan V&V using simulation and digital twins; secure AI in operational technology; and set autonomy limits and approval gates for AI coding agents and agentic workflows. The credential serves OEMs, Tier 1 suppliers, manufacturers, utilities, infrastructure and construction firms, semiconductor and telecom companies, and the digital engineering and IT services firms that build and validate AI for them.

The regulatory picture changed materially in 2026. The Digital Omnibus on AI, Regulation (EU) 2026/1744, moved machinery to Annex I Section B of the AI Act and set Annex I application to 2 August 2028, while the Machinery Regulation (EU) 2023/1230 applies from 20 January 2027 with third-party assessment for self-evolving safety functions. Cyber Resilience Act reporting has applied since 11 September 2026, the revised Product Liability Directive must be transposed by 9 December 2026, EN 18286 became the first harmonised AI Act standard in October 2026, and WP.29 adopted UN Regulation No 185 and GTR No 26 for automated driving in June 2026. Engineering organisations need people who can turn these into working engineering practice now.

2. Normative references and terms

- ISO/IEC 17024:2026, Conformity assessment: General requirements for bodies operating certification of persons
- ISO/IEC 17000, Conformity assessment: Vocabulary and general principles
- ISO/IEC TS 17027, Conformity assessment: Vocabulary related to competence of persons used for certification of persons
- ISO/IEC 42001:2023, Information technology: Artificial intelligence: Management system
- GAICC Recertification Procedure, GAICC-QMS-PRO-REC-001, and the GAICC renewal register, GAICC-QMS-FR-RECERT-001
- EAIGP Examination Content Outline, GAICC-ECO-EAIGP-001, and Candidate Handbook, GAICC-CH-EAIGP-001

Terms used in this document follow ISO/IEC 17000, ISO/IEC TS 17027 and ISO/IEC 22989. "Certified professional" means a person holding a current certificate under this scheme.

3. Scheme ownership and governance

Body	Role in this scheme
GAICC Board	Approves the scheme and material changes to it. Holds overall accountability for impartiality.
Certification Scheme Committee	Develops and maintains the scheme, monitors performance data and recommends changes to the Board. Includes representatives of employers, practitioners and regulators or their advisers, with no single interest predominating.
Subject Matter Expert Panel (engineering)	Validates the Examination Content Outline, writes and reviews items, and sets the passing standard. Members hold relevant engineering, manufacturing, mobility, infrastructure and industrial technology and AI governance expertise and sign confidentiality and conflict-of-interest declarations.
Impartiality Committee	Identifies and treats threats to impartiality, including any threat arising from training, commercial or client relationships.
Certification Decision Maker	Makes certification decisions. Has not been involved in training or examining the candidate concerned.

3.1 Separation of training and certification

Training is not a condition of the certification decision beyond evidence that the training requirement has been met. Training providers, including GAICC Authorised Training Partners and the GAICC self-paced course, have no access to live examination items, item statistics or candidate results other than aggregate pass rates. Personnel who train a candidate do not examine or certify that candidate.

4. Job and task description

The EAIGP job and task description consists of the eight domains and the task statements in the Examination Content Outline. Domain titles and weightings are summarised below. The full task and knowledge statements are in Annex A.

Domain	Title	Weight	Tasks
I	Engineering AI Landscape and Professional Accountability	10%	5
II	Product Regulation and Liability for AI-Enabled Systems	14%	6
III	AI Safety Engineering and Functional Safety Integration	16%	6
IV	Data, Model Lifecycle and Configuration Management	12%	5
V	Verification, Validation and Robustness Assurance	14%	6
VI	Cybersecurity and Resilience of AI-Enabled Systems	11%	5
VII	Human Oversight, Ethics and Societal Impact	10%	5
VIII	Generative, Agentic and Physical AI in Practice	13%	6

5. Competence requirements

5.1 Knowledge

The knowledge statements in Annex A, including the reference frameworks listed in Annex B.

5.2 Skills

- Interpreting engineering regulation and standards and translating them into proportionate AI controls.
- Assessing AI risk and impact, including technical, legal, ethical, operational and third-party risk.
- Designing governance arrangements, lifecycle gates, human oversight and monitoring.
- Gathering, evaluating and presenting assurance evidence to regulators, auditors, clients and boards.
- Responding to AI incidents and communicating clearly with technical and non-technical stakeholders.

5.3 Personal attributes

Integrity, professional scepticism, sound judgement under uncertainty, and the willingness to escalate concerns. These are reinforced through the GAICC Code of Ethics, which every candidate accepts before the examination and reaffirms at renewal.

6. Prerequisites

Requirement	Status	Detail
Training	Required	32 contact hours of EAIGP training, completed before the exam, by any of the three routes below. Hours are counted per certification and do not transfer between certifications.
Experience	Recommended, not required	At least five years in engineering, safety, verification, quality, cybersecurity or product compliance roles, including work on safety-related or regulated products, is recommended but not required. Experience is never used to refuse a candidate.

Requirement	Status	Detail
Prior credential	Recommended, not required	GAICC Certified Professional in AI Governance (CPAIG) or equivalent foundational AI governance knowledge.

6.1 Training routes

Training route	What it involves
GAICC self-paced course	Structured eLearning on the GAICC platform with a certificate of completion.
GAICC Authorised Training Partner or Certified Instructor	Instructor-led, in person or live online, delivered to the 32-hour GAICC curriculum.
GAICC-recognised institution	A university, professional body or employer programme that GAICC has recognised as covering the Examination Content Outline.

Evidence of training (a certificate of completion stating the course, provider, dates and contact hours) is verified before an examination booking is confirmed. GAICC may sample-check training records with the provider.

7. Assessment

7.1 Examination specification

Examination **80 questions, all scored**	**Duration** **120 minutes**	**Pass mark** **70%, 56 of 80 items (scaled score of 350 on a 100 to 500 scale)**
Format **Scenario-based multiple choice, single best answer from four options, no negative marking**	**Delivery** **Online with AI-assisted proctoring through the GAICC Hub, available 24/7. A person makes any final integrity decision**	**Conditions** **Closed book. No reference material, notes or AI tools**
Training requirement **32 contact hours, completed before the exam**	**Validity and renewal** **3 years · 60 CPD hours per cycle**	**Credential awarded** **GAICC Engineering AI Governance Professional (GAICC-EAIGP)**

Cognitive level	Share of scored items	What it looks like
Understanding	25% (about 20 items)	Explain concepts, obligations and the purpose of controls in the sector context.
Application	45% (about 36 items)	Apply frameworks, regulations and controls to realistic sector scenarios.
Analysis and Evaluation	30% (about 24 items)	Weigh competing risks and obligations, judge evidence, and choose the most defensible course of action.

7.2 Item development

- Items are written by trained SME Panel members to a single task code and cognitive level, and reviewed independently for accuracy, relevance, clarity, bias and currency.
- Each item has a documented reference and rationale. Items referring to laws or standards are reviewed whenever the source changes.
- Every item on every examination form is scored. New items enter a live form only after SME Panel review and approval.
- Item statistics are reviewed after each window. Items that perform poorly, show differential item functioning or become outdated are retired.

7.3 Standard setting and scoring

The passing standard is set by the SME Panel using a modified Angoff method, describing the minimally competent sector professional. Raw scores are converted to a scale of 100 to 500 with 350 as the passing score, so that results are comparable across equated forms. The initial passing standard corresponds to 70% of the 80 items (56 correct answers).

7.4 Examination security and conduct

Examinations are delivered online through the GAICC Hub with AI-assisted proctoring and recorded sessions. A person reviews every flag and makes any final integrity decision. Item banks are access-controlled and forms are rotated. Any breach is handled under the misconduct rules in the Candidate Handbook.

7.5 Reasonable adjustments

Candidates with a disability, a medical condition or other documented need may request reasonable adjustments, such as extra time or assistive technology, without changing what the examination measures.

8. Certification decision, validity and recertification

8.1 Certification decision

The Certification Decision Maker confirms that the candidate has met the training requirement, accepted the Code of Ethics and achieved the passing standard, and then issues the certificate and digital badge. The decision is made only on the information gathered through the certification process.

8.2 Certificate content

The certificate shows the holder's name, the credential title, a unique certificate number, the date of certification and the expiry date. Certificates can be verified on the GAICC public register.

8.3 Validity and recertification

- The credential is valid for 3 years from the certification decision.
- Earn 60 CPD hours in each three-year cycle, split Technology 27, Humanity 12 and Strategy 21.
- Hours can be earned through engineering AI governance work such as risk and impact assessment, assurance and audit, incident handling, policy and control design, teaching, writing, standards work and structured learning.
- Reaffirm the GAICC Code of Ethics, remain in good standing and pay the renewal fee.
- A three months grace period applies after expiry. After the grace period, re-examination is required.
- Re-examination is also required where CPD evidence is insufficient, the credential has lapsed, or a major scheme change requires it.

Competency (GAICC AI Competence Triangle)	What it covers	CPD hours
Technology	AI systems, data, models, tooling and technical controls.	27
Humanity	Ethics, human oversight, fairness, transparency and impact on people.	12
Strategy	Governance, policy, risk, assurance and organisational alignment.	21
Total per three-year cycle	No elective category. Every hour maps to one competency.	**60**

CPD records are subject to random audit. Holders keep evidence for the full cycle. Recertification follows GAICC-QMS-PRO-REC-001, with CPD categories recorded in register GAICC-QMS-FR-RECERT-001.

9. Suspension, withdrawal and reduction of scope

- Suspension may follow a breach of the Code of Ethics, misuse of the certificate or marks, failure to respond to a CPD audit, or non-payment of the renewal fee.
- Withdrawal follows a proven serious breach, examination misconduct, fraudulent application, or failure to resolve a suspension within the stated period.
- Suspended or withdrawn holders must stop using the certificate, badge and marks. The public register is updated promptly.

10. Use of certificates, logos and marks

Holders may use the post-nominal "EAIGP" and the GAICC digital badge while their certificate is current. They must not imply that the certification applies to an organisation, product or service, or that it covers work outside its scope.

11. Appeals and complaints

Candidates may appeal an examination result or certification decision within 30 days by writing to support@gaicc.org. Appeals are handled by people not involved in the original decision. Complaints about GAICC, a training provider or a certified professional are acknowledged, investigated and closed with a written outcome.

12. Records and confidentiality

Application, examination and certification records are kept securely for at least the period of certification plus one full cycle. Candidate information is confidential and is disclosed only with consent or where required by law.

13. Scheme review and maintenance

The scheme is reviewed at least annually. Because AI regulation in engineering, manufacturing, mobility, infrastructure and industrial technology is changing quickly, a review is also triggered when a reference framework in Annex B is adopted, amended, delayed or withdrawn, or when a new class of AI technology (for example, a new form of autonomous agent) changes practice materially. A full role analysis is repeated at least every five years.

Horizon topics monitored for future revisions

- 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

Annex A. Domains, tasks and knowledge

Domain I. Engineering AI Landscape and Professional Accountability (10%, about 8 scored items)

Understand where AI is used across the engineering lifecycle and how professional duty, sign-off, governance roles and insurance shape accountability for AI-assisted work.

Code	Task: the certified professional can	Knowledge of
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.	• Generative design, topology optimisation and simulation surrogate models • Predictive maintenance, inspection and condition monitoring failure modes • Perception, autonomy, robotics and closed-loop process control applications • AI-generated code, tests and documentation in engineering deliverables
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.	• Engineering NZ AI in professional practice guidance and Quick Kit • Engineering Council and RAEng Statement of Ethical Principles, February 2026 • Engineers Europe advice note and NSPE position statement on AI • Statutory duties under building and health and safety legislation
EAIGP-1.3	Define engineering AI governance roles, decision rights and escalation paths linking design authority, functional safety, cybersecurity, quality and responsible AI functions.	• Design authority, safety manager and independent assessor roles • Decision rights for model release, change approval and incident response • Competence management for engineers who use and assure AI
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.	• Inventory attributes: purpose, owner, version, supplier, integrity level • Unrecorded AI in engineering tools, scripts and design assistants • Linking inventory entries to hazard logs and AI bills of materials
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.	• Professional indemnity AI exclusions and disclosure duties to insurers • Warranties, indemnities and limitation clauses for AI deliverables • Evidence retention to support the defence of liability claims

Domain II. Product Regulation and Liability for AI-Enabled Systems (14%, about 12 scored items)

Classify AI-enabled products and systems under AI, product safety, cybersecurity and liability law across key markets, and plan conformity assessment against current application dates.

Code	Task: the certified professional can	Knowledge of
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.	• Regulation (EU) 2026/1744 and revised application dates • Narrowed safety component definition and assistance or optimisation exclusions • Section A products versus Section B products such as machinery and vehicles • Registration of non-high-risk assessments; draft Article 6 guidelines status
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.	• Annex I Part A points 5 and 6 on self-evolving behaviour • Annex III sections 1.1.9 protection against corruption and 1.2.1 control systems • Application from 20 January 2027 and expected harmonised standards • Delegated acts adding AI requirements for machinery by 2 August 2028
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.	• CRA essential requirements, support periods, product classes and EU Data Act duties • CRA compliance as a contribution to AI Act Article 15 cybersecurity • PLD treatment of software, AI and updates as products • PLD presumptions of defect and causation and court-ordered disclosure
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.	• UN R185 and GTR No 26 safety management and in-service reporting • EASA Concept Paper AI levels and NPA 2025-07 trustworthiness objectives • FAA distinction between learned and learning AI • Interaction of type-approval with AI Act Annex I Section B
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.	• Presumption of conformity from standards cited in the Official Journal • EN 18286 status and AI Act standards still in preparation • GB machinery update plans and UKCA marking • South Korea high-impact AI in energy and transport
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.	• US advanced chip controls, Jan 2026 licensing changes, rescinded model-weight rule • Dual-use classification of engineering technology and technical data • Deemed exports through offshore delivery centres and cloud access

Domain III. AI Safety Engineering and Functional Safety Integration (16%, about 13 scored items)

Integrate machine learning into established functional safety and SOTIF practice, and argue that residual risk is acceptable within a defined operational design domain.

Code	Task: the certified professional can	Knowledge of
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.	• STPA unsafe control actions and loss scenarios involving learned components • HAZOP guidewords adapted to perception and prediction outputs • ML failure modes: distribution shift, long tail, spurious correlation
EAIGP-3.2	Specify the operational design domain and its monitoring, covering environmental, behavioural and data conditions, and define system behaviour on ODD exit.	• ODD taxonomies and attributes for vehicles, robots and plants • Mapping ODD attributes to data coverage and test scenarios • ODD exit detection, minimal risk conditions and fallback
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.	• IEC 61508 lifecycle, IEC 61511 process sector and systematic capability • ISO/IEC TR 5469 AI technology classes and usage levels • ISO/IEC TS 22440 drafting status and expected scope • Expected ISO 26262 edition 3 direction on machine learning
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.	• SOTIF known and unknown hazardous scenario areas • ISO/PAS 8800 AI safety requirements, data and assurance arguments • Triggering conditions and acceptance criteria for residual risk
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.	• Goal Structuring Notation and assurance case patterns for ML • UL 4600 claims, evidence and safety performance indicators • ISO/TS 5083 safety by design and verification for ADS • Defeaters, confidence and assurance deficit management
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.	• Decomposition and architectural patterns that limit reliance on ML • ED-324/ARP6983 ML constituent scope up to DAL C • Why ML alone rarely carries the highest integrity claims

Domain IV. Data, Model Lifecycle and Configuration Management (12%, about 9 scored items)

Govern datasets, models and their configuration across the engineering lifecycle so that every fielded AI version is traceable, reproducible and changed under control.

Code	Task: the certified professional can	Knowledge of
EAIGP-4.1	Implement ISO/IEC 5338 AI lifecycle processes and MLOps controls aligned with engineering configuration management, systems engineering and quality systems.	• ISO/IEC 5338 processes and their relation to ISO/IEC/IEEE 15288 • MLOps pipelines, drift monitoring and continuous training gates • Reproducibility: seeds, environments, toolchains and training records
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.	• Dataset specifications linked to ODD and safety requirements • Labelling quality, bias, coverage and independence of test sets • Provenance and limits of synthetic and simulation-generated data • EN 18284 dataset standard, still in preparation
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.	• SPDX 3.0 AI and Dataset profiles • CycloneDX ML-BOM (ECMA-424) components and relationships • G7 minimum elements for AI SBOM, May 2026
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.	• UN R156 software update management and RXSWIN • Change impact analysis triggers for retraining and threshold changes • Rollback, staged rollout and fleet configuration status accounting
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.	• Learned versus learning systems and predetermined change limits • Obsolescence of models, frameworks and accelerators over long asset lives • Supplier flow-down clauses for data, model and update evidence • Substantial modification triggers for continuously learning systems

Domain V. Verification, Validation and Robustness Assurance (14%, about 11 scored items)

Plan and execute verification and validation that produce defensible evidence of AI performance, robustness and safe behaviour, in simulation, on test rigs and in the field.

Code	Task: the certified professional can	Knowledge of
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.	• V&V planning, independence levels and acceptance criteria • Requirements-based versus data-based test evidence • Statistical confidence and test set sufficiency
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.	• Scenario databases, criticality metrics and search-based testing • SIL, HIL and vehicle or plant-in-the-loop configurations • Sim-to-real gap measurement and simulator qualification
EAIGP-5.3	Assess model robustness, quality and uncertainty using ISO/IEC 24029, ISO/IEC 25059 and uncertainty quantification methods.	• ISO/IEC 24029-2 formal methods for neural network robustness • ISO/IEC 25059 quality characteristics for AI systems • Calibration, out-of-distribution detection and uncertainty estimates
EAIGP-5.4	Specify run-time monitors and safety envelopes that detect anomalous AI behaviour and enforce safe states independently of the learned component.	• Safety envelopes, safety cages and simplex architectures • Monitor integrity, independence and diagnostic coverage • Monitor indicators that feed field monitoring
EAIGP-5.5	Validate AI-generated code, tests and designs against coding standards, requirements traceability and test oracles, and qualify the AI tools used.	• MISRA, CERT and project coding standards for generated code • Tool confidence and qualification under ISO 26262-8 and DO-330 • Oracle problem: tests that confirm implementation rather than specification • Coverage metrics and their limits as completeness arguments
EAIGP-5.6	Assess digital twin fidelity, validity range and digital thread integrity before twin results are used as verification or certification evidence.	• ISO 23247 framework and Part 5 digital thread • Twin calibration, validity envelope and divergence detection • Credibility assessment of models and simulations used for decisions

Domain VI. Cybersecurity and Resilience of AI-Enabled Systems (11%, about 9 scored items)

Protect AI-enabled systems and operational technology from cyber and adversarial attack, and meet vulnerability handling and reporting duties across the supply chain.

Code	Task: the certified professional can	Knowledge of
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.	• IEC 62443-3-3 security levels and zone and conduit models • Principles for the Secure Integration of AI in OT, December 2025 • Separating AI inference, training and cloud links from control networks
EAIGP-6.2	Threat model AI-enabled systems for adversarial ML, including evasion, physical adversarial patches, model extraction and prompt injection, using MITRE ATLAS.	• MITRE ATLAS tactics and techniques • Physical-world adversarial attacks on perception • Prompt injection risks for LLM assistants connected to engineering tools
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.	• Data and model poisoning, backdoors and integrity controls • Code signing, secure boot and model integrity verification • Machinery Regulation 1.1.9 protection against corruption
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.	• CRA reporting via the single reporting platform from 11 September 2026 • Coordinated vulnerability disclosure and support period obligations • Interaction of CRA, NIS2 and sector incident reporting
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.	• Supplier security assurance for pretrained models and datasets • ISO 10218-1 and -2:2025 cybersecurity provisions • Model repository, dependency and container image risks

Domain VII. Human Oversight, Ethics and Societal Impact (10%, about 8 scored items)

Design human oversight and ethical safeguards that work in process time, protect workers and communities, and account for the environmental impact of engineering AI.

Code	Task: the certified professional can	Knowledge of
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.	• ISO/IEC TS 8200 controllability characteristics • Process safety time and human response limits • Takeover, override and minimal risk manoeuvre design

Code	Task: the certified professional can	Knowledge of
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.	• Automation bias and complacency in reviewers and operators • Explanation and confidence displays for operators • Just culture, reporting and challenge of AI recommendations
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.	• IEEE 7000-2021 ethical value requirements process • IEEE 7009-2024 fail-safe mechanisms for autonomous systems • Graceful degradation and safe state definition
EAIGP-7.4	Evaluate worker safety and workforce impact of AI and automation, including consultation, competence and psychosocial risk, under health and safety duties.	• Duties to consult workers under HSWA 2015 and equivalents • Collaborative robots and shared workspaces • Reskilling, job design and psychosocial risk
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.	• Energy and water use of training and inference • ISO/IEC 42005 impact assessment for affected stakeholders • Te Tiriti o Waitangi principles and engagement with iwi and hapū • Data sovereignty for infrastructure and environmental data

Domain VIII. Generative, Agentic and Physical AI in Practice (13%, about 10 scored items)

Govern generative, agentic and physical AI as they enter engineering workflows and products, and run integrated management systems, supplier obligations and field monitoring that keep evidence current.

Code	Task: the certified professional can	Knowledge of
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.	• Human verification proportional to artefact integrity level • Traceability from requirement to AI-generated artefact and reviewer • Copyright, open source licences and standards licence terms in prompts
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.	• Careful Adoption of Agentic AI Services guidance, May 2026 • OWASP Agentic Top 10 risks • Approval gates, kill switches and rollback for irreversible actions • Agent registry, identity and audit logging

Code	Task: the certified professional can	Knowledge of
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.	• Vision-language-action models and AI Act general-purpose AI duties • ISO 25785-1 drafting status for legged and humanoid robots • Speed and separation monitoring and power and force limiting
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.	• ISO/IEC 42001 and EN 18286 scope and differences • Harmonised Structure mapping across management system standards • Integrating functional safety management and CSMS audits
EAIGP-8.5	Determine services-provider obligations under the AI Act, including provider versus supplier roles, substantial modification and validation evidence packs for clients.	• Article 25 value chain responsibilities and written agreements • Substantial modification and becoming a provider • Evidence packs: model cards, test reports, logs and AIBOMs • Accountability in statements of work and service levels
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.	• UN R185 and NHTSA crash reporting order in-service monitoring • Post-market monitoring plans and safety performance indicators • AI Act serious incident reporting for high-risk systems • Evidence preservation for PLD disclosure requests

Annex B. Reference frameworks

Framework, law or standard	Jurisdiction	Status (October 2026)	What a holder must be able to do
EU AI Act (Regulation (EU) 2024/1689) as amended by Regulation (EU) 2026/1744	EU	In force; Annex III high-risk applies 2 Dec 2027, Annex I 2 Aug 2028	Classify AI under Article 6, choose Annex I Section A, Section B or Annex III routes, and plan conformity evidence.
Machinery Regulation (EU) 2023/1230	EU	Applies 20 Jan 2027 with no transition; harmonised standards list expected end 2026	Identify self-evolving safety functions needing third-party assessment and meet requirements on corruption and control systems.
Cyber Resilience Act (Regulation (EU) 2024/2847)	EU	Reporting obligations apply from 11 Sep 2026; full application 11 Dec 2027	Run vulnerability handling, 24-hour and 72-hour reporting and support periods for AI-enabled products with digital elements.
Product Liability Directive (EU) 2024/2853	EU	Member State transposition due 9 Dec 2026	Assess strict liability for AI software and updates, and keep evidence ready for presumptions and court-ordered disclosure.
EN 18286:2026 Quality management system for EU AI Act regulatory purposes	EU	Cited in OJ by Implementing Decision (EU) 2026/2274, 14 Oct 2026	Build an AI quality management system that integrates with ISO 9001, IATF 16949 or AS9100 and ISO/IEC 42001.
GB machinery and product safety regulation (UKCA)	UK	Government response 25 Feb 2026; 2008 machinery regulations to be updated	Plan dual UKCA and CE routes and track GB alignment with EU rules on AI in machinery.
UN Regulations No 155 (CSMS) and No 156 (SUMS)	UNECE / EU	Mandatory for all new EU vehicle registrations since July 2024	Link AI model updates to the software update management system, RXSWIN records and vehicle cybersecurity management.
UN Regulation No 185 and UN GTR No 26 (Automated Driving Systems)	UNECE	Adopted by WP.29 on 24 Jun 2026	Prepare ADS safety management, safety case against a competent and careful human driver, data storage and in-service reporting.
EASA AI Concept Paper, NPA 2025-07 (RMT.0742) and FAA Roadmap for AI Safety Assurance	EU / US	Concept Paper Issue 03 consulted Jun 2026; NPA published Nov 2025	Classify aviation AI by level, apply trustworthiness objectives and distinguish learned from learning AI.
EUROCAE ED-324 / SAE ARP6983 (ML Constituent)	International	Publication targeted Q4 2026	Plan assurance of offline-trained, non-adaptive supervised ML constituents in airborne systems up to DAL C.
IEC 61508 with ISO/IEC TR 5469:2024 and ISO/IEC TS 22440	International	IEC 61508 Ed 2 current; TS 22440 in drafting, not published	Integrate AI technology classes and usage levels into the functional safety lifecycle and systematic capability arguments.
ISO 26262:2018 and ISO 21448:2022 (SOTIF)	International	Published; ISO 26262 edition 3 expected 2027 with ML guidance	Combine hazard and risk analysis, ASIL allocation and SOTIF triggering condition analysis for AI functions.

Framework, law or standard	Jurisdiction	Status (October 2026)	What a holder must be able to do
ISO/PAS 8800:2024 Road vehicles: Safety and artificial intelligence	International	Published 2024	Derive AI safety requirements, data requirements and assurance arguments for AI elements in road vehicles.
ISO/TS 5083:2025 and UL 4600 Ed 3	International / US	ISO/TS 5083 published 2025; UL 4600 Ed 3 published 2023	Structure autonomous system safety cases, safety performance indicators and verification for automated driving and autonomy.
IEC 62443 series and Principles for the Secure Integration of AI in OT	International / Five Eyes	IEC 62443 published; joint agency principles issued Dec 2025	Place AI in zones and conduits, set security levels and govern AI connectivity to control networks.
Careful Adoption of Agentic AI Services, OWASP Agentic Top 10 and MITRE ATLAS	International	Joint agency guidance published 1 May 2026	Apply least privilege, approval gates, reversibility, agent registries and adversarial threat modelling to engineering agents.
ISO 10218-1 and -2:2025 and ISO 25785-1	International	ISO 10218:2025 published; ISO 25785-1 in drafting	Assess collaborative, mobile and humanoid robot safety, including the cybersecurity provisions added in 2025.
ISO/IEC 42001:2023, ISO/IEC 23894:2023, ISO/IEC 42005:2025 and NIST AI RMF	International / US	ISO/IEC standards published; NIST AI RMF 1.0 under revision	Run an AI management system, AI risk management and impact assessment across engineering portfolios.
ISO/IEC 5338:2023 AI system life cycle processes	International	Published 2023	Align AI lifecycle and MLOps processes with ISO/IEC/IEEE 15288 systems engineering and configuration management.
ISO/IEC 24029-2:2023 and ISO/IEC 25059:2023	International	Published 2023	Assess neural network robustness with formal methods and specify AI quality characteristics for acceptance criteria.
ISO/IEC TS 8200:2024, IEEE 7000-2021 and IEEE 7009-2024	International	Published	Design controllability, value-based ethical requirements and fail-safe mechanisms for autonomous and semi-autonomous systems.
ISO 23247 Digital twin framework for manufacturing	International	Part 5 digital thread published Jun 2026	Judge digital twin fidelity and digital thread integrity before twin results count as verification evidence.
SPDX 3.0, CycloneDX ML-BOM (ECMA-424) and G7 minimum elements for AI SBOM	International	Specifications published; G7 minimum elements issued May 2026	Produce AI bills of materials recording models, datasets, dependencies and provenance for customers and regulators.
South Korea AI Basic Act	South Korea	In force 22 Jan 2026	Identify high-impact AI in energy, transport and similar sectors and meet obligations for products sold into Korea.

Framework, law or standard	Jurisdiction	Status (October 2026)	What a holder must be able to do
US export controls on advanced AI chips and computing items	US	AI Diffusion Rule rescinded May 2025; chip licensing revised Jan 2026	Screen chips, compute access and technical data in global delivery and cloud arrangements, and track any model weight rules.
Professional guidance: Engineering NZ, Engineering Council and RAEng, Engineers Europe, NSPE	NZ / UK / EU / US	Engineering NZ guidance Jul 2025; Statement of Ethical Principles refreshed 23 Feb 2026	Apply professional duty, record AI use and keep competent engineer sign-off for AI-assisted work.