Global AI Certification Council

GAICC CERTIFICATION · EXAMINATION CONTENT OUTLINE

[FAIGP]

Finance AI Governance Professional

Examination Content Outline

1st Edition | 2026 | v1.2

Certification	GAICC Finance AI Governance Professional (GAICC-FAIGP)
Document code	GAICC-ECO-FAIGP-001
Version	1.2 · 30 October 2026
Level	Tier 3, Senior and Specialty (sector professional)
Examination	80 questions · 120 minutes · 70% pass

1. About this Examination Content Outline

This Examination Content Outline (ECO) defines what the Finance AI Governance Professional (FAIGP) examination measures. It lists the eight domains, their weightings, and the tasks and knowledge a certified professional is expected to demonstrate. Every examination item is written to, and traceable to, one task code in this outline.

Use this outline to plan your preparation. Training providers use it to design courses, but no training provider sees live examination content, and every training route is treated equally.

> **How the content was defined**
>
> The domains and tasks were defined from a role analysis of AI governance work in banking, insurance, capital markets and payments, current regulation and standards, and employer needs across regulated enterprises and the technology and services firms that support them. They have been validated by the GAICC Subject Matter Expert Panel and approved by the GAICC Board.

2. Purpose of the certification

Banks, insurers, asset managers, payment firms and fintechs now use AI in decisions that move money and decide access to credit, cover and advice: credit and underwriting, pricing, claims, fraud and AML detection, trading, servicing and treasury. These uses sit inside some of the most heavily supervised activities in the economy, where model risk, conduct, prudential, data protection and operational resilience rules all apply at once. Generative and agentic AI add failure modes, such as inaccurate AI-written customer communications and agents that can initiate payments, that classic model risk management was not designed to catch.

FAIGP holders translate these overlapping regimes into one proportionate control framework. They tier AI by materiality, challenge and validate machine learning and large language models, test credit and insurance AI for unfair discrimination, govern third-party and foundation model dependencies under DORA and equivalent regimes, engineer controls for AI agents, and produce the evidence that boards, auditors and supervisors expect. The credential is equally relevant to the technology, consulting and services firms that build and run AI for financial institutions as ICT third-party providers, and to supervisory staff who examine it.

The timing matters. In April 2026 the US banking agencies replaced SR 11-7 with risk-based model risk guidance that excludes generative and agentic AI, leaving firms to design those controls themselves while examiners ask how agents are limited, audited and shut down. In October 2026 MAS finalised its Guidelines on AI Risk Management, the HKMA issued its ART framework, the FSB finalised its Sound Practices for Responsible Adoption of AI and the FCA set out good and poor AI practice. EU AI Act high-risk obligations for credit scoring and life and health insurance pricing apply from 2 December 2027. Firms need people who can act on all of this together.

3. Who the certification is for

The FAIGP is designed for professionals who govern, assure, deliver or advise on AI in banking, insurance, capital markets and payments, including:

- Model risk managers and model validators
- Chief risk officers and AI risk leads
- Compliance, conduct and fair lending specialists

- Actuaries, data scientists and quantitative analysts
- Internal auditors and supervisory examination staff
- Third-party, outsourcing and resilience managers
- Financial crime and fraud analytics leads
- Technology, consulting and fintech delivery teams

Roles the certification supports

- Head of AI Risk and Governance
- Model Validation Lead (AI and Machine Learning)
- Responsible AI Lead, Financial Services
- AI Assurance Manager, Internal Audit
- Financial Services AI Governance Consultant

What certified professionals can do

1. Map AI use cases to accountable senior managers, risk appetite and a materiality-tiered inventory.
2. Interpret EU, US, UK and APAC financial AI rules and build one obligations map.
3. Validate machine learning and large language models with credible effective challenge and monitoring.
4. Test credit and insurance AI for proxy discrimination and produce accurate adverse action reasons.
5. Govern financial data, privacy and financial crime AI to examiner-ready standards.
6. Manage AI third-party, foundation model and concentration risk under DORA and equivalent regimes.
7. Engineer controls for AI agents, including identity, limits, dual approval and kill switches.
8. Assure AI through audits, incident reporting and board risk reporting against appetite.

4. The examination at a glance

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 Finance AI Governance Professional (GAICC-FAIGP)

Cognitive levels

Most items present a realistic sector scenario and ask for the most appropriate action, judgement or control. Recall of clause numbers is not tested.

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.

5. Domain weighting

The 80 scored items are distributed across eight domains as follows. Item counts are approximate and may vary by one or two items between examination forms.

Dom.	Title	Relative weight	Weight	Items
I	Financial Services AI Landscape and Accountability		**10%**	8
II	Financial AI Regulation and Supervisory Expectations		**15%**	13
III	Model Risk Management for AI		**15%**	13
IV	Fairness, Explainability and Consumer Outcomes		**13%**	10
V	Data Governance, Privacy and Financial Crime AI		**11%**	9
VI	Third-Party, Concentration and Operational Resilience		**12%**	9
VII	Generative, Agentic and Emerging AI in Finance		**12%**	9
VIII	Assurance, Audit, Incidents and Board Reporting		**12%**	9
	Total scored items		**100%**	**80**

6. Domains, tasks and knowledge

Each task is a statement of what a certified professional can do. The knowledge statements describe what a candidate must know to perform the task. Task codes are used to trace every examination item and every training module.

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

How AI is used across banking, insurance, capital markets and payments, and how boards, senior managers and the three lines own its risks. Covers AI strategy, risk appetite, individual accountability and a materiality-based AI inventory.

Code	Task: the certified professional can	Knowledge of
FAIGP-1.1	Map AI use cases across credit, underwriting, pricing, claims, fraud, AML, trading, advice, servicing and treasury, and classify each by decision impact and regulatory exposure.	• Typical AI use cases and failure modes in each financial value chain • Differences between decision-making, decision-support and back-office AI • Predictive, generative, agentic and embedded vendor AI in financial products • Which uses trigger high-risk, conduct, prudential or market integrity rules
FAIGP-1.2	Advise the board on an AI strategy and risk appetite statement with measurable limits, escalation triggers and links to the enterprise risk management framework.	• Board AI responsibilities under FSB, MAS, HKMA and APRA expectations • Qualitative and quantitative AI risk appetite metrics and tolerances • Board AI literacy expectations and how to evidence them • Linking AI risk to model, operational, conduct and strategic risk taxonomies
FAIGP-1.3	Allocate senior manager accountability for AI under SM&CR, FAR, MAS individual accountability guidelines and equivalent regimes, including statements of responsibilities and reasonable steps.	• SM&CR prescribed responsibilities, statements of responsibilities and duty of responsibility • Australian Financial Accountability Regime obligations that replaced BEAR • MAS individual accountability guidelines and Hong Kong manager-in-charge expectations • Evidence of reasonable steps when AI-driven decisions cause customer harm
FAIGP-1.4	Design a three lines operating model for AI, defining committee mandates and the roles of business, risk, compliance, model validation, data and internal audit.	• First line ownership of AI use, controls and customer outcomes • Second line roles across model, compliance, operational and conduct risk • Third line independence and internal audit coverage of AI • Common weaknesses: governance after deployment, weak challenge, unclear ownership

Code	Task: the certified professional can	Knowledge of
FAIGP-1.5	Establish and maintain an enterprise AI inventory covering in-house, vendor, embedded, generative and agentic AI, with materiality ratings that drive control intensity.	• Minimum inventory attributes expected by MAS, HKMA, APRA and the FSB • Materiality factors: customer and financial impact, autonomy, complexity, reliance • Discovery methods for shadow AI and AI embedded in vendor software • How the AI inventory relates to the model inventory and DORA register

Domain II. Financial AI Regulation and Supervisory Expectations (15%, about 13 scored items)

The regulation and supervisory expectations that apply to AI in financial services across the EU, US, UK, Asia-Pacific and global standard setters, and how to reconcile them into one control set. Covers current status, deadlines, withdrawals and areas of conflict.

Code	Task: the certified professional can	Knowledge of
FAIGP-2.1	Determine whether financial AI systems are high-risk under the EU AI Act, and whether the firm acts as provider, deployer or both, including through substantial modification.	• Annex III point 5: natural-person creditworthiness and life and health insurance pricing • The fraud detection carve-out and treatment of AI used for legal persons • Omnibus timetable: Annex III duties from 2 December 2027, Annex I 2028 • Article 25 value chain roles and becoming a provider through modification • Financial supervisors acting as market surveillance authorities under Article 74
FAIGP-2.2	Integrate AI Act deployer duties and fundamental rights impact assessments into existing banking and insurance governance, using EBA, EIOPA and ESMA supervisory positions.	• Article 26 deployer duties: instructions for use, oversight, logging, monitoring • Article 27 FRIA content and its link to data protection impact assessments • Provisions treating financial governance rules as meeting certain AI Act duties • EBA mapping factsheet, EIOPA AI Opinion and ESMA retail investment statement • Article 5 prohibitions relevant to finance, including exploiting vulnerabilities and social scoring
FAIGP-2.3	Interpret US federal and state expectations for financial AI, including SR 26-2, Regulation B, SEC and FINRA priorities, the NAIC bulletin, Colorado and NYDFS requirements.	• SR 26-2 scope, risk-based tiering and its exclusion of generative and agentic AI • Regulation B changes effective July 2026 and the requirements that remain • NAIC bulletin adoption, Colorado SB 26-189 and NYDFS Circular Letter No. 7 • Federal and state conflict after the December 2025 executive order on AI

Code	Task: the certified professional can	Knowledge of
FAIGP-2.4	Apply UK expectations for AI from the PRA and FCA, including SS1/23, Consumer Duty, SM&CR, AI Live Testing and the October 2026 good and poor practice findings.	• PRA SS1/23 principles and the April 2026 letter on AI • FCA outcomes-based approach: no AI rulebook, existing rules apply • AI Live Testing cohorts, including agentic payments and AML use cases • FCA October 2026 findings on good and poor AI governance practice
FAIGP-2.5	Apply Asia-Pacific expectations, including MAS AI Risk Management Guidelines, HKMA ART, APRA prudential standards, BNM RMiT, RBI guidance and New Zealand FMA and RBNZ expectations.	• MAS Guidelines phasing: sections 3-4 from October 2027, 5-6 from 2028 • HKMA ART framework, supervisory guidance and proposed registry of material agents • APRA April 2026 AI letter read with CPS 230 and CPS 234 • Status and direction of BNM, RBI FREE-AI and draft RBI MRM guidance • FMA thematic review of AI in advice and October 2026 RBNZ-FMA expectations
FAIGP-2.6	Build and maintain a multi-jurisdiction obligations map that reconciles FSB, IOSCO and Basel positions with national rules into one common control set with tracked regulatory change.	• FSB Sound Practices: the 12 practices and their supervisory use • IOSCO AI toolkit and the Basel Committee ICT risk practices report • Mapping overlapping obligations to common controls and evidence • Handling proposed, delayed, withdrawn and litigated requirements in a control library • IAIS Application Paper on the supervision of AI and insurance expectations

Domain III. Model Risk Management for AI (15%, about 13 scored items)

How model risk management must change for machine learning, generative and agentic AI, from scope and tiering to validation, monitoring and change control. Covers vendor models and the use of AI in capital, provisioning and actuarial models.

Code	Task: the certified professional can	Knowledge of
FAIGP-3.1	Define model and AI scope and tier each system on inherent risk and materiality, including generative and agentic AI that fall outside SR 26-2.	• Model definitions in SR 26-2, PRA SS1/23 and draft RBI guidance • Inherent risk and materiality factors used to tier AI • Governing non-model AI and GenAI under a firm-wide AI risk standard • Calibrating validation depth and frequency to risk tier

Code	Task: the certified professional can	Knowledge of
FAIGP-3.2	Assess the conceptual soundness of machine learning models, including data representativeness, feature design, algorithm choice, hyperparameter tuning, overfitting and stability.	• Bias-variance trade-offs, overfitting and target leakage in financial data • Representativeness across economic cycles and customer segments • Monotonicity and business intuition constraints for credit and pricing • Documentation standards that allow independent replication
FAIGP-3.3	Plan and perform independent validation and effective challenge using benchmarks, challenger models, sensitivity analysis, stress testing and replication of developer results.	• Independence, competence and influence as tests of effective challenge • Benchmarking and challenger model techniques for machine learning • Sensitivity, stress and scenario testing of AI under adverse conditions • Finding severity ratings, compensating controls and conditional approvals
FAIGP-3.4	Validate generative AI and large language model applications where classic tests fail, using task-specific evaluations, groundedness checks, red teaming and structured human review.	• Why holdout accuracy and stability tests do not suffice for LLMs • Evaluation set design, groundedness, hallucination and retrieval quality metrics • Limits of LLM-as-judge scoring and vendor benchmark results • Red teaming for prompt injection, jailbreaks and harmful financial advice
FAIGP-3.5	Establish ongoing monitoring, outcomes analysis and model change management, including drift thresholds, recalibration triggers, material change definitions and vendor version updates.	• Data drift, concept drift and performance decay indicators • Back-testing and outcomes analysis for credit, pricing and fraud models • Material change definitions and re-validation triggers • Version pinning and regression testing for foundation model updates
FAIGP-3.6	Evaluate vendor and third-party models, and the use of AI in regulatory capital, provisioning and actuarial models, including supervisory approval implications.	• Validating vendor models with limited transparency and proprietary components • AI in IRB models and supervisory approval of model changes • AI in IFRS 9 and CECL expected credit loss estimates • AI in Solvency II internal models and actuarial reserving

Domain IV. Fairness, Explainability and Consumer Outcomes (13%, about 10 scored items)

How to test and evidence fair treatment and understandable decisions when AI is used in credit, insurance and customer journeys. Covers discrimination law, explanation duties, consumer outcomes, complaints and redress.

Code	Task: the certified professional can	Knowledge of
FAIGP-4.1	Test credit models for fair lending risk, including disparate treatment, proxy discrimination and disparate impact where it still applies, and search for less discriminatory alternatives.	• ECOA after July 2026, the Fair Housing Act and state fair lending laws • Proxy detection for protected characteristics in alternative and behavioural data • Fairness metrics, their trade-offs and why they cannot all be met • Less discriminatory alternative searches and documented business justification
FAIGP-4.2	Design adverse action and explanation processes that give specific, accurate principal reasons for decisions made by complex credit and insurance models.	• Regulation B specific principal reasons, unchanged by withdrawn CFPB circulars • Translating feature attributions into accurate, actionable reason codes • Colorado SB 26-189 explanation, correction, human review and deemed-compliance carve-outs • GDPR Article 22, UK Articles 22A to 22D and AI Act Article 86 rights
FAIGP-4.3	Assess insurance AI and external consumer data for unfair discrimination using Colorado quantitative testing, NYDFS Circular Letter No. 7, the NAIC bulletin and EIOPA expectations.	• Actuarial justification versus unfair discrimination in underwriting and pricing • Colorado ECDIS testing methods using inferred demographic data • NYDFS expectations for ECDIS, governance and third-party vendors • Price optimisation, price walking and UK and EU fair pricing concerns
FAIGP-4.4	Evaluate customer outcomes of AI under the FCA Consumer Duty and equivalent regimes, including vulnerable customers, cohort outcome monitoring and AI personalisation risks.	• Consumer Duty outcomes and cross-cutting rules applied to AI • Identifying vulnerable customers without harmful profiling • Outcome monitoring metrics by customer cohort and channel • Sludge, dark patterns and AI exploitation of behavioural biases
FAIGP-4.5	Select explainability methods suited to model type and audience, and judge their limits, stability and suitability as evidence for customers, validators and supervisors.	• Global versus local explanations and inherently interpretable models • SHAP, LIME, counterfactuals and surrogate models: strengths and failure modes • Explanation stability, faithfulness and manipulation risks • Explaining generative AI outputs: citations, retrieval traces and their limits

Code	Task: the certified professional can	Knowledge of
FAIGP-4.6	Design complaints handling, contestation, human review and redress processes for AI-driven decisions, and use complaint data as an early warning signal.	• Meaningful human review versus rubber-stamping automated decisions • Complaint root cause analysis linked to model monitoring • Redress design and remediation of affected customer populations • Ombudsman and supervisor expectations for AI-related complaints

Domain V. Data Governance, Privacy and Financial Crime AI (11%, about 9 scored items)

How to govern the data that financial AI depends on, protect customer information when AI is used, and govern AI that fights financial crime. Covers data quality and lineage, alternative data, privacy, AML, sanctions, fraud and identity.

Code	Task: the certified professional can	Knowledge of
FAIGP-5.1	Apply BCBS 239 data quality, lineage and aggregation principles to AI training, feature and inference data, including feature stores and data pipelines.	• BCBS 239 principles on accuracy, completeness, timeliness and adaptability • Data lineage from source systems to features and model outputs • Quality controls for labels, sampling and reject inference • Dataset and feature versioning for reproducibility
FAIGP-5.2	Assess alternative and third-party data for legal permissibility, accuracy, consent, provenance and proxy risk before use in credit, insurance or marketing AI.	• Alternative data types: open banking, telematics, behavioural and device data • Consumer reporting rules that constrain alternative data use • Provenance, licensing and consent evidence for purchased data • Proxy and stability testing of new data sources
FAIGP-5.3	Control privacy, confidentiality and data leakage risks when using AI, including LLM prompts, retrieval stores, data residency, processor duties and banking secrecy.	• DPIAs and lawful basis for AI processing of customer data • Leakage through prompts, outputs, logs, fine-tuning and retrieval stores • Data residency, cross-border transfer and banking secrecy constraints • Processor and subprocessor duties of AI and services providers
FAIGP-5.4	Govern AI used in AML/CFT transaction monitoring, sanctions screening and fraud detection, including tuning, below-the-line testing, alert suppression and defending models to examiners.	• SR 26-2 retirement of SR 21-8 and supervisor acceptance of AI monitoring • Threshold tuning, below-the-line testing and alert suppression risks • Fuzzy matching, transliteration and false negative risks in sanctions screening • Evidence packs that explain AML model logic to examiners

Code	Task: the certified professional can	Knowledge of
FAIGP-5.5	Design KYC, onboarding and authentication controls that resist deepfakes and synthetic identities, drawing on the FATF horizon scan and current fraud typologies.	• FATF December 2025 horizon scan findings on AI and deepfakes • Presentation and injection attack detection in remote onboarding • Synthetic identity patterns and AI-enabled authorised push payment fraud • Layered authentication and out-of-band verification for high-risk instructions

Domain VI. Third-Party, Concentration and Operational Resilience (12%, about 9 scored items)

How to manage AI dependencies on technology suppliers, cloud and foundation model providers, and keep important business services resilient. Covers DORA, critical third-party regimes, contracts, exit and the obligations of technology and services suppliers.

Code	Task: the certified professional can	Knowledge of
FAIGP-6.1	Apply DORA to AI and model providers, including the register of information, pre-contract risk assessment, subcontracting chains, incident duties and oversight of critical providers.	• Register of information content and treatment of AI services • Assessing ICT services that support critical or important functions • Subcontracting chain requirements for services built on foundation models • Oversight of critical ICT third-party providers and what remains with firms
FAIGP-6.2	Assess concentration and fourth-party risk in cloud, compute and foundation model supply chains, including base-model provenance and the geopolitics of model origin.	• Concentration in cloud, chips, foundation models and data providers • Fourth-party risk when vendors embed third-party base models • Provenance, licensing and jurisdiction-of-origin risks for open-weight models • Supervisory concern about correlated failures and systemic concentration
FAIGP-6.3	Negotiate and review AI contract clauses, including audit and access rights, notice of model changes, data use limits, intellectual property, incident support, service levels and exit.	• DORA Article 30 key contractual provisions and equivalent outsourcing rules • Model change notification, testing windows and version pinning clauses • Restrictions on provider use of client data for model training • Liability, indemnity and intellectual property terms for AI outputs

Code	Task: the certified professional can	Knowledge of
FAIGP-6.4	Design exit strategies, substitutability tests and resilience measures for important business services that rely on AI, under DORA, APRA CPS 230 and UK impact tolerances.	• Important business services, impact tolerances and severe but plausible scenarios • Exit plans, substitutability and multi-vendor architectures for AI • CPS 230 material service provider and business continuity requirements • Threat-led penetration testing scope that includes AI components
FAIGP-6.5	Define the obligations of technology, consulting and services firms that build or run AI for financial clients, as ICT providers and under AI Act value chain rules.	• Provider versus deployer's supplier roles and Article 25 triggers • Contractual flow-down of DORA, outsourcing and confidentiality requirements • Technical documentation, logging and evidence clients need from suppliers • Governing AI-assisted engineering, coding and human verification in client delivery

Domain VII. Generative, Agentic and Emerging AI in Finance (12%, about 9 scored items)

How to govern generative and agentic AI in financial services, from copilots and AI-written communications to agents that move money and AI in trading. Covers frontier-AI cyber threats and horizon technologies.

Code	Task: the certified professional can	Knowledge of
FAIGP-7.1	Govern generative AI copilots and customer communications, addressing suitability, advice boundaries, AI-washing, transparency, recordkeeping and supervision of AI-assisted staff.	• Suitability and advice boundaries for GenAI in investment and insurance • AI-washing risk in marketing and investor disclosures • Recordkeeping and supervision of AI communications under FINRA and SEC rules • AI Act Article 50 transparency and SFC generative AI expectations
FAIGP-7.2	Design controls for AI agents, including unique agent identity, least privilege, tool scoping, transaction limits, dual approval, tamper-evident logs and tested kill switches.	• Non-human identity management and credential scoping for agents • Hard limits enforced outside the model versus prompt-level instructions • Dual approval thresholds and human-in-the-loop design • Kill switch, rollback and safe-state design and testing

Code	Task: the certified professional can	Knowledge of
FAIGP-7.3	Establish an agent registry and lifecycle governance for single and multi-agent systems, aligned to FSB, HKMA, IMDA and US examiner expectations.	• Registry attributes: owner, purpose, autonomy level, tools, limits, dependencies • IMDA agentic AI framework and FSB agent control practices • Multi-agent interaction risks, cascading errors and agentic contagion • Evaluation and monitoring of agent behaviour in production
FAIGP-7.4	Assess agentic payments and commerce, including customer mandates, authorisation and authentication, liability for unauthorised transactions, fraud and dispute handling.	• Customer mandate design and scope limits for payment agents • Strong customer authentication when agents initiate payments • Liability allocation under the PSD3 and Payment Services Regulation texts and UK APP fraud reimbursement • Fraud, dispute and chargeback implications of agent-initiated transactions
FAIGP-7.5	Govern AI in trading and investment management under MiFID II RTS 6, ESMA and IOSCO expectations, addressing herding, procyclicality and market abuse risks.	• RTS 6 self-assessment, testing, kill functionality and change records • Ability to stop third-party and AI-driven algorithms • Herding, procyclicality and correlated model behaviour in markets • Market abuse surveillance of and by AI systems
FAIGP-7.6	Evaluate frontier-AI cyber threats and horizon technologies, including quantum computing and tokenisation, and their implications for financial AI risk and controls.	• Frontier-AI offensive cyber capabilities flagged by financial stability bodies • Prompt injection, model theft and AI supply chain attacks • Post-quantum cryptography migration and AI system dependencies • Tokenised assets and AI-driven smart contract risks

Domain VIII. Assurance, Audit, Incidents and Board Reporting (12%, about 9 scored items)

How to give boards, auditors and supervisors justified confidence that AI is under control, and how to respond when it is not. Covers second and third line review, ISO/IEC 42001 audits, supervisory examinations, incidents, reporting, literacy and horizon scanning.

Code	Task: the certified professional can	Knowledge of
FAIGP-8.1	Plan and perform second line reviews and internal audits of AI governance, controls and individual AI systems using a risk-based methodology.	• Risk-based AI audit universe and coverage planning • Auditing data, models, prompts, agents and human oversight • Testing design and operating effectiveness of AI controls • Reporting AI findings to audit and risk committees
FAIGP-8.2	Prepare evidence packs for supervisory examinations and ISO/IEC 42001 certification audits, including model cards, impact assessments, validation reports and control testing results.	• ISO/IEC 42001 clauses and Annex A controls most relevant to finance • ISO/IEC 42006 auditor competence and audit process requirements • Typical supervisor requests in AI thematic reviews and examinations • Model cards, system cards and ISO/IEC 42005 impact assessments
FAIGP-8.3	Classify, escalate and report AI incidents, aligning internal taxonomies with DORA major ICT incident criteria, AI Act serious incident duties and conduct breach reporting.	• AI incident types: performance, bias, security, misuse and agent malfunction • DORA major ICT incident classification criteria and reporting stages • AI Act serious incident reporting duties for high-risk system providers • Post-incident review, customer remediation and lessons learned
FAIGP-8.4	Design key risk indicators, dashboards and board reports that show AI risk against appetite, emerging issues, validation backlog and regulatory change.	• Leading and lagging AI KRIs and threshold setting • Aggregating model, conduct, third-party and cyber AI risk • Board reporting formats that support challenge and decisions
FAIGP-8.5	Design AI literacy and competence programmes for boards, senior managers, control functions, staff and large delivery workforces, with role-based content and evidence of competence.	• Board and senior manager AI literacy expectations across regimes • Role-based curricula for first, second and third line staff • Scaling literacy across multinational delivery centres and suppliers • Measuring competence rather than course completion
FAIGP-8.6	Run horizon scanning across 2027-2028 regulatory deadlines and emerging AI practice, and turn changes into prioritised updates to policies, controls and training.	• Key dates: MAS 2027 and 2028, AI Act December 2027, Colorado 2027 • Pending items: US AI model risk RFI, HKMA agentic paper, MAS consultation • Impact assessment and prioritisation of regulatory change

7. Reference frameworks

Candidates should be familiar with the intent, scope and practical consequences of the following laws, regulations, guidance and standards. Questions test the ability to apply them, not to recite them. Where a framework is proposed, delayed or being phased in, candidates are expected to understand its status and direction.

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 duties apply from 2 December 2027	Classify credit scoring and life and health insurance pricing AI, assign provider or deployer roles, and run Article 27 FRIAs.
Digital Operational Resilience Act (Regulation (EU) 2022/2554)	EU	Applies since 17 January 2025; critical ICT third-party providers designated November 2025	Record AI and model providers in the register, apply Article 30 contract terms, report major ICT incidents and plan exit.
EBA AI Act mapping factsheet and EIOPA AI Opinion	EU	EBA factsheet November 2025; EIOPA Opinion August 2025	Show how banking and insurance governance rules already meet AI Act duties, and apply proportionate controls to non-high-risk insurance AI.
Consumer Credit Directive (EU) 2023/2225	EU	Applies from 20 November 2026 under national transposing laws	Run creditworthiness assessments with permitted data, and give rights to human intervention, explanation and contest for automated decisions.
MiFID II RTS 6 (Delegated Regulation (EU) 2017/589) and ESMA algorithmic trading briefing	EU	RTS 6 in force; ESMA supervisory briefing issued 26 February 2026	Include AI in algorithmic trading self-assessments, test and record material changes, and keep the ability to stop third-party algorithms.
GDPR Article 22 and UK GDPR automated decision-making rules	EU and UK	In force; UK reforms under the Data (Use and Access) Act 2025 apply from 5 February 2026	Decide when automated credit or insurance decisions need human intervention, explanation and contest rights, and run DPIAs.
Interagency Guidance on Model Risk Management (SR 26-2 / OCC Bulletin 2026-13)	US	Issued 17 April 2026; rescinds SR 11-7; excludes generative and agentic AI	Tier models on inherent risk and materiality, and design separate controls for generative and agentic AI outside its scope.
Equal Credit Opportunity Act and Regulation B	US	Final rule effective 21 July 2026 removes ECOA disparate-impact liability	Give specific, accurate principal reasons for adverse action and test for disparate treatment, including through proxies.
NAIC Model Bulletin on the Use of AI Systems by Insurers	US	Adopted by 29 jurisdictions as at October 2026; evaluation tool in pilot	Build a written insurer AI governance framework covering third-party data and models, and prepare for examiner questionnaires.
Colorado SB21-169 and Division of Insurance AI governance regulation	US (Colorado)	Amended regulation effective 15 October 2025; annual compliance reports required	Govern external consumer data and algorithms in life, auto and health insurance, including quantitative unfair discrimination testing.

Framework, law or standard	Jurisdiction	Status (October 2026)	What a holder must be able to do
Colorado SB 26-189 (replacing SB 24-205)	US (Colorado)	Signed 14 May 2026; effective 1 January 2027; federal constitutional challenge expected	Identify where lending and insurance decisions need notice, explanation, correction and human review, and where existing compliance suffices.
NYDFS Insurance Circular Letter No. 7 and AI cybersecurity industry letter	US (New York)	Circular Letter July 2024; Part 500 AI cybersecurity letter October 2024	Test ECDIS and AI underwriting for unfair discrimination and address AI-enabled cyber threats under Part 500.
SEC examination priorities and FINRA 2026 Regulatory Oversight Report	US	SEC predictive analytics proposal withdrawn June 2025; FY2026 priorities include AI-washing	Supervise GenAI use under FINRA Rule 3110, keep required records and substantiate every AI capability claim to clients.
PRA SS1/23 Model Risk Management Principles for Banks	UK	In force since May 2024; April 2026 letter confirms existing rules apply to AI	Apply the five principles to AI models, including identification, tiering, validation, independent challenge and senior manager accountability.
FCA Consumer Duty, SM&CR and AI good and poor practice findings	UK	Duty in force; AI practice findings published 19 October 2026	Evidence good outcomes for retail customers, including vulnerable customers, and allocate senior manager accountability for AI from design.
UK Critical Third Parties regime	UK	First designations made July 2026	Explain how designated cloud and technology providers are overseen, and which responsibilities stay with each firm.
MAS Guidelines on AI Risk Management	Singapore	Final 7 October 2026; sections 3-4 apply from 7 October 2027	Establish board oversight, an AI inventory, risk materiality assessment, lifecycle controls and third-party AI management.
HKMA ART framework and Supervisory Guidance for Responsible Adoption of AI	Hong Kong	Issued 15 October 2026; agentic AI discussion paper forthcoming	Apply accountability, resilience and trust expectations, and anticipate the proposed registry of material AI agents.
APRA CPS 230, CPS 234 and AI letter to industry	Australia	CPS 230 in force 1 July 2025; AI letter issued 30 April 2026	Treat AI suppliers as material service providers, plan exit, and control prompt injection and non-human identities.
BNM RMiT and Discussion Paper on AI in the Financial Sector	Malaysia	RMiT revised November 2025, reissued September 2026; AI discussion paper August 2025, not final	Apply technology risk, cloud and outsourcing controls to AI and track the expected AI policy document.
RBI FREE-AI Committee report and draft Model Risk Management guidance	India	FREE-AI report 13 August 2025; MRM guidance draft issued 24 June 2026	Map the seven Sutras and draft model risk principles to bank and NBFC AI portfolios in India.
FSB Sound Practices for Responsible Adoption of AI	Global	Final 15 October 2026; 12 non-binding practices	Benchmark board AI strategy, risk appetite, lifecycle controls, human oversight and third-party AI practices.
IOSCO Supervisory Toolkit for AI in Capital Markets	Global	Final 25 May 2026	Anticipate securities supervisors' questions on AI governance, testing, conflicts of interest and market integrity.

Framework, law or standard	Jurisdiction	Status (October 2026)	What a holder must be able to do
BCBS 239 Principles for Effective Risk Data Aggregation and Risk Reporting	Global	Published 2013; supervisory expectation for systemically important banks	Extend data quality, lineage and aggregation controls to AI training, feature and inference data.
FATF Horizon Scan: AI and Deepfakes	Global	Published 22 December 2025	Design customer due diligence and fraud controls that resist deepfakes and synthetic identities.
ISO/IEC 42001:2023, ISO/IEC 42005:2025, ISO/IEC 42006:2025 and NIST AI RMF 1.0 with GenAI Profile	International	Published standards; NIST Cyber AI Profile (IR 8596) in draft	Build an AI management system, run impact assessments and prepare for certification audits by competent bodies.

Status reflects published information as at October 2026. GAICC reviews this list at least annually; examination items are not based on changes published less than six months before an examination window.

8. Sample questions

These questions show the style and level of the examination. They are not drawn from the live item bank.

Sample question 1 · FAIGP-2.1 · Analysis and Evaluation

An EU bank is building its AI Act inventory. It uses (1) a machine learning model to assess the creditworthiness of sole traders applying for business overdrafts, (2) the same model design to score limited companies, and (3) a model that flags card transactions as likely fraud and holds them until the customer confirms. Which assessment is most defensible?

A. All three are high-risk, because each one is used in decisions that affect customers' access to financial services and products.

B. Only the fraud model is high-risk, because it holds transactions automatically without prior human review.

C. The sole trader model is high-risk, with obligations from 2 December 2027; the other two fall outside Annex III.

D. None is high-risk, because business lending falls outside consumer credit law and the fraud model only affects card payments.

> **Answer: C**
>
> Annex III point 5(b) covers creditworthiness assessment and credit scoring of natural persons, which includes sole traders, and expressly excludes AI used to detect financial fraud. Scoring limited companies is not covered. Option A extends the category to legal persons and fraud; B inverts the fraud carve-out; D wrongly ties scope to consumer credit law.

Sample question 2 · FAIGP-3.4 · Analysis and Evaluation

A UK retail bank plans to deploy a large language model that reads incoming complaints, assigns a category and urgency, and flags signs of customer vulnerability for priority handling. The vendor reports high accuracy on a public benchmark. The validation team proposes approval based on that benchmark plus an accuracy test on a random sample of historic complaints. What is the strongest validation approach?

A. Accept the benchmark and random sample test, because the model only routes complaints and a person makes every final decision on each complaint.

B. Exclude the model from validation entirely, because the latest US interagency model risk guidance treats generative AI as out of its scope.

C. Fine-tune the model on the bank's own historical complaints first, so that the vendor's published benchmark becomes representative of the bank's customers.

D. Build a task-specific test set rich in vulnerability cues, measure missed vulnerability and misrouting against human labels, and monitor live.

> **Answer: D**
>
> Overall accuracy on a benchmark or random sample hides failures on rare, high-harm cases such as vulnerable customers, which Consumer Duty makes critical. D targets those failure modes and continues after deployment. B is wrong: the SR 26-2 exclusion is a US position and does not remove PRA and FCA expectations. A understates the harm of misrouting.

Sample question 3 · FAIGP-4.2 · Application

A US card issuer declines applicants using a gradient-boosted model. Its adverse action notices pick four reasons from a standard checklist through a lookup table built years ago. Validation finds that for many declines the largest attributions come from an interaction between recent credit inquiries and cash advance behaviour, which the table maps to 'insufficient length of credit history'. What should the issuer do?

A. Rebuild the reason mapping so notices state the factors that actually drove each decline, and test reasons for accuracy and stability.

B. Make no change, because the CFPB withdrew its adverse action circulars in May 2025 and checklist reasons are now sufficient.

C. Stop giving reasons for model-based declines, because the July 2026 Regulation B rule removed disparate-impact liability under ECOA.

D. Send each declined applicant the full table of feature attributions from the model, so they can see every factor that contributed to the score.

Answer: A

Regulation B still requires specific principal reasons that reflect the factors actually considered. Withdrawing the circulars removed guidance, not the requirement, so B fails. The July 2026 rule concerns disparate impact, not notices, so C fails. A raw attribution table is neither a statement of principal reasons nor understandable to applicants, so D fails.

Sample question 4 · FAIGP-6.3 · Application

An EU insurer uses an IT services firm to run a claims assistant built on a third-party foundation model. The assistant supports a function the insurer classes as important. A review finds that the model provider replaced the underlying model version twice last quarter without notice, and the style and content of claims summaries changed. Under DORA, what is the most appropriate response?

A. Rely on the model provider's published independent assurance report, because a foundation model provider is not part of the ICT supply chain under DORA.

B. Move at once to a self-hosted open-weight model, which removes the third-party dependency and gives the insurer full control over model versions and change timing.

C. Amend the contracts to require advance notice of material model changes with a test window, extend audit and exit rights down the chain, update the register.

D. Treat the issue as model risk only, and re-validate the assistant in full after each provider update before it goes back into live claims handling.

Answer: C

DORA requires firms to manage ICT third-party risk through subcontracting chains that support critical or important functions, with Article 30 terms on audit, access, notice and exit. C fixes the root cause and records the dependency. D is useful but only reacts after each change. B is a disproportionate move that creates new risks, and A misreads DORA scope.

Sample question 5 · FAIGP-7.2 · Application

A bank pilots an AI agent that reads supplier invoices, matches them to purchase orders and initiates payments in the accounts payable system. The project team proposes that the agent use the accounts payable team's existing service account, and that its system prompt instruct it never to pay above the approved limit. Which control design best addresses the main risks?

A. Keep the proposed design and have a person review a weekly sample of agent payments after they are made.

B. Give the agent its own least-privilege identity, enforce limits in the payment system, require dual approval above a threshold and test a kill switch.

C. Require a person to approve every payment the agent prepares, which removes the need for a separate agent identity or limits.

D. Replace the prompt instruction with a separate guardrail model that checks every payment instruction against the approved limit before the agent submits it.

Answer: B

Prompt instructions and guardrail models can be bypassed, for example by injected text in an invoice, so limits must be enforced outside the model, and a shared account defeats attribution and least privilege. Approving every payment (C) invites rubber-stamping and leaves credentials unscoped. After-the-fact sampling (A) cannot prevent loss. B reflects emerging supervisory expectations for agent controls.

9. Eligibility

Certification is open to anyone who completes the training requirement. There is no academic or years-of-experience requirement.

Requirement	Status	Detail
Training	Required	32 contact hours of FAIGP 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 financial services risk, compliance, model development or validation, audit, or technology delivery to financial institutions, including two years working with AI or quantitative models, is recommended. Experience is never used to refuse a candidate.
Prior credential	Recommended, not required	GAICC Certified Professional in AI Governance (CPAIG) or equivalent foundational AI governance knowledge.

Three equal 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.

No route gives an examination advantage. Certification decisions are made independently of training.

10. Maintaining the certification

- 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 financial services 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

Competency (GAICC AI Competence Triangle)	What it covers	CPD hours
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**

The GAICC Candidate Handbook and the GAICC Recertification Procedure (GAICC-QMS-PRO-REC-001) are the authority on renewal.

11. Frequently asked questions

Do I need work experience?

No. Experience is recommended, not required, and is never used to refuse a candidate. The only eligibility requirement is the 32 contact hours of training.

Do I need the CPAIG before the FAIGP?

No. The CPAIG or equivalent foundational knowledge is recommended because the FAIGP builds on core AI governance concepts and applies them to banking, insurance, capital markets and payments.

I work in insurance, not banking. Is the FAIGP relevant?

Yes. Insurance runs throughout: underwriting and pricing AI, claims automation, external consumer data testing under Colorado and NYDFS rules, the NAIC bulletin, the EIOPA AI Opinion, Solvency II internal models and AI Act high-risk duties for life and health insurance pricing. Cases alternate between banking, insurance, asset management and payments.

I work for a technology vendor or IT services firm that serves banks. Is this for me?

Yes. Domain VI covers your obligations as an ICT third-party provider under DORA and similar regimes, and when you become an AI Act provider or a deployer's supplier. You learn what evidence, contract terms, change notices and incident support financial clients and their supervisors will expect from you.

I already work in model validation. What does the FAIGP add?

It extends model risk practice to areas classic validation does not reach: large language models, AI agents, vendor foundation models, fairness and explanation duties, and third-party and resilience rules. It also connects validation findings to senior manager accountability, board reporting and supervisory evidence.

SR 11-7 has been rescinded. How does the course handle US model risk expectations?

The course teaches SR 26-2 and OCC Bulletin 2026-13, issued 17 April 2026, including risk-based tiering and the exclusion of generative and agentic AI. Because those uses sit outside the guidance, you learn to govern them through a firm-wide AI risk standard that answers the questions examiners are now asking.

Can our firm run the course for its own staff with our own cases?

Yes. GAICC Authorised Training Partners can deliver the 32-hour curriculum to enterprise cohorts across countries, with case studies tailored to your products, jurisdictions and delivery model. The Examination Content Outline and the examination stay the same for every candidate.

Where are the fees?

Examination, membership and renewal fees are published in the applicable GAICC Candidate Handbook and at certifications.gaicc.org. To maintain a single source of truth, fee amounts are not reproduced in this document.

Document control

Document	Examination Content Outline: Finance AI Governance Professional (FAIGP)
Document code	GAICC-ECO-FAIGP-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