Global AI Certification Council

GAICC TRAINING · COURSE CURRICULUM

[FAIGP]

Finance AI Governance Professional

32-Hour Course Curriculum

1st Edition | 2026 | v1.1

Course	Finance AI Governance Professional (FAIGP) certification course
Document code	GAICC-CUR-FAIGP-001
Version	1.1 · 30 October 2026
Duration	4 days · 32 contact hours · 32 CPD hours
Prepares for	GAICC Finance AI Governance Professional (GAICC-FAIGP)

1. Course overview

The 32-hour course runs over four days, two domains per day, in the order a financial institution meets AI risk: strategy and accountability, regulation, model risk, fairness and conduct, data and financial crime, third parties and resilience, generative and agentic AI, and assurance. Every module uses realistic cases from banking, insurance, capital markets and payments, and from the technology and services firms that build and run AI for them. Learners work on templates they can take back to their firm, and Day 4 ends with an integrated capstone and exam readiness session.

Duration **4 days · 32 contact hours**	**CPD** **32 CPD hours on completion**	**Modules** **18 modules plus capstone**
Delivery **In person, live online, or GAICC self-paced**	**Class size** **Recommended maximum of 24 learners**	**Leads to** **GAICC Finance AI Governance Professional (GAICC-FAIGP)**

Course learning outcomes

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

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.

Who should attend

- 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

2. Course at a glance

Module	Title	Domains	Hours
Day 1	**Landscape, accountability and regulation**	Domains I, II	**8.0 h**
M01	AI across the financial services value chain	I	1.5 h
M02	Board strategy, accountability and three lines	I	2.0 h
M03	EU AI Act and European supervisory positions	II	2.0 h
M04	US, UK, APAC and global supervisory expectations	II	2.5 h
Day 2	**Model risk and fair outcomes**	Domains III, IV	**8.0 h**
M05	Model scope, tiering and conceptual soundness	III	1.5 h
M06	Validation, effective challenge and GenAI evaluation	III	2.0 h
M07	Monitoring, model change, vendor and capital models	III	1.0 h
M08	Fair lending, insurance fairness and explainability	IV	2.0 h
M09	Consumer outcomes, complaints and redress	IV	1.5 h
Day 3	**Data, crime and third parties**	Domains V, VI	**8.0 h**
M10	Financial data governance and privacy for AI	V	2.0 h
M11	Financial crime AI and deepfake-resistant KYC	V	2.0 h
M12	DORA, AI contracts and supplier obligations	VI	2.0 h
M13	Concentration, exit and operational resilience	VI	2.0 h
Day 4	**Agentic AI and assurance**	Domains VII, VIII, I, II, III, IV, V, VI	**8.0 h**
M14	GenAI advice, communications and AI in trading	VII	1.5 h
M15	Agentic AI controls, registries and payments	VII	2.0 h
M16	Assurance, audit and supervisory evidence	VIII	1.5 h
M17	Incidents, board reporting, literacy and horizon scanning	VIII	1.5 h
M18	Capstone and exam readiness	I, II, III, IV, V, VI, VII, VIII	1.5 h
Total			**32.0 h**

3. Detailed curriculum

DAY 1

Landscape, accountability and regulation

Who owns financial AI risk and which rules apply, across the EU, US, UK, Asia-Pacific and global standard setters.

M01 AI across the financial services value chain · 1.5 hours

Domains I · Competencies FAIGP-1.1, FAIGP-1.5

Learning outcomes	• Classify financial AI use cases by decision impact and regulatory exposure • Build materiality-tiered inventory entries that capture vendor and embedded AI • Distinguish predictive, generative and agentic AI risks in finance
Topics	Credit, underwriting, pricing and claims AI · Fraud, AML, trading and treasury AI · Advice, servicing and staff copilots · Shadow AI and AI embedded in vendor platforms · Inventory attributes and materiality factors · Linking the AI inventory, model inventory and DORA register
Activity	Learners triage fifteen AI use cases from a composite universal bank and insurer, rate materiality and decide which belong in the model inventory, the AI inventory or both.

M02 Board strategy, accountability and three lines · 2.0 hours

Domains I · Competencies FAIGP-1.2, FAIGP-1.3, FAIGP-1.4

Learning outcomes	• Draft an AI risk appetite statement with measurable limits and escalation triggers • Allocate senior manager responsibilities for AI and evidence reasonable steps • Design committee mandates and three lines roles for AI
Topics	Board AI strategy and risk appetite · SM&CR, FAR and Asian individual accountability regimes · Statements of responsibilities for AI · Three lines of defence for AI · FCA good and poor practice findings on AI governance · Board AI literacy
Activity	In a simulated board risk committee, teams defend a draft AI risk appetite statement and responsibilities map for a mid-sized bank after a chatbot mis-selling incident.

M03 EU AI Act and European supervisory positions · 2.0 hours

Domains II · Competencies FAIGP-2.1, FAIGP-2.2

Learning outcomes	• Determine high-risk status and value chain role for credit and insurance AI • Scope a fundamental rights impact assessment within existing governance • Explain where financial services law already meets AI Act duties
Topics	Annex III point 5 and the fraud detection carve-out · Omnibus timetable to December 2027 and August 2028 · Provider, deployer and Article 25 substantial modification · Article 26 deployer duties and Article 27 FRIA · EBA, EIOPA and ESMA positions · Financial supervisors as market surveillance authorities
Activity	Learners classify six AI systems at an EU bancassurance group, including a small business credit model used for sole traders, and scope the FRIA for a life insurance pricing model.

M04 US, UK, APAC and global supervisory expectations · 2.5 hours

Domains II · Competencies FAIGP-2.3, FAIGP-2.4, FAIGP-2.5, FAIGP-2.6

Learning outcomes	• Interpret SR 26-2, Regulation B and state insurance AI rules after recent changes • Apply UK, Singapore, Hong Kong, Australian, Malaysian, Indian and NZ expectations • Build a multi-jurisdiction obligations map with common controls
Topics	SR 26-2 scope and the generative and agentic AI gap · Regulation B, Colorado, NYDFS and the NAIC bulletin · Federal and state conflict and litigation risk · PRA SS1/23, Consumer Duty and AI Live Testing · MAS Guidelines, HKMA ART, APRA, BNM and RBI · New Zealand FMA and RBNZ expectations · FSB, IOSCO and Basel Committee positions
Activity	Teams build an obligations map for a banking and insurance group operating in the UK, US, Singapore, Hong Kong and Australia, then reconcile it into twelve common controls with named evidence owners.

DAY 2

Model risk and fair outcomes

How to validate machine learning and generative models and prove that credit, insurance and customer decisions are fair and explainable.

M05 Model scope, tiering and conceptual soundness · 1.5 hours

Domains III · Competencies FAIGP-3.1, FAIGP-3.2

Learning outcomes	• Tier AI on inherent risk and materiality, including GenAI outside SR 26-2 • Assess the conceptual soundness of a machine learning credit model • Specify documentation that permits independent replication
Topics	Model definitions across SR 26-2, SS1/23 and the RBI draft · Inherent risk and materiality tiering · A firm-wide AI risk standard for non-model AI · Data representativeness and target leakage · Monotonic constraints and business intuition · Developer documentation standards
Activity	Learners review the development pack for a gradient-boosted mortgage default model and raise conceptual soundness findings on target leakage, through-the-cycle representativeness and monotonicity.

M06 Validation, effective challenge and GenAI evaluation · 2.0 hours

Domains III · Competencies FAIGP-3.3, FAIGP-3.4

Learning outcomes	• Plan an independent validation with benchmarks, challengers and stress tests • Design an evaluation approach for an LLM application where classic tests fail • Rate validation findings and set conditions for approval
Topics	Effective challenge: independence, competence and influence · Challenger and benchmark models · Sensitivity and stress testing · LLM evaluation sets, groundedness and hallucination metrics · Red teaming and the limits of LLM-as-judge · Findings, severity and conditional approval
Activity	Teams validate an LLM complaints-triage model at a retail bank, building a stratified evaluation set that tests vulnerable customer detection and routing of reportable complaints.

M07 Monitoring, model change, vendor and capital models · 1.0 hours

Domains III · Competencies FAIGP-3.5, FAIGP-3.6

Learning outcomes	• Set drift thresholds, outcomes analysis and material change triggers • Assess AI use in IRB, expected credit loss and Solvency II models
Topics	Drift and performance decay indicators · Back-testing and outcomes analysis · Material change and foundation model version updates · Vendor model validation with limited transparency · AI in IRB, IFRS 9, CECL and Solvency II internal models
Activity	Learners decide whether a vendor's unannounced upgrade to the base model behind a fraud scoring service is a material change, and what re-validation it requires.

M08 Fair lending, insurance fairness and explainability · 2.0 hours

Domains IV · Competencies FAIGP-4.1, FAIGP-4.2, FAIGP-4.3, FAIGP-4.5

Learning outcomes	• Test a credit model for proxy discrimination and less discriminatory alternatives • Generate accurate adverse action reason codes from feature attributions • Run an external consumer data unfair discrimination test for an insurer • Choose explainability methods and state their limits
Topics	ECOA and Regulation B after July 2026 · Proxy discrimination and alternative data · Fairness metrics and trade-offs · Reason codes from SHAP values and counterfactuals · Colorado and NYDFS ECDIS testing · Explainability methods and failure modes
Activity	Learners produce adverse action reason codes for a gradient-boosted credit card model and run a Colorado-style inferred-demographic bias test on a life insurer's accelerated underwriting model.

M09 Consumer outcomes, complaints and redress · 1.5 hours

Domains IV · Competencies FAIGP-4.4, FAIGP-4.6

Learning outcomes	• Design cohort outcome monitoring for an AI-driven customer journey • Build human review, contestation and redress for AI decisions
Topics	Consumer Duty outcomes and vulnerable customers · Personalisation, sludge and dark patterns · Meaningful human review · Complaint root cause analysis and redress
Activity	Teams design outcome metrics and a redress plan after a home insurance renewal pricing model is found to charge long-standing customers in a vulnerable cohort more.

DAY 3

Data, crime and third parties

How to govern the data, financial crime models and supplier chains that financial AI depends on, and keep AI-dependent services resilient.

M10 Financial data governance and privacy for AI · 2.0 hours

Domains V · Competencies FAIGP-5.1, FAIGP-5.2, FAIGP-5.3

Learning outcomes	• Apply BCBS 239 lineage and quality controls to AI features • Assess alternative data for permissibility, consent and proxy risk • Control leakage of customer data into LLM prompts and retrieval stores
Topics	BCBS 239 applied to AI data · Feature stores, lineage and dataset versioning · Open banking, telematics and other alternative data · DPIAs, lawful basis and banking secrecy · Leakage through prompts, logs and retrieval stores · Data residency and processor duties
Activity	Learners trace lineage for a small business lending model that uses open banking data, then design data controls for a relationship manager copilot that retrieves client files.

M11 Financial crime AI and deepfake-resistant KYC · 2.0 hours

Domains V · Competencies FAIGP-5.4, FAIGP-5.5

Learning outcomes	• Govern AML monitoring and sanctions screening AI to examiner standards • Design onboarding and authentication controls that resist deepfakes
Topics	AI in transaction monitoring and sanctions screening · Tuning, below-the-line testing and alert suppression · Explaining AML models to examiners · FATF horizon scan on AI and deepfakes · Injection attacks and synthetic identities · AI-enabled authorised push payment fraud
Activity	Teams prepare an examiner evidence pack for a machine learning alert-scoring model that suppresses low-risk alerts, then redesign remote onboarding after a deepfake-enabled account takeover.

M12 DORA, AI contracts and supplier obligations · 2.0 hours

Domains VI · Competencies FAIGP-6.1, FAIGP-6.3, FAIGP-6.5

Learning outcomes	• Record AI services in the DORA register and assess critical function support • Review AI contracts for Article 30 terms and model change notice • Define what a services firm must evidence as ICT supplier and AI Act actor
Topics	DORA register of information and AI services · Article 30 key contractual provisions · Subcontracting chains and foundation model providers · Oversight of critical ICT third-party providers · Model change, data use and intellectual property clauses · Supplier roles under AI Act Article 25
Activity	Learners mark up a master services agreement between an insurer and an IT services firm delivering a claims assistant built on a third-party foundation model.

M13 Concentration, exit and operational resilience · 2.0 hours

Domains VI · Competencies FAIGP-6.2, FAIGP-6.4

Learning outcomes	• Assess concentration and fourth-party risk in a foundation model supply chain • Design an exit plan and substitutability test for an AI-dependent service
Topics	Cloud, compute and foundation model concentration · Base-model provenance and jurisdiction of origin · UK Critical Third Parties regime and APRA CPS 230 · Important business services and impact tolerances · Exit plans and multi-vendor architecture · Threat-led penetration testing that includes AI
Activity	Teams write a DORA exit plan for a foundation model provider that supports a bank's customer servicing, including a tested fallback model and a severe but plausible outage scenario.

DAY 4

Agentic AI and assurance

How to govern generative and agentic AI that acts on money and markets, and how to assure, report and respond when things go wrong.

M14 GenAI advice, communications and AI in trading · 1.5 hours

Domains VII · Competencies FAIGP-7.1, FAIGP-7.5, FAIGP-7.6

Learning outcomes	• Set boundaries and supervision for GenAI in advice and communications • Apply RTS 6 and IOSCO expectations to AI-driven trading • Assess frontier-AI cyber threats to financial AI systems
Topics	Suitability and AI-washing · Recordkeeping and supervision of AI communications · RTS 6 self-assessment and kill functionality · Herding and procyclicality · Frontier-AI cyber offence and prompt injection · Quantum and tokenisation as horizon items
Activity	Learners review a wealth manager's GenAI portfolio commentary tool for suitability, AI-washing and recordkeeping gaps, then test an AI trading strategy's RTS 6 kill functionality and frontier-AI cyber exposure.

M15 Agentic AI controls, registries and payments · 2.0 hours

Domains VII · Competencies FAIGP-7.2, FAIGP-7.3, FAIGP-7.4

Learning outcomes	• Design identity, limit, dual approval and kill switch controls for agents • Build an agent registry entry and monitoring plan • Assess mandate, authentication and liability for agentic payments
Topics	Agent identity and least privilege · Transaction limits enforced outside the model · Dual approval and human-in-the-loop design · Kill switches and safe states · Agent registries and multi-agent risks · Agentic payments, mandates and liability
Activity	Teams design controls for an agentic payments pilot that pays supplier invoices, with dual approval above thresholds, out-of-band payee verification and a live kill switch test.

M16 Assurance, audit and supervisory evidence · 1.5 hours

Domains VIII · Competencies FAIGP-8.1, FAIGP-8.2

Learning outcomes	• Plan a risk-based audit of AI governance and of one AI system • Assemble an evidence pack for an examination or ISO/IEC 42001 audit
Topics	AI audit universe and methodology · Testing AI control design and operation · ISO/IEC 42001 and ISO/IEC 42006 · Supervisory examination evidence packs · Model cards and impact assessments
Activity	Learners respond to a mock supervisory request list on AI agents, assembling evidence on limits, audit trails and shutdown capability within a set time.

M17 Incidents, board reporting, literacy and horizon scanning · 1.5 hours

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

Learning outcomes	• Classify an AI incident against DORA and AI Act criteria • Design AI KRIs and a board report against appetite • Plan role-based AI literacy and a 2027-2028 horizon scan
Topics	AI incident taxonomy and escalation · DORA major ICT incident criteria · KRIs and board dashboards · Role-based AI literacy at scale · 2027-2028 deadlines and pending items
Activity	Teams classify an incident in which a servicing assistant gave thousands of customers wrong fee information, then draft the board report and the regulator notification decision.

M18 Capstone and exam readiness · 1.5 hours

Domains I, II, III, IV, V, VI, VII, VIII · Competencies FAIGP-1.2, FAIGP-2.6, FAIGP-3.4, FAIGP-4.2, FAIGP-5.4, FAIGP-6.4, FAIGP-7.2, FAIGP-8.3

Learning outcomes	• Integrate governance, risk and assurance decisions across a full AI lifecycle case • Apply exam technique to scenario-based questions
Topics	Integrated capstone case · Defending decisions to a mock supervisory panel · Domain review · Practice questions and exam technique
Activity	Teams take an agentic credit decisioning assistant at a cross-border bank from proposal to supervisory review, then complete timed practice questions.

4. Capstone and exam readiness

Teams take a cross-border bank's proposed agentic credit decisioning assistant, built by an external services firm on a third-party foundation model, from use case approval to supervisory review. They tier it, map obligations across the EU, UK and Singapore, and design validation, fairness testing, agent controls, contract terms and an exit plan. They then defend their decisions to a mock supervisory panel and board risk committee.

Assessment for learning

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

5. Learner toolkit

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

- AI use case and materiality tiering template
- AI risk appetite statement and KRI library
- Senior manager AI responsibilities map
- Multi-jurisdiction obligations map and common control set
- AI model validation plan with LLM evaluation checklist
- Fair lending and ECDIS testing workbook
- Adverse action reason code design guide
- DORA AI provider register and Article 30 clause checklist
- AI exit plan and substitutability template
- Agent control design and registry template
- AI incident classification and reporting decision tree
- Supervisory evidence pack index

6. Future watch

A recurring horizon-scanning segment keeps the course current. It covers emerging technology, regulation and practice in banking, insurance, capital markets and payments, and is refreshed at every curriculum review:

- US agencies' expected request for information on AI in model risk management
- HKMA agentic AI discussion paper and registries of material agents
- MAS consultation on agentic AI expected in 2027
- European Commission high-risk classification guidelines due by 1 August 2027
- Agentic payments and commerce: mandates, authentication and liability
- Frontier-AI cyber capabilities and financial stability
- Post-quantum cryptography and tokenised assets

- Concentration in foundation model and compute supply

7. Delivery requirements

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

8. Competency coverage matrix

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

Code	Task	Modules
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.	M01
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.	M02, M18
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.	M02
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.	M02
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.	M01
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.	M03
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.	M03
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.	M04
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.	M04
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.	M04
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.	M04, M18
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.	M05
FAIGP-3.2	Assess the conceptual soundness of machine learning models, including data representativeness, feature design, algorithm choice, hyperparameter tuning, overfitting and stability.	M05
FAIGP-3.3	Plan and perform independent validation and effective challenge using benchmarks, challenger models, sensitivity analysis, stress testing and replication of developer results.	M06

Code	Task	Modules
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.	M06, M18
FAIGP-3.5	Establish ongoing monitoring, outcomes analysis and model change management, including drift thresholds, recalibration triggers, material change definitions and vendor version updates.	M07
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.	M07
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.	M08
FAIGP-4.2	Design adverse action and explanation processes that give specific, accurate principal reasons for decisions made by complex credit and insurance models.	M08, M18
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.	M08
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.	M09
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.	M08
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.	M09
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.	M10
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.	M10
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.	M10
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.	M11, M18
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.	M11
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.	M12
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.	M13

Code	Task	Modules
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.	M12
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.	M13, M18
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.	M12
FAIGP-7.1	Govern generative AI copilots and customer communications, addressing suitability, advice boundaries, AI-washing, transparency, recordkeeping and supervision of AI-assisted staff.	M14
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.	M15, M18
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.	M15
FAIGP-7.4	Assess agentic payments and commerce, including customer mandates, authorisation and authentication, liability for unauthorised transactions, fraud and dispute handling.	M15
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.	M14
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.	M14
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.	M16
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.	M16
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.	M17, M18
FAIGP-8.4	Design key risk indicators, dashboards and board reports that show AI risk against appetite, emerging issues, validation backlog and regulatory change.	M17
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.	M17
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.	M17

9. CPD and progression

Completing the course earns 32 CPD hours, recorded on the certificate of completion. The course meets the training requirement for the FAIGP examination. For existing GAICC holders, the hours can

count towards renewal of other GAICC certifications under the Technology, Humanity and Strategy split, as recorded in the GAICC renewal register.

Document control

Document	32-Hour Course Curriculum: Finance AI Governance Professional (FAIGP)
Document code	GAICC-CUR-FAIGP-001
Version	1.1
Issued	30 October 2026
Status	Issued for courseware development
Owner	Global AI Certification Council Limited (GAICC), Certification Scheme Committee
Review cycle	At least annually, and whenever a material regulatory or standards change occurs in the sector