TRUST AI STANDARDS

Independent AI Governance Standards Body

Trust AI Governance Practitioner (TAIGP)

Level 1 — Practitioner Qualification

Two-Day Instructor-Led Program

Classroom or Virtual Live Training

Multiple-Choice Examination

Trust AI Academy

Aligned to Trust AI Standard v1.5 (Polaris)

Trust AI Governance Practitioner (TAIGP) — Course Prospectus
Document Version: v1.3
Approved By Trust AI Standards
Approval Date: 06 June 2026

1. About Trust AI Standards

Trust AI Standards is an independent AI Governance Accreditation Body and Authority. Trust AI Standards develops, maintains and licenses the Trust AI Certification Scheme — a global, controls-based assurance scheme that confirms an organization has implemented documented governance, risk management and technical control mechanisms for its AI Systems across thirteen mandatory Domains.

The Trust AI Academy is the official training and certification pathway for individuals seeking knowledge, implementation expertise, governance capability and assessor competence under the Trust AI Certification Scheme. All Trust AI Academy qualifications are issued under the authority of Trust AI Standards and are delivered exclusively by authorized Training Partners and Certification Bodies.

> *Trust AI Standards is the independent authority behind the world's first dedicated, controls-based AI certification scheme — accessible, proportionate and aligned to international AI assurance norms.*

2. Program Overview

The Trust AI Governance Practitioner (TAIGP) is the foundational qualification of the Trust AI Academy. It provides candidates with the awareness, vocabulary and conceptual framework required to engage credibly with AI governance, risk management and the Trust AI Certification Scheme.

TAIGP is an open-entry, two-day, instructor-led program. It is designed for non-specialists and specialists alike who need to understand how the Trust AI Standard structures AI governance, risk classification, Domain controls, and certification, and how to contribute effectively to AI governance activities within their own organizations.

On successful completion of the multiple-choice examination, candidates are awarded the Trust AI Governance Practitioner (TAIGP) designation, valid for three years.

3. Course Purpose and Learning Outcomes

3.1 Purpose

The TAIGP qualification confirms that the holder has demonstrated awareness and understanding of the Trust AI Standard, the 13 Domains, the Risk Tier model, the Provider and Deployer role classifications, the principles of the Trust AI Certification Scheme, the foundations of AI governance as a discipline, and the ethical, security and risk content AI governance must navigate.

3.2 Program-Level Learning Outcomes

On successful completion of the TAIGP program, candidates will be able to:

- Define Artificial Intelligence, describe its origin, evolution and core capabilities, and differentiate the main AI classifications — narrow, general, generative and autonomous.

- Describe the international responsible AI principles landscape and position the Trust AI Standard within it.
- Explain the purpose, structure, scope and authoritative status of the Trust AI Standard v1.5 (Polaris).
- Identify the five Risk Tiers and apply the six-dimension Tier 0 to Tier 4 classification model at an introductory level.
- Distinguish between Provider and Deployer organizational roles (and the Dual classification) and the associated obligations.
- Describe the purpose of each of the thirteen mandatory Domains and identify their cross-Domain dependencies.
- Recognize the Automatic Failure conditions and the Major Non-Compliance framework under Section 7 of the Standard.
- Explain the Trust AI Certification Scheme — Trust AI Essentials and Trust AI Essentials Plus — and the four-phase engagement journey.
- Describe the four-layer AI governance operating model and the five-stage governance maturity model.
- Recognize the four foundational ethical principles applied to AI, the three classical ethics frameworks, and the four core ethical tradeoffs.
- Recognize the five common AI and machine learning adversarial threats and the AI risk lifecycle.
- Recognize common AI governance failure patterns and the evidence artefacts that demonstrate strong governance.
- Engage credibly in AI governance, risk, compliance, ethics and assurance discussions within an organizational context.

3.3 Module-Level Learning Outcomes

The TAIGP program is delivered across fourteen modules over two days. Each module has specific awareness-level learning outcomes. The full module map is set out below — Day One covers the foundations of AI and the Trust AI Standard; Day Two covers the remaining Domains, fundamentals of governance, ethics and security, applied case studies and the examination.

Day One — Foundations and the Trust AI Standard

Module 1 — Introduction to AI, Opportunities and Risks

- Define Artificial Intelligence and describe its origin, evolution and four defining characteristics (autonomy, adaptiveness, inference, output that influences environments).
- Differentiate between narrow, general, generative and autonomous AI Systems.
- Explain core AI capabilities — pattern recognition, prediction, generation, optimization, reasoning.

- Compare Machine Learning, Deep Learning and Natural Language Processing in simple, practical terms.
- Evaluate the impact of AI on business, government and society and recognise the eight AI risk categories.
- Recognize why AI Governance is essential for managing risk, building trust and ensuring accountability.

Module 2 — Responsible AI Principles

- Describe the international responsible AI principles landscape (OECD AI Principles, NIST AI RMF, ISO/IEC 42001, EU AI Act, UAE AI Charter and equivalents).
- Identify the common themes — accountability, fairness, transparency, human oversight, privacy, robustness/security/safety.
- Describe the seven Trust AI Design Principles (Proportionate, Controls-based, Role-aware, Risk-tier driven, Internationally aligned, Accountability-anchored, Evidence-driven).
- Position the Trust AI Standard within the global responsible AI principles landscape.

Module 3 — Trust AI Standard v1.5 (Polaris) Overview

- Describe the purpose, scope, structure and authoritative status of the Trust AI Standard v1.5 (Polaris).
- Explain the organizational role classifications — Provider, Deployer and Dual roles.
- Identify the thirteen mandatory Domains and their architectural relationships across three clusters.
- Define the certification scope and the in-scope AI System concept.
- Distinguish the Trust AI Standard from management-system certifications and explain how it complements them.

Module 4 — Trust AI Risk Tier Model

- Identify the five Risk Tiers — Tier 0 (Prohibited) through Tier 4 (Critical Risk).
- Apply the highest-dimension rule and the higher-tier-prevails principle.
- Score AI Systems against the six risk dimensions — Fundamental Rights, Safety, Privacy, Fairness, Security, Oversight.
- Recognize Tier 4 escalation triggers and the mandatory Trust AI Essentials Plus requirement for Tier 4 systems.
- Apply the Tier model at an introductory level to classify realistic AI System scenarios.

Module 5 — Trust AI Certification Scheme

- Distinguish between Trust AI Essentials and Trust AI Essentials Plus.
- Describe the four phases of a Trust AI engagement — Scoping, Implementation, Assessment, Ongoing Conformity.

- Apply the Section 7.5 and 7.6 certification decision rules — zero AFs, up to two NCs subject to corrective action, plus independent validation for Plus.
- Distinguish Automatic Failures, Major Non-Compliances, Observations and Opportunities for Improvement under Section 7.
- Recognize twelve-month certificate validity, annual reassessment, the duty-to-notify on material change, and the operational role of the Trust AI Certification Rules and Assessment Policy.

Module 6 — Overview of Domains 1 to 7

- Describe the purpose of Domains 1 through 7 at an awareness level.
- Identify the key controls and Automatic Failures within each Domain — approximately 19 AFs across Domains 1 to 7.
- Recognize the cross-Domain dependencies and how each Domain reinforces the others.
- Identify common evidence artefacts associated with each Domain.

Module 7 — Day One Knowledge Check and Workshop

- Demonstrate awareness-level command of Day One content through a cumulative 10-question knowledge check spanning Modules 1 to 6.
- Apply Day One learning to a realistic AI System scoping scenario through a facilitated workshop.
- Identify gaps in candidates' own organizational AI governance posture using the Gap Identification Worksheet.

Day Two — Day 2 Domains, Fundamentals, Applied Practice and Examination

Module 8 — Overview of Domains 8 to 13

- Describe the purpose of Domains 8 through 13 at an awareness level.
- Identify the key controls and Automatic Failure conditions concentrated in Domain 8 (Oversight) and Domain 9 (Security).
- Recognize worked-example patterns from real cases — including the meaningful oversight analogue, public AI endpoint exposure, model drift, foundation model provider outage, hallucination incidents, and the convergence resilience test.
- Identify Practitioner deliverables and evidence artefacts across the technical assurance cluster.

Module 9 — AI Governance Fundamentals

- Describe what makes AI governance a distinct discipline from corporate, IT and data governance.
- Recognize why AI governance is inherently cross-functional — the eight functions typically engaged.
- Explain the four-layer governance operating model — Accountable Person, AI Governance Forum, Decisions, Evidence.

- Recognize the five governance maturity stages — Nascent, Emerging, Developing, Established, Optimizing.
- Identify common AI governance failure patterns — paper governance, shadow AI, Forum without authority, Forum without competence, delegated-only accountability, one-and-done compliance.

Module 10 — AI Ethics Fundamentals

- Distinguish AI ethics from AI governance and from general ethics.
- Describe the four foundational ethical principles applied to AI — autonomy, beneficence, non-maleficence, justice (with sub-types distributive, procedural, recognition).
- Recognize the three classical ethics frameworks — deontological, consequentialist, virtue.
- Identify the four core ethical tradeoffs that AI governance regularly navigates — fairness vs accuracy, transparency vs security, privacy vs utility, individual vs collective benefit.
- Explain how AI ethics maps to the Trust AI Standard's controls and apply the Practitioner action pattern (recognise, surface, document, engage).

Module 11 — AI Security and Risk Fundamentals

- Describe what makes AI security a distinct discipline from general IT security.
- Recognize the five common AI and machine learning adversarial threats — prompt injection, data poisoning, model extraction, adversarial examples, membership inference.
- Describe what makes AI risk distinct from general enterprise risk — drift, fairness, opacity, supply chain dimensions.
- Apply the six AI risk dimensions and the four-stage AI risk lifecycle (identify, assess, treat, monitor).
- Apply the Practitioner action pattern at awareness level — recognise, surface, escalate, partner.

Module 12 — Trust AI in Practice

- Describe the four phases of a Trust AI engagement journey (Scoping, Implementation, Assessment, Ongoing Conformity).
- Recognize what the evidence pack consists of across the thirteen Domains in six categories.
- Describe the Certification Body relationship and what to expect across the four phases.
- Recognize common implementation patterns and the integrated Practitioner role across the journey.

Module 13 — Case Studies and Workshop

- Apply the six-dimension Tier classification methodology to four worked cases across sectors — healthcare radiology backlog prioritization, financial services credit scoring, retail GenAI customer service chatbot, public sector benefit eligibility.
- Identify Provider, Deployer and Dual role classifications in each case.

- Recognize the primary Standard controls engaged and the Practitioner action priorities for each case.
- Apply the four-step method (describe, score, identify role, map) to any AI System encountered in practice.

Module 14 — Examination and Close

- Demonstrate awareness-level command of the Trust AI Standard through the formal multiple-choice examination.
- Achieve the 70 percent pass mark across forty multiple-choice questions in sixty minutes.
- On successful completion, qualify for the Trust AI Governance Practitioner (TAIGP) designation.

4. Target Audience and Suitable Roles

TAIGP is suitable for any professional seeking foundational knowledge of AI governance under the Trust AI Standard. It is particularly relevant for the following audiences:

- Business leaders and senior managers responsible for AI investment, oversight or accountability
- Risk, compliance, legal and privacy professionals adding AI to their existing remit
- Information security and technology managers with AI Systems in their portfolio
- Consultants entering the AI governance, AI risk and AI assurance market
- Internal AI champions, program managers and product owners
- Internal auditors preparing to audit AI Systems and governance controls
- Students and graduates seeking a recognised foundational AI governance credential
- Public-sector officials, policy professionals and regulators studying AI assurance frameworks

4.1 Typical Job Roles

On successful completion, candidates are typically positioned for roles such as:

- AI Governance Coordinator
- AI Risk Analyst
- AI Compliance Analyst
- AI Governance Champion
- Junior Consultant — AI Governance, Risk and Compliance
- Internal Audit Associate — AI Systems

5. Career Benefits

Holding the Trust AI Governance Practitioner (TAIGP) designation positions candidates for a growing range of AI governance, risk, compliance and assurance roles. As demand for trained AI governance professionals continues to expand across regulated sectors, public services and consultancy, TAIGP holders are well placed to support hands-on AI governance work and progress into more senior implementation and assessor roles.

Successful candidates may support roles such as:

- AI Governance Coordinator
- AI Risk Analyst
- AI Compliance Analyst
- Responsible AI Officer
- AI Assurance Associate
- Junior AI Governance Consultant

Holding the designation signals to employers, clients and regulators that the candidate has demonstrated awareness of the Trust AI Standard, the Risk Tier model, the 13 mandatory Domains, and the principles of the Trust AI Certification Scheme — a recognised foundation for further specialisation in AI governance, AI assurance and AI risk management.

6. Entry Requirements

TAIGP is an open-entry qualification. There are no mandatory prerequisites and no minimum experience requirement.

6.1 Recommended Familiarity

While not required, candidates may benefit from prior familiarity with:

- Basic concepts of artificial intelligence, machine learning or generative AI
- General governance, risk and compliance principles
- Information security, data protection or privacy frameworks

7. Duration, Delivery and Format

Element	Detail
Duration	Two days (typically 14 contact hours)
Delivery	Instructor-led classroom OR virtual live training
Group size	Typically 10 to 20 candidates per cohort
Language	English (other languages by arrangement with Training Partner)
Materials	Branded student workbooks per module, slide decks, knowledge checks, case-study briefs, glossary
Instructor	Trust AI Standards authorized trainer
Pre-reading	Trust AI Standard v1.5 high-level summary (provided)

8. Detailed Syllabus

The TAIGP syllabus is delivered across two days. Each day is structured into modules with instructor-led content, interactive workshops, knowledge checks and case study discussion. The full syllabus is summarised below.

8.1 Day One — Foundations and the Trust AI Standard

Module 1 — Introduction to AI, Opportunities and Risks

Sets the conceptual stage for the program.

- What is AI — the four defining characteristics; OECD/EU AI Act definition
- Origin and evolution of AI — Dartmouth 1956 through deep learning (2012), transformer (2017), GenAI era (2022+)
- Four AI classifications — narrow, general, generative, autonomous
- Core AI capabilities — pattern recognition, prediction, generation, optimization, reasoning
- ML, DL and NLP — relationships and distinctions
- AI in practice — Build/Buy/Embed/Augment sourcing patterns; common system categories
- AI opportunities — efficiency, scale, insight, personalisation, innovation
- Eight AI risk categories — bias, privacy, opacity, misuse, hallucination, security, concentration, skill loss
- Why AI governance is essential — case for proportionate, controls-based assurance

Module 2 — Responsible AI Principles

- International landscape — OECD AI Principles, NIST AI RMF, ISO/IEC 42001, EU AI Act, UAE AI Charter, Council of Europe AI Convention
- Common themes — accountability, fairness, transparency, human oversight, privacy, robustness/security/safety
- The seven Trust AI Design Principles — Proportionate, Controls-based, Role-aware, Risk-tier driven, Internationally aligned, Accountability-anchored, Evidence-driven
- How responsible AI principles translate into operational controls
- Position of the Trust AI Standard within the global landscape

Module 3 — Trust AI Standard v1.5 (Polaris) Overview

- Purpose, scope and authoritative status of the Standard
- Structure — nine Sections; thirteen mandatory Domains; controls in Dn-n.x format
- Organizational Role Classification — Provider, Deployer and Dual roles
- AI System scope and certification scope definition; the in-scope AI System concept

- How Trust AI complements ISO/IEC 27001, ISO/IEC 42001, SOC 2 and EU AI Act conformity assessment

Module 4 — Trust AI Risk Tier Model

- Tier 0 — Prohibited (assessment terminated)
- Tier 1 — Minimal Risk (eligible)
- Tier 2 — Limited Risk (eligible)
- Tier 3 — High Risk (eligible with enhanced requirements)
- Tier 4 — Critical Risk (eligible with mandatory Essentials Plus validation)
- Six risk dimensions — Fundamental Rights, Safety, Privacy, Fairness, Security, Oversight
- Highest-dimension rule, higher-tier-prevails principle, reassessment on material change
- Tier 4 escalation triggers; worked classification examples

Module 5 — Trust AI Certification Scheme

- Trust AI Essentials — baseline certification level
- Trust AI Essentials Plus — Essentials + independent validation activities (interviews, sampling, control testing, evidence triangulation)
- Four phases of a Trust AI engagement — Scoping, Implementation, Assessment, Ongoing Conformity
- Section 7 decision rules — 7.4 Automatic Failures, 7.5 Essentials rule, 7.6 Plus rule, 7.7 Observations and OFIs
- Findings hierarchy — AF, Non-Compliance, Observation, OFI
- Section 8 ongoing conformity — 12-month validity, ongoing conformity obligation on the organisation, material change duty-to-notify, annual reassessment
- Operational role of the Trust AI Certification Rules and Assessment Policy

Module 6 — Overview of Domains 1 to 7

Each Domain introduced with purpose, key controls, Automatic Failures and typical evidence artefacts.

- Domain 1 — AI Governance, Ethics and Accountability (4 AFs)
- Domain 2 — AI System Inventory and Risk Classification (3 AFs)
- Domain 3 — AI Risk Assessment and Impact Evaluation (4 AFs)
- Domain 4 — Legal, Regulatory and Contractual Compliance (2 AFs)
- Domain 5 — Data Governance and Privacy Protection (3 AFs)
- Domain 6 — Fairness and Bias Mitigation (1 dual-trigger AF)
- Domain 7 — Transparency, Explainability and Disclosure (2 AFs)
- Cross-Domain dependencies and common evidence artefacts

Module 7 — Day One Knowledge Check and Workshop

- Cumulative knowledge check — 10 multiple-choice questions spanning Modules 1 to 6
- Facilitated workshop — apply Day 1 learning to a realistic UK mid-sized fintech scoping scenario (ScaleUp Financial Ltd)
- Gap Identification Worksheet — applied to candidates' own organisation (take-home asset)
- Day 1 reflection and bridge to Day 2

8.2 Day Two — Day 2 Domains, Fundamentals and Applied Practice

Module 8 — Overview of Domains 8 to 13

Each Domain taught through discipline fundamentals, Standard controls, and a walked-through worked example.

- Domain 8 — Human Oversight and Intervention (3 AFs; meaningful oversight, automation bias, intervention authority)
- Domain 9 — Security and Technical Safeguards (5 AFs; OWASP LLM Top 10; public endpoint exposure pattern)
- Domain 10 — Robustness, Validation and Performance Monitoring (data drift vs concept drift; COVID-era model drift)
- Domain 11 — AI Supply Chain and Third-Party Dependencies (Foundation Model Provider Outage Pattern)
- Domain 12 — AI Incident Management and Harm Response (AI-specific incident types; Air Canada chatbot precedent)
- Domain 13 — Operational Resilience and Continuity (fallback patterns; convergence resilience test)
- Cross-Domain dependencies that bind Day 2 Domains to Day 1 Domains

Module 9 — AI Governance Fundamentals

AI governance as a distinct discipline (awareness level; implementation depth deferred to TAIGPro).

- What AI governance is — distinct from corporate, IT and data governance
- Why AI governance is inherently cross-functional — eight functions typically engaged
- The four-layer governance operating model — Accountable Person, AI Governance Forum, Decisions, Evidence
- Five governance maturity stages — Nascent, Emerging, Developing, Established, Optimising
- Six common AI governance failure patterns — paper governance, shadow AI, Forum without authority, Forum without competence, delegated-only accountability, one-and-done compliance

Module 10 — AI Ethics Fundamentals

- What AI ethics is — distinct from AI governance and from general ethics
- Four conditions that make AI ethically distinct — scale, speed, opacity, power asymmetry
- Four foundational ethical principles — autonomy, beneficence, non-maleficence, justice (with sub-types distributive, procedural, recognition)
- Three classical ethics frameworks at high level — deontological (Kant), consequentialist (Mill), virtue (Aristotle)
- Four core ethical tradeoffs with worked examples — fairness vs accuracy (Amazon recruitment AI), transparency vs security, privacy vs utility (Italian DPA / ChatGPT example), individual vs collective benefit
- How AI ethics maps to the Trust AI Standard's controls; Practitioner action pattern — recognise, surface, document, engage

Module 11 — AI Security and Risk Fundamentals

- What AI security is — distinct from general IT security
- Five common AI and machine learning adversarial threats — prompt injection (OWASP LLM Top 10 #1), data poisoning, model extraction, adversarial examples, membership inference
- Security worked example — Microsoft Tay 2016 and the pattern that recurs
- What AI risk is — distinct from general enterprise risk (drift, fairness, opacity, supply chain dimensions)
- Six AI risk dimensions and the four-stage AI risk lifecycle (identify, assess, treat, monitor)
- Risk worked example — foundation model dependency case applying the lifecycle
- Practitioner action pattern at awareness level — recognise, surface, escalate, partner (with CISO on D9; Risk function on D3)

Module 12 — Trust AI in Practice

Integration module — brings Day 1 and Day 2 together.

- Four phases of a Trust AI engagement journey — Scoping (1-2 months), Implementation (3-12 months varying by size/scope), Assessment (4-12 weeks), Ongoing Conformity (continuous, 12-month cycles)
- The evidence pack across the 13 Domains — six categories from governance to operational
- Working with Certification Bodies — what to expect across the four phases
- Common implementation patterns and challenges — shadow AI late, Accountable Person stalling, Risk Appetite Statement skipped, Tier-specific controls missed, AI literacy assumed, evidence pack at end
- The integrated Practitioner role across the engagement — recognise, surface, partner, orchestrate
- Bringing the 13 Domains into a coherent posture

Module 13 — Case Studies and Workshop

Four worked cases across sectors. Per case: setup, four-step method (describe, score six dimensions, identify role, map to Standard), debrief.

- Case 1 — Healthcare: AI prioritisation of radiology backlog (Tier 3/4 boundary; teaches the boundary debate)
- Case 2 — Financial Services: credit scoring AI for personal loans (Tier 3; teaches fairness assessment, lawful basis)
- Case 3 — Retail: GenAI customer service chatbot (Tier 2; teaches Air Canada precedent, hallucination as foreseeable incident)
- Case 4 — Public Sector: benefit eligibility AI at population scale (Tier 4 via population-scale + consequential impact + fairness exposure)
- Cross-case patterns and the integrated Practitioner role

Module 14 — Examination and Close

- Recap and final Q&A
- Examination briefing — format, rules, five practical strategies
- Multiple-choice examination — 40 questions, ~60 minutes, closed book
- Programme close — TAIGP designation, recertification and CPD requirements, TAIGPro pathway, full Trust AI Academy progression
- Provisional result on completion; formal designation issued within 5 working days

9. Practical Components

The TAIGP program is designed to be interactive and applied, not lecture-only. Throughout the two days candidates will participate in:

- Module-level knowledge checks — used for formative assessment; cumulative coverage across the program
- Module 7 Day One Knowledge Check Workshop — 10-question cumulative check and applied scoping scenario (Scaleup Financial Ltd)
- Module 13 Case Studies Workshop —worked cases across healthcare, financial services, retail and public sector
- Gap Identification Worksheet — Module 7 take-home asset applied to candidates' own organizations
- Domain pattern-recognition exercises — recognizing common failure modes
- Group discussion — applying the Standard to candidates' own organizational contexts

10. Examination

Element	Detail
Format	Multiple-choice examination (4 options per question)
Number of questions	60 questions
Duration	Approximately 60 minutes
Pass mark	70 % (42 of 60 correct)
Invigilation	In-person or live online proctoring
Coverage	Training modules 1 through 13 — distribution proportional to module weight.
Question style	Recognition, application and Practitioner-judgement scenarios (not pure recall)
Re-sit policy	One free re-sit within 30 days of first attempt; further attempts at standard fee
Result	Provisional result on completion; formal designation issued within 5 working days

10.1 Examination Blueprint (indicative)

Topic area	Weight	Questions
AI fundamentals (Module 1)	7.5 %	3
Responsible AI principles + Trust AI design principles (Module 2)	7.5 %	3
Trust AI Standard structure, Provider/Deployer roles, scope (Module 3)	10 %	4
Risk Tier model and classification (Module 4)	12.5 %	5
Certification Scheme — decision rules, material change, level selection (Module 5)	10 %	4
Domains 1 to 7 — applied (Module 6)	12.5 %	5
Domains 8 to 13 — applied (Module 8)	12.5 %	5
Governance fundamentals (Module 9)	7.5 %	3
Ethics fundamentals (Module 10)	7.5 %	3
Security and risk fundamentals (Module 11)	7.5 %	3
Trust AI in Practice — integration (Module 12)	5 %	2

11. Certification and Validity

Element	Detail
Designation awarded	Trust AI Governance Practitioner (TAIGP)
Issued by	Trust AI Standards
Validity	Three years from date of award — reflecting the pace of change in AI governance, regulation and standards
Digital credential	Verifiable digital badge and certificate
Use of designation	Holders may use 'TAIGP' after their name during validity period
Recertification	Structured CPD evidence + light-touch reassessment (short online assessment covering significant changes to the Standard and the AI governance landscape) OR repeat the full TAIGP examination

11.1 Professional Recognition

Holders of the Trust AI Governance Practitioner qualification are formally recognised by Trust AI Standards as having demonstrated awareness and understanding of AI governance under the Trust AI Standard v1.5.

During the three-year validity period, holders may:

- Use the post-nominal designation TAIGP after their name (for example: Jane Smith, TAIGP)
- State 'Trust AI Governance Practitioner (TAIGP) — issued by Trust AI Standards' on professional profiles, CVs and email signatures
- Display the verifiable digital badge issued by Trust AI Standards
- Reference the qualification in proposals, tenders and procurement responses where AI governance capability is required

The TAIGP designation is recognised globally under the Trust AI Certification Scheme and is acceptable as evidence of foundational AI governance literacy for hiring, procurement and contractual purposes.

12. Continuing Professional Development (CPD)

CPD is mandatory for TAIGP holders during the three-year validity period.

Element	Detail
CPD requirement	Minimum 30 hours of relevant AI governance CPD over the 3-year validity period (10 hours per year)
Benchmarking	Calibrated against comparable professional bodies (ISACA, ISC2, IAPP, ISO certification bodies)

Element	Detail
Recertification options	Path 1: structured CPD evidence + light-touch reassessment (short online assessment covering significant changes to the Standard and the AI governance landscape) | Path 2: repeat the full TAIGP examination
CPD logging	Through the Trust AI Standards practitioner register

12.1 Recommended CPD activities

- Trust AI Standards events — quarterly Practitioner Forums and annual Trust AI Standards conference
- Reading the OWASP Top 10 for Large Language Model Applications quarterly
- Tracking regulatory updates — EU AI Act implementation, UK AI Regulation guidance, sector-specific developments
- Established AI governance and ethics references — OECD AI Observatory, NIST AI publications, ISO/IEC standards, ENISA, ICO and NCSC guidance, IAPP and ISACA AI tracks
- Applied practice — applying the TAIGP framework in candidates' own organizations or client engagements (documented as CPD)
- Progression to Trust AI Governance Professional (TAIGPro) Level 2

13. Fees and Registration

Element	Detail
Standard fee	USD 595 per candidate
Inclusions	Training, course materials, examination, one free re-sit, digital credential
Group / corporate	Discounts available for cohorts of 10+ candidates — contact Training Partner
Currency	USD and AED pricing set by local authorized Training Partner
Registration	Through any authorized Trust AI Standards Training Partner or Certification Body

14. Progression Pathway

TAIGP is the foundational qualification of the Trust AI Academy. The full progression pathway is:

14.1 Trust AI Academy Learning Path

Level	Qualification	Duration	Validity
Level 1	Trust AI Governance Practitioner (TAIGP)	2 days	3 years
Level 2	Trust AI Governance Professional (TAIGPro)	5 days	3 years
Level 3	Trust AI Essentials Assessor (TAIEA)	5 days	3 years
Level 4	Trust AI Essentials Plus Assessor (TAIEPA)	5 days	3 years

14.2 Why Progress to Trust AI Governance Professional?

Trust AI Governance Practitioner (TAIGP) teaches awareness and understanding. Trust AI Governance Professional (TAIGPro) builds directly on that foundation and teaches the practical skills required to design, implement, operate, maintain and continually improve AI governance programmes aligned to the Trust AI Standard.

TAIGPro candidates learn how to build the governance, risk, compliance and operational artefacts an organisation must produce to achieve and sustain certification, including:

- Designing the AI Governance Forum — membership, mandate, Terms of Reference, cadence and escalation
- Decision register structure, RACI matrix design, delegation arrangements
- AI Governance Policy components and review cycle
- AI System inventories and Risk Tier classification across the portfolio
- AI risk assessment methodology, Risk Register design and Risk Appetite Statement
- AI impact evaluations and fairness risk and impact assessments
- Compliance Registers covering legal, regulatory and contractual obligations
- AI Supplier Registers, due diligence packs and contingency plans
- AI Incident Handling Policies, Incident Registers and Root Cause Analysis frameworks
- Operational Resilience and Continuity plans including table-top exercise design
- Ethical Impact Assessment templates and structured deliberation methods
- AI security control framework partnered with the CISO function
- Evidence packs ready for Trust AI Essentials and Essentials Plus assessment
- AI governance KPIs and the 90-day implementation playbook

TAIGPro is a five-day, instructor-led program. Entry is via either TAIGP or an equivalent recognised qualification (such as AIGP, CISM, CRISC, CGEIT, CISSP, CGRC, ISO/IEC 42001 Lead Implementer or ISO/IEC

27001 Lead Implementer). Progress when your role requires implementation capability — some practitioners are ready immediately, others develop into the role over time.

> *TAIGP teaches you to understand AI governance. TAIGPro teaches you to operate it.*

15. Why Trust AI Standards

The Trust AI Standard and the Trust AI Academy were created to address three fundamental gaps in the AI assurance market:

15.1 Proportionate

Trust AI is calibrated to AI System Risk Tier and organizational role. A Tier 1 deployment of a marketing copilot does not face the same controls as a Tier 4 clinical decision-support system. The Standard's proportionality principle makes certification accessible to organizations of every size and sector.

15.2 Controls-Based

Unlike principles-based frameworks, the Trust AI Standard prescribes specific controls organized across thirteen Domains, with clear Automatic Failure conditions and Major Non-Compliance triggers. This produces an unambiguous certification scheme and a defensible assurance posture.

15.3 Internationally Aligned

The Trust AI Standard interoperates with — and is informed by — the EU AI Act, OECD AI Principles, UAE AI Charter, NIST AI Risk Management Framework and ISO/IEC 42001. It is not a management-system certification; it complements ISO/IEC 42001 and other governance standards rather than replacing them.

16. About the Trust AI Standard v1.5

The Trust AI Standard v1.5 ('Polaris') is the authoritative reference of the Trust AI Certification Scheme. It is issued by the Trust AI Standards Advisory Council and maintained by Trust AI Standards FZC-LLC. The Standard is structured around:

- Thirteen mandatory Domains, each with explicit controls
- Five Risk Tiers (Tier 0 to Tier 4)
- Provider, Deployer and Dual role classifications
- Explicit Automatic Failure conditions
- Major Non-Compliance triggers and certification decision rules
- Twelve-month certificate validity with annual reassessment

TAIGP candidates receive a high-level overview of the Standard at the awareness level. The Trust AI Governance Professional (TAIGPro) qualification provides detailed implementation expertise.

17. How to Register

TAIGP is delivered exclusively by authorized Trust AI Standards Training Partners and Certification Bodies. To register:

1. Identify an authorized Trust AI Standards Training Partner serving your region.
2. Confirm cohort dates, delivery mode (classroom or virtual) and pricing.
3. Complete registration through us or through our Training Partner.
4. Receive joining instructions, pre-reading and access to the candidate portal.
5. Attend the two-day program and sit the examination on day two.

17.1 Contact

For enquiries about TAIGP, Trust AI Academy qualifications or the Trust AI Certification Scheme, contact us at info@trustaistandards.com. You can also reach out to our authorized Training Partner or visit the Trust AI Standards website.

18. Document Control

Document	Trust AI Governance Practitioner (TAIGP) — Course Prospectus
Issued by	Trust AI Standards
Aligned to	Trust AI Standard v1.5 (Polaris), Doc ID TAI-STD-1.5
Version	v1.3
Year	2026
Approval Date	06 June 2026
Change summary	v1.3 — aligned to final modules as built: Modules 5/9/10/11/12/13 syllabus refreshed; CPD made mandatory at 30 hours over 3 years; light-touch reassessment defined; examination blueprint updated to reflect actual question distribution; Module-Level Outcomes refreshed throughout.
Classification	Public