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 Governance Practitioner (TAIGP) — Course Prospectus
Document Version: v1.4
Approved By Trust AI Standards
Approval Date: 06 June 2026

1. About Trust AI Standards

Trust AI Standards is an independent AI Governance Standards Body and the owner of the Trust AI Certification Scheme. Trust AI Standards develops, maintains and licenses the Trust AI Certification Scheme, a global, controls-based assurance scheme that enables organizations to demonstrate the effective governance, risk management and control of Artificial Intelligence systems across thirteen mandatory Domains.

Trust AI Standards also develops and maintains the Trust AI qualification and assessor pathways, providing structured learning, implementation and assurance certifications for individuals seeking knowledge, governance capability, implementation expertise and assessor competence under the Trust AI Certification Scheme. Training and certifications are issued by Trust AI Standards and delivered through authorized Training Partners and Licensed Certification Bodies.

Trust AI Standards provides an accessible, proportionate and internationally aligned framework for AI governance and assurance, supporting organizations in demonstrating trustworthy, responsible, secure and compliant use of Artificial Intelligence.

2. TAIGP Program Overview

Trust AI Governance Practitioner (TAIGP) is a foundational AI governance qualification that equips professionals with the knowledge, awareness and practical understanding required to participate effectively in AI governance, risk management, ethics, compliance and assurance activities. The qualification enables candidates to recognize, understand and support the responsible, secure and trustworthy use of Artificial Intelligence through the application of the Trust AI Standard.

TAIGP is an open-entry, two-day, instructor-led program designed for both non-specialists and specialists who need to understand how the Trust AI Standard structures AI governance, risk classification, requirements and the thirteen governance Domains. The program provides candidates with the skills and vocabulary required to engage credibly with AI governance initiatives and contribute effectively to AI governance activities within their own organizations.

Upon successful completion of the multiple-choice examination, candidates are awarded the Trust AI Governance Practitioner (TAIGP) designation, which is valid for three years and serves as the foundation for progression to advanced implementation, assurance and assessor qualifications within the Trust AI certification pathway.

3. Course Purpose and Learning Outcomes

3.1 Purpose

The purpose of the Trust AI Governance Practitioner qualification is to establish a common foundation of AI governance knowledge and provide candidates with the awareness, vocabulary, concepts and practical

understanding necessary to support the trustworthy, responsible, secure and compliant use of AI systems. Specifically, TAIGP enables candidates to:

- **Understand AI Governance**

  Understand why AI governance is necessary and how organizations can govern AI systems responsibly throughout their lifecycle.

- **Understand AI Risks**

  Recognize AI-related risks including fairness, transparency, privacy, security, safety, accountability and human oversight challenges.

- **Understand the Trust AI Standard**

  Understand the structure, purpose and application of the Trust AI Standard, including the 13 Domains, Trust AI Risk Tier Model and Certification Scheme.

- **Support AI Governance Programmes**

  Participate effectively in AI governance forums, risk assessments, compliance activities, assurance reviews and AI-related projects.

- **Prepare for Advanced Roles**

  Provide the foundation for progression into implementation, assurance and assessor pathways including:

  - Trust AI Governance Professional (TAIGPro)
  - Trust AI Essentials Assessor (TAIEA)
  - Trust AI Essentials Plus Assessor (TAIEPA)

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, AI Governance and the Trust AI Standard; Day Two covers the Trust AI Standard Domains, 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 — Trust AI Principles

- Describe the international trust and 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 — 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 4 — 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 (recognize, surface, document, engage).

Module 5 — 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).

Module 6 — 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 7 — 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 8 — 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 9 — 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 10 — 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.

Module 11 — 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 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 recognized 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 demonstrates foundational knowledge of AI governance, AI risk management, AI assurance and responsible AI practices. As organizations increasingly adopt Artificial Intelligence and seek to strengthen governance, compliance and assurance arrangements, TAIGP provides a strong foundation for professionals wishing to develop expertise in AI governance and related disciplines.

The qualification is suitable for individuals seeking to contribute to AI governance initiatives and may support progression towards roles such as:

- AI Governance Coordinator
- AI Risk Analyst
- AI Compliance Analyst
- AI Assurance Associate
- AI Governance Consultant
- Governance, Risk and Compliance (GRC) Professional
- Information Security and Risk Professional
- Technology Governance Professional

Holding the TAIGP designation signals to employers and clients that the candidate has demonstrated an understanding of AI governance principles, AI risk management concepts, the Trust AI Risk Tier Model, the thirteen Trust AI Domains and the Trust AI Certification Scheme.

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 14-16 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. 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 and formative assessments.
- Knowledge Check Workshop comprising a cumulative ten question review and applied scoping scenario.
- Case Studies Workshop covering healthcare, financial services, retail and public sector environments.
- Risk Tier classification and Provider/Deployer role classification exercises.
- Domain pattern recognition exercises focused on common governance and control weaknesses.
- Group discussions applying the Trust AI Standard to real world organizational contexts.

These practical activities are designed to reinforce learning and help candidates apply Trust AI concepts confidently in practice.

9. Examination

Element	Detail
Format	Multiple-choice examination (3 to 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

9.1 Examination Blueprint (indicative)

Topic Area	Weight	Questions
AI fundamentals (Module 1)	5 %	3
Trust AI principles (Module 2)	5 %	3
AI Governance fundamentals (Module 3)	10 %	6
Ethics fundamentals (Module 4)	10 %	6
AI Security and risk fundamentals (Module 5)	10 %	6
Trust AI Standard structure, Provider/Deployer roles, scope (Module 6)	10 %	6
Trust AI Risk Tier model (Module 7)	10 %	6
Trust AI Certification Scheme — decision rules, material change, level selection (Module 8)	10 %	6
Domains 1 to 7 — applied (Module 9)	10 %	6
Domains 8 to 13 — applied (Module 10)	10 %	6
Trust AI in Practice — integration (Module 12)	10 %	6
TOTAL	**100%**	**60**

10. 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

10.1 Professional Recognition

Holders of the Trust AI Governance Practitioner qualification are formally recognized 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 recognized globally under the Trust AI Certification Scheme and is acceptable as evidence of foundational AI governance literacy for hiring, procurement and contractual purposes.

11. 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)
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 portal

11.1 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

12. 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

13. Progression Pathway

TAIGP is the foundational individual level qualification in AI Governance. The full progression pathway is:

13.1 Learning Pathway

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

13.2 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 organization 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 recognized 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 how to operate it.*

14. Why Trust AI Standards?

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

14.1 Proportionate

The Trust AI Standard is calibrated to both AI System Risk Tier and organizational role. A Tier 1 marketing copilot should not be subject to the same governance requirements as a Tier 4 clinical decision support system. This proportionate approach makes certification practical, scalable and accessible for organizations of all sizes and sectors.

14.2 Controls-Based

Unlike principles-based frameworks, the Trust AI Standard defines specific, auditable controls across thirteen mandatory Domains. Clear assessment criteria, Automatic Failure conditions and Non-Compliance triggers provide a consistent, objective and defensible certification process.

14.3 Internationally Aligned

The Trust AI Standard is informed by and aligned with recognized international frameworks and guidance, including the EU AI Act, OECD AI Principles, UAE AI Charter, NIST AI Risk Management Framework and ISO/IEC 42001. The Standard complements existing AI governance and management system frameworks by providing a practical, controls-based certification and assurance mechanism.

15. About the Trust AI Standard

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.

16. How to Register

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

1. Contact Trust AI Standards or authorized 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.

For enquiries about TAIGP, Trust AI qualifications or the Trust AI Certification Scheme, contact us at info@trustaistandards.com.

17. 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	v1.4
Year	2026
Approval Date	06 June 2026
Change summary	v1.4 — 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