IAPP EUROPE CONGRESS 2026

Privacy | AI governance | Cybersecurity law

Training 16-17 November

Workshops 17 November

Conference 18-19 November

BRUSSELS

#IAPPCongress26

What is AI Assurance?

Navigating the Evolving AI Assurance Landscape

WELCOME AND INTRODUCTIONS



Lara Groves

Senior Researcher

Ada Lovelace Institute



Anahita Valakche

Senior Strategist of AI Policy in the Office of Responsible AI and European Government Affairs

Microsoft



Ashley Casovan

Managing Director, AI Governance Centre,

IAPP

AGENDA OUTLINE

I. Welcome and Introductions
II. Why AI Assurance?
III. What is AI Assurance?
IV. Who does AI Assurance?
V. How do I get started?
VI. Questions and Answers
VII. Closing Remarks

Why AI Assurance?

AI Assurance in the Headlines (September edition)

SB 813

Governor Newsom signs first-in-the-nation AI safeguards to protect Californians

Office of Gov. Gavin Newsom
Sept 9, 2026

CA EXECUTIVE ORDER

Newsom signs executive order to speed up AI regulations and creation of 'kill switch'

San Francisco Chronicle
Sept 19, 2026

PACING THE FRONTIER

Anthropic CEO calls for 'pacing the frontier' of AI race amid safety concerns

CNN
Sept 12, 2026

EMBEDDED EVALUATORS

Anthropic selects Accenture as first embedded evaluator to help implement Amodei's slowdown proposal

CNBC
Sept 18, 2026

WHITE HOUSE ACCORD

Trump releases self-regulatory accord for frontier AI models

MLex
Sept 2026

WHITE HOUSE ACCORD

Pledge signed by President Trump and top AI leaders misspells the United States

TechCrunch
Sept 30, 2026



PACT AI

Continuous, independent auditing is what makes responsible AI accountable and keeps it trustworthy

The rules are still being written.

Whoever is in the room while they are written shapes them, and once they are set, they are hard to change.

The systems are already deciding.

Algorithms are already deciding who gets hired, who gets a loan, who gets health care, who gets benefits.

Recognition is becoming law, but not yet practice.

The recognition is there. The profession to meet it is not.

The gap. AI auditing is fragmented. Shared standards, through the CAIA, turn that into a recognized, trusted profession.

Example. Illinois just passed the first US law requiring large frontier labs to undergo independent third-party AI audits of their safety practices every year. It says the auditors must be independent and qualified, but not what the audit should cover, how to do it, or who counts as qualified.

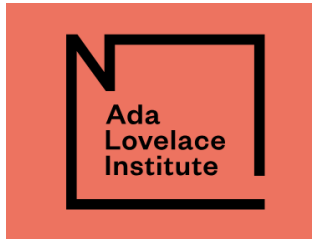


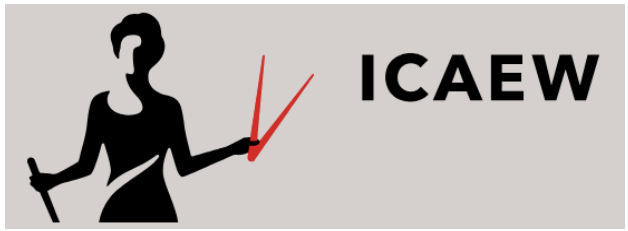






















International Network of AI Safety Institutes











AI Evaluator Forum



The Omidyar Group

AI Governance Vendor Directory

#IAPPCongress26

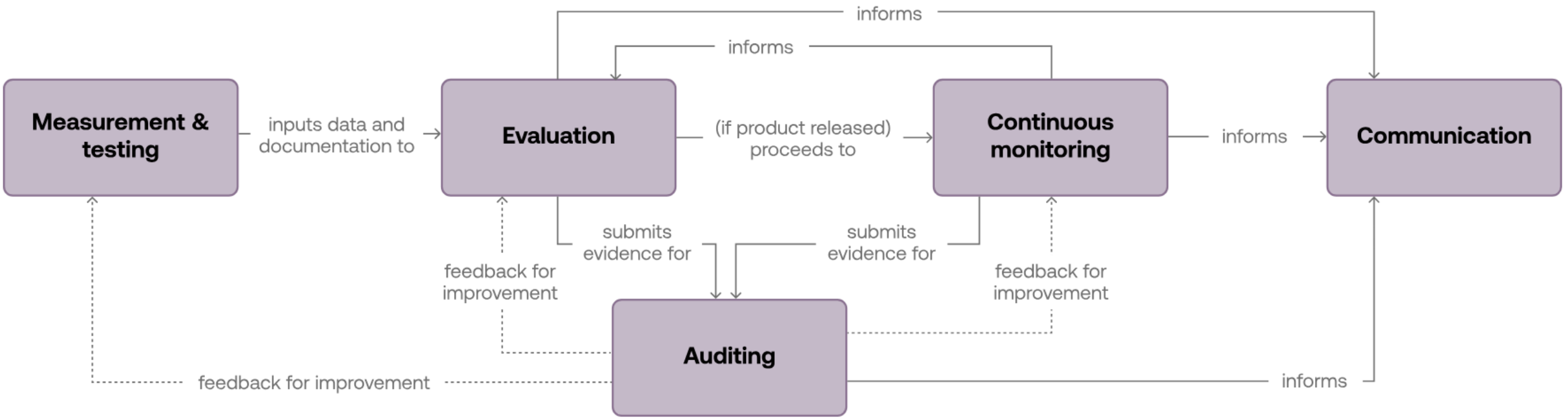
What is AI Assurance?

TECH & DIGITALISATION

AI-Assurance Ecosystems: Building the Infrastructure to Enable Confident Adoption of Safe AI

TONY BLAIR INSTITUTE FOR GLOBAL CHANGE

Core AI-assurance process activities



You already do assurance

Profession	What others rely on	Shared rules
Law	Closing opinion	Tribar Report
Audit	Financial statement opinion	Accounting and audit standards
Assurance	SOC 2 report	Trust Services Criteria
Privacy	Impact assessment	GDPR and regulator guidance
Compliance & governance	Control assessment	Control frameworks
Engineering	Acceptance testing	Test specs and acceptance criteria

Shared rules let others trust and reuse your judgment.

AI Assurance Categories (What)

Category	Focus	Example Risks/Harms Addressed	Cross-cutting
Internal deployment risk evaluations	Is the model safe for release to internal lab researchers?	● Alignment ● Loss-of-control ● Cybersecurity ● RSI	Governance Software Development Process
Pre-release catastrophic risk model evaluations	Is the model safe for release to external users?	● CBRN uplift ● Manipulation ● Reward structure (sycophancy, engagement)	
Post-release societally important harm model evaluations	Is the model safe for use by external users?	● Mental health ● Bias and fairness ● Misuse	
Use-case level commercial risk evaluations	Is the model safe for deployment to our employees and customers?	● Reliability ● Privacy and confidentiality	

Who does AI Assurance?

What implementation gaps is Appia meant to close?

Current gap

- High-level standards and regulations exist, but organizations still often recreate evidence pathways from scratch.
- Without shared evaluation methods and reusable evidence, implementation becomes duplicative, costly, and hard to rely on across the supply chain.
- Downstream actors often face shifting obligations even when much of the technical evidence already exists upstream.

Appia solution

- Translate high-level obligations into reusable requirements, evaluation methods, and evidence patterns.
- Adapt and integrate AI specific requirements and guidance into existing sector specific standards rather than building from the ground up.
- Define objects of conformity and modular pathways so different actors can assess only what is relevant to their role and context.
- Enable more consistent evidence handoffs across the supply chain instead of repeated re-documentation.

What this means for industry

- Appia can be described as implementation-oriented and modular, not as a monolithic specification “stack.”
- It is a shared infrastructure for assessable implementation and interoperable assurance.
- Most importantly, it allows for sector-specific rigor without forcing every domain into the same detailed implementation or assessment approach.

What are the emerging considerations for professionalising AI assurance?

Grounded qualitative research with practitioners in US and UK:

- AI assurance professionals need defined scope, required competencies and core practices
- Core skills: technical knowledge, legal fluency, risk management
- Certification and accreditation must standardise to raise the impact of AI assurance

Ada Lovelace Institute

CENTER FOR DEMOCRACY & TECHNOLOGY

What are the emerging considerations for professionalising AI assurance?

- Some assurance competencies will require specialised knowledge and experience
- Flexible, modular approach to skills and certification will create career development pathways
- Professionals need strong professional norms and ethical culture to complement formal standards and accountability structures

Ada Lovelace Institute

CENTER FOR DEMOCRACY & TECHNOLOGY

AI Assurance Categories

- An **investigator** establishes what happened after an incident. They reconstruct events and identify probable cause.
- An **evaluator** measures what the system does. Their work is empirical: tests, benchmarks, and red-teaming.
- An **assessor** appraises risk. An assessor asks whether something is good enough for a stated purpose.
- An **auditor** concludes. An audit is a systematic, independent examination against fixed criteria, ending in a conclusion on whether those criteria are met.

Primary questions: what were the criteria, who set them, what information will this give me, and who is the performer independent of?

AI assurance needs two layers

Certified professionals

Training to apply shared rules

Professional skepticism and independent judgment

Independent criteria

Developed by multiple stakeholders

Appia Foundation's public specifications

Four questions for every assessor

What am I assessing?
AI objects of conformity

Where does it belong in the AI value chain?
Shared responsibilities

What are the requirements?
Specs, standards, regulations, obligations

How do we know it meets requirements?
Evaluation criteria

THE ASSURANCE STACK

An ecosystem, not a single audit

Foundational science	Research, metrology, benchmarks, and standards
Direction and governance	Laws, regulatory guidance, and voluntary commitments
Operational assurance	Testing, audit, conformity assessment, and reporting
Oversight and meta-assurance	Accreditation, market surveillance, and monitoring

US touchpoints: NIST AI RMF, CAISI frontier evaluations, California SB 53, federal use case registers.

Felecia Webb, Chief Strategy Officer, Partnership on AI

Source: PAI (2026), Strengthening the AI Assurance Ecosystem, Figure 3

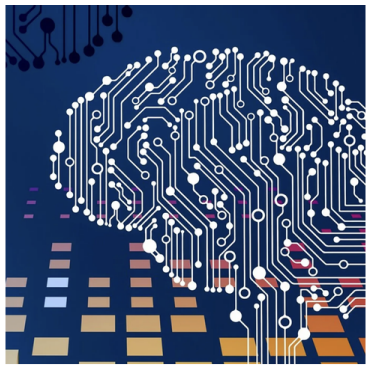
AI Governance Skills Framework (AIGSF)

TOOLS AND TRACKERS MEMBER

AI Governance Professional Profiles: Assurance

This resource maps out a standardized job template for assurance professionals working in AI governance.

Published
30 Sept. 2026



AI assurance lead

Alternative titles: AI governance auditor, AI compliance auditor, Responsible AI auditor, Internal auditor — AI governance.

Summary statement: Provides independent, nontechnical assurance over AI governance, risk management, compliance and organizational controls to ensure responsible and compliant use of AI.

Key purpose: Delivers objective assurance that AI governance frameworks, policies, processes and oversight mechanisms are effectively designed and operational.

- Deliverable(s), primary functions and subfunctions
- Main task(s)
- Key skill(s)
- Key knowledge

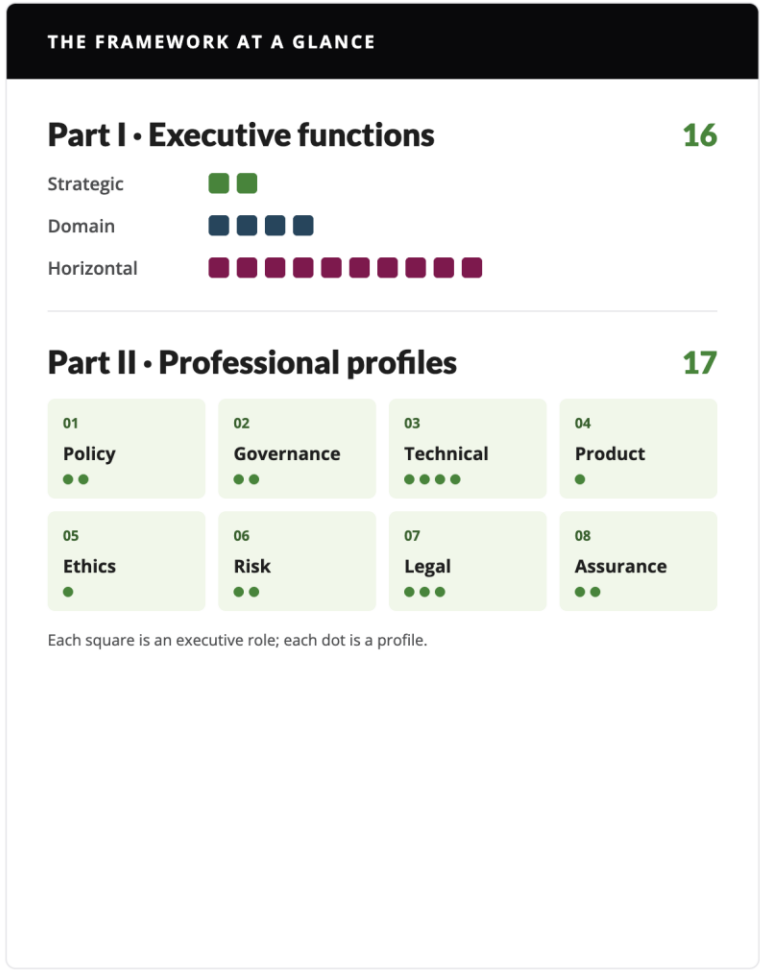
WHO IS AN AI GOVERNANCE PROFESSIONAL?

AI Governance Skills Framework

AIGSF

> A common language for the roles, tasks, skills and knowledge behind AI governance — because AI governance is a team sport.

OCTOBER 2026 DRAFT · NOT FOR DISTRIBUTION



PART I AI GOVERNANCE SKILLS FRAMEWORK

Executive functions

The leaders who hold oversight and ultimate accountability for AI governance. Each is involved when a decision touches their area of practice.

- Strategic
- Domain
- Horizontal

Strategic leaders

Set direction and tone for AI across the organization

CEO Chief executive officer

Aligns AI with mission, values and long-term goals; sets the tone for AI use, prioritizes responsible use and is the public face of AI adoption.

COO Chief operating officer

Embeds governance into AI processes, manages cross-functional coordination, and executes and enforces AI policies, monitoring and controls.

Domain leaders

Own AI governance within a business domain

CAIO

Chief AI officer

Leads enterprise AI strategy, implementation and risk management — the most prominent specialized AI governance role.

CHRO

Chief human resources officer

Oversees AI across the employee life cycle, high-risk HR use cases, fairness risks and AI literacy.

CMO

Chief marketing officer

Ensures ethical, transparent AI in customer engagement, personalization and public-facing campaigns.

CFO

Chief financial officer

Budgets AI investments, evaluates ROI and financial risk, and ensures financial compliance in AI procurement.

Horizontal leaders

Bring cross-cutting expertise that spans every AI use case

CPO / CDPO

Chief privacy / data protection officer

Privacy compliance, privacy risk assessments and privacy-by-design for AI.

CISO

Chief information security officer

Secures AI systems, data and model integrity; coordinates AI incident response.

CDO

Chief data officer

Data quality, lineage, bias risk and documentation for the data that fuels AI.

CCO

Chief compliance and ethics officer

Compliance policies, ethical AI principles, assessments and investigations.

CLO

Chief legal officer

Oversees the legal function, regulatory compliance and third-party relationships.

CIO / CTO

Chief information / technology officer

Integrates AI with enterprise architecture and IT governance; secures budget, talent and tools.

CPO

Chief product officer

Builds responsible AI into the product life cycle and manages product AI risk.

CRO

Chief risk officer

Integrates AI risk into enterprise risk management and reports exposure to leadership.

CPrO

Chief procurement officer

AI vendor due diligence, third-party risk and responsible AI contract clauses.

CRO / CSO

Chief revenue / sales officer

Accurate AI sales claims and responsible commercialization of AI.

Source: AI Governance Skills Framework (AIGSF), October 1, 2026 draft

NOT FOR DISTRIBUTION

PART II AI GOVERNANCE SKILLS FRAMEWORK

AI governance professional profiles

Eight categories of work and the 17 profiles that perform it. AI governance is a team sport: few organizations need every profile, and one role often covers two or more.

8 categories | **17** profiles

CATEGORY 01

Policy

Keeps AI governance aligned with the evolving external regulatory landscape.

- **AI policy lead**
  Shapes internal AI policy from external regulation
- **AI policy analyst**
  Policy research, regulatory tracking and briefings

CATEGORY 02

Governance

Runs the internal machinery that makes responsible AI use operational.

- **AI governance lead**
  Committees, inventories, frameworks and AI literacy
- **AI governance analyst**
  Use-case intake, documentation and committee prep

CATEGORY 03

Technical

Builds governance into AI infrastructure and makes requirements measurable.

- **Responsible AI engineering lead**
  Evaluation gates, monitoring and governance-ready architecture
- **AI safety engineer**
  Red teaming, threat detection and incident response
- **Responsible AI technician**
  Runs evaluations, monitoring and documentation
- **Responsible AI data scientist**
  Builds and assesses models for fairness and compliance

CATEGORY 04

Product

Owns the platforms and features that manage AI risk, compliance and life-cycle evaluation.

- **AI governance product lead**
  Use-case intake, governance roadmaps and build-vs.-buy tooling decisions

CATEGORY 05

Ethics

Evaluates the social and ethical implications of AI and weighs the trade-offs.

- **AI ethics officer**
  Ethics reviews, value-alignment reports and pre-deployment evaluations of risk to vulnerable groups

CATEGORY 06

Risk

Identifies, tracks and escalates AI risk — challenging assessments without owning remediation.

- **AI risk officer**
  Independent oversight and escalation of AI risk
- **AI risk manager**
  Risk registers, indicators, dashboards and mitigation

CATEGORY 07

Legal

Translates AI law into practical engineering and business controls.

- **AI legal**
  Owns legal's AI governance framework and operating model
- **Development and engineering legal**
  Product counsel across the development life cycle
- **Procurement legal**
  AI vendor due diligence and contract safeguards

CATEGORY 08

Assurance

Provides independent assurance that AI systems and governance work as designed.

- **Technical AI assurance lead**
  Audits AI systems, models and technical controls
- **AI assurance lead**
  Audits governance, policy and oversight processes

Source: AI Governance Skills Framework (AIGSF), October 1, 2026 draft

NOT FOR DISTRIBUTION

RESOURCE LIST

- IAPP - AI Governance Skills Framework
- Appia Foundation
- Partnership for Assurance, Credibility, and Trust in AI (PACT AI)
- Center for Democracy & Technology - Professionalizing AI Assurance
- Partnership on AI – Strengthening AI assurance ecosystem
- UK Government - AI Assurance Roadmap
- TechUK – AI Assurance Ecosystem Mapping
- Ada Lovelace Institute – Going Pro? Considerations for the Emerging Field of AI Governance

RESOURCE LIST

- Insert list of additional resources attendees can use or repeat speaker contact information here.

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Europe Congress 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!