iapp

Scaling responsible innovation with AI governance

Thursday, 14 May
08:00–09:00 PDT
11:00–12:00 EDT
17:00–18:00 CEST

Optro & AI Governance

Optro

The future is AI Governance

“The work of the company is increasingly going to shift to monitoring and overseeing all of the AI systems and agents running the company.”

- Jack Clark, Co-founder Anthropic

Optro

AI Governance growth

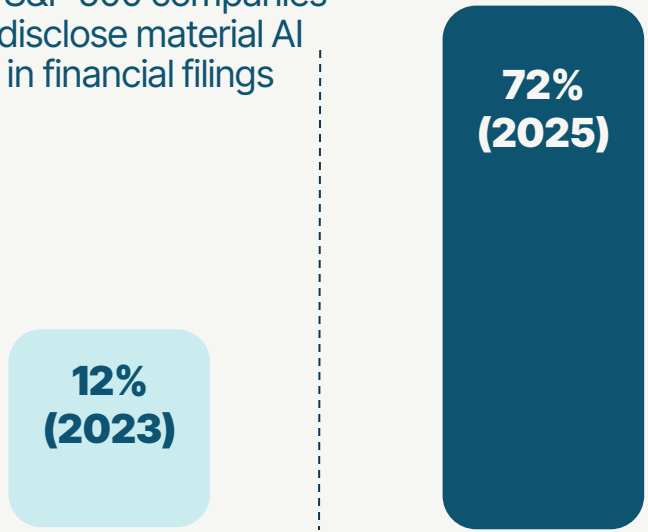
5-10x
Increase in search for AI Governance frameworks and tools in the last year

35-45%*
CAGR in AI Governance spending / market

34%
Higher op profits for orgs who invest in AI Gov (IBM, 2025)

$500M
Investment $ in AI Governance & Safety startups in 2025

% of S&P 500 companies that disclose material AI risks in financial filings



*Market growth from several hundred million today to single digits billions in 2030 to $20b-$30b by 2035 as AI agents become ubiquitous

Optro

AI Governance has two-sided ROI

AI Governance as an enabler to build trust in AI, move faster

AI Governance reduces business and regulatory risk

The growing risk of ungoverned AI

AI is everywhere...

Third party tools
Are racing to bake new AI into their tools, sometimes without informing customers

Employee AI usage
Half of US employees use AI tools for work, whether AI is sanctioned or not*

Internal model builds
Data scientists & developers are building AI systems for internal use or sale

...and the risks are growing

insecurechart

Data & Security

*According to a Q4 2025 study, "**40%** of files uploaded into GenAI tools contain PII or PCI."*

*More than **26%** of "agent skills" in tools like Github have at least one vulnerability, e.g., prompt injection*

Regulations & Legal

*GenAI lawsuit filings have increased by **978%** between 2021 and 2025.*

*Dozens of global regulations, including the EU AI Act, going into effect in 2026-27 (**27** new AI bills passed in past 2 years by G20 countries alone)*

April 26 Gallup Poll; Hacker News; Cornell University Research; Gallagher study, 2026 Stanford AI report

Optro

The AI regulatory landscape is already complex

Global Requirements

- **GDPR** Automated individual decision making (Article 22)
- **EU AI Act** (prohibitions + GPAI)
- **EU AI Act** (high-risk systems)
- **EU** AI Product Liability Directive
- **South Korea** AI Basic Act
- **China** Synthetic Content Rules
- **China** Measures for GenAI

US Federal and State

- **U.S.** Executive Order 14179
- **Colorado** AI Act
- **California** GenAI Training Data
- **California** ADMT Rules
- **Connecticut** AI Act
- **Maine** Chatbot Transparency
- **Utah** AI Policy Act
- **Texas** TRAIGA
- **Illinois** Human Rights Act 3773

Industry-Focused

- **California** Employer ADS Rules
- **California** Healthcare services AI
- **NYC** Local Law 144
- **Illinois** Video Interview Act
- **Colorado** Insurance SB 21-169
- **Colorado** AI in Healthcare
- **Maryland** HB 1202
- **Texas** AI in Health Records
- **FDA** AI-Enabled Device Guidance
- **NAIC** Use of AI by Insurers
- **SR 26-2** Model Risk Guidance
- **Canada** Guideline E-23

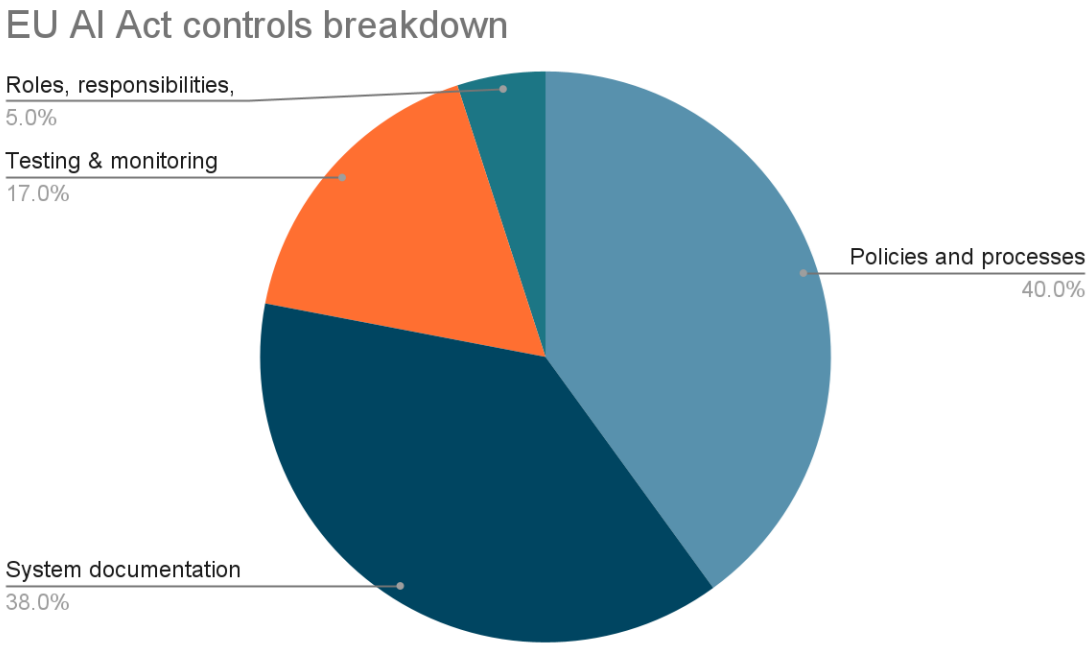
Voluntary Standards

- ISO/IEC 42001
- NIST AI RMF
- OECD AI Principles
- **Singapore** Fwk for Agentic AI
- **Australia** AI Safety Standards
- **Hong Kong** Ethical AI Framework
- **Japan** AI Utilization Guidelines

Optro tracking; list not comprehensive

Optro

The EU AI Act: an update



Digital Omnibus Amendments

GenAI Systems & Content

Feb. 2, 2027 → Dec. 2, 2026
Accelerated 3 months

- Transparency & watermarking rules
- "Reasonable safety measures" on any image/video system to prevent misuse

Standalone High-Risk AI Systems

Aug. 2, 2026 → Dec. 2, 2027
Delayed 16 months

- Compliance requirements for most developers & deployers **did not change**
- Extended simplified requirements to small-mid companies (750 employees)

High-Risk Systems in Regulated Products

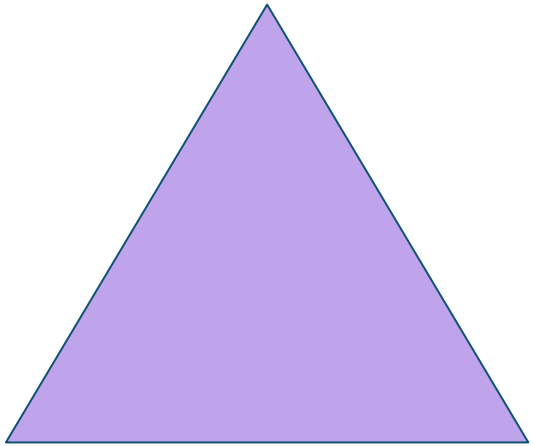
Aug. 2, 2027 → Aug. 2, 2028
Delayed 12 months

- Most machinery now exempt
- Other regulated products - guidance to come from EU

Optro

The business risks of AI

Cybersecurity & Data:
Data leakage, data privacy, security, prompt injection, data poisoning

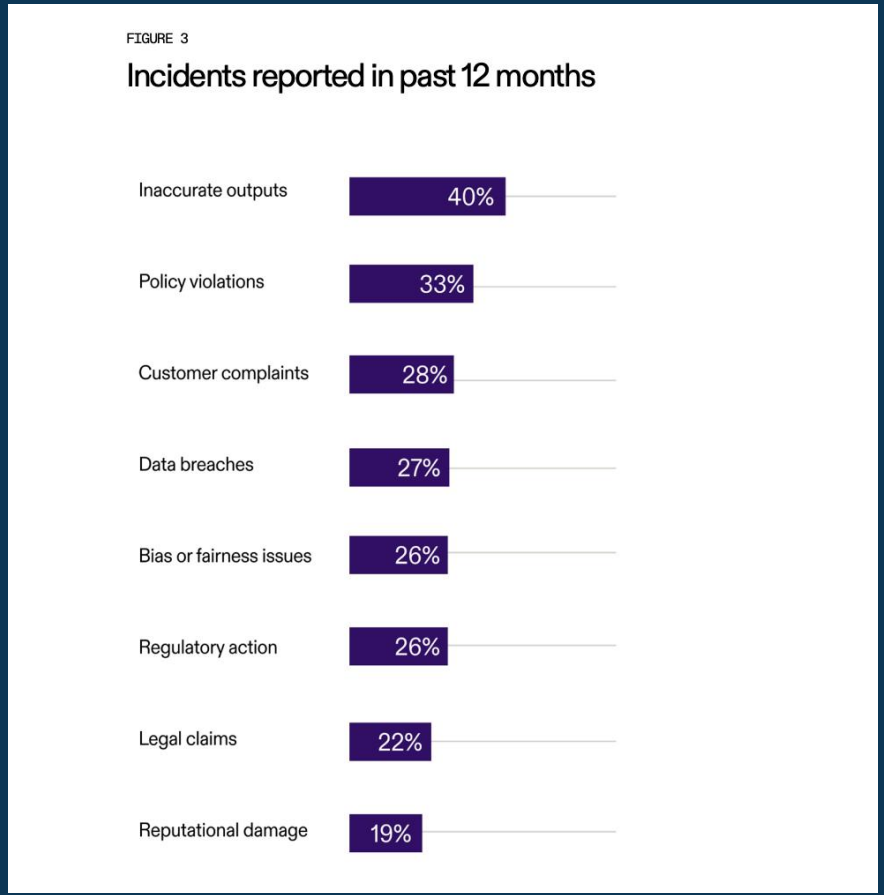


Performance & Integrity:
Performance drift, bias, hallucinations, reliability, toxicity

Transparency:
Transparency, explainability, auditability

The era of AI risks

- The real-world cost: reviewing the 12-month surge in AI-related data breaches (27%), regulatory actions (26%), and legal claims (22%).



Optro

Human risk

- The "human layer" risk: addressing the workforce as the most significant, yet least governed, risk surface.

Primary drivers of risky behavior

34% cite inputting sensitive data into AI systems as the top employee risk concern.

21% say insufficient training accounts for the majority of risky behavior, not malicious intent.

21% note pressure to move quickly is cited equally as a primary driver of unsafe AI use.

Optro

AI Governance is the set of policies, processes, and people that help you ensure responsible deployment of AI

Policies

- Compliance with external regulations and standards
- Development of and compliance with internal policies and guardrails

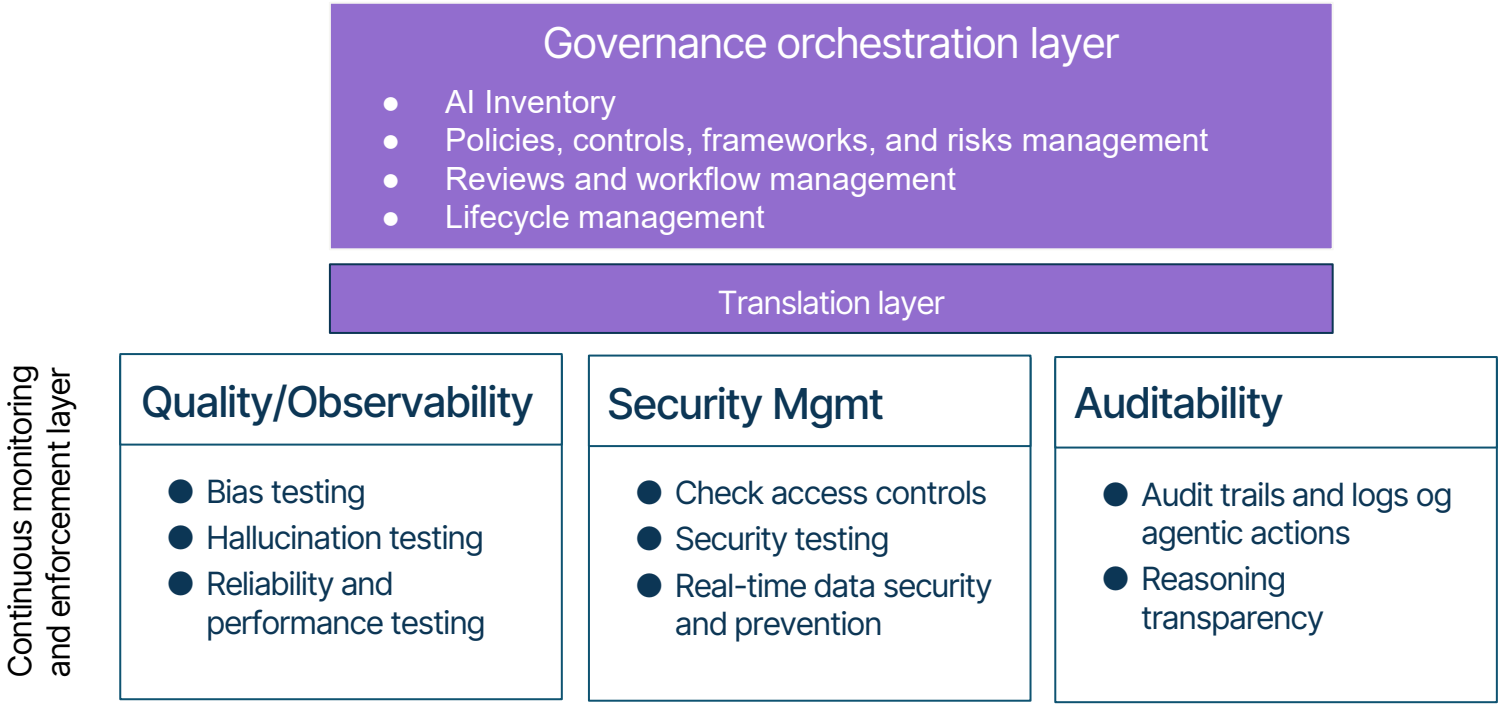
Processes

- Registry of AI systems and metadata
- Risk assessments
- Life cycle management
- Testing and monitoring
- Regular risk reviews
- Documentation

People

- Key stakeholders defined
- Roles and responsibilities defined
- AI governance training

Full-stack AI Governance will require continuous monitoring, orchestration, and human over-the-loop



Optro

While every company needs AI Governance, the urgency is higher for some

Geography: North America and EU due to regulatory expectations

Regulated industries: Financial services, Healthcare, HR, gov't, telecom

Vendors looking to demonstrate trust (e.g. ISO 42001)

Every company will need AI Governance

AI Governance is a team sport

First line: Eng./AI/Business

- Eng./AI: Focus on testing, monitoring
- Business: Focus on risk vs value trade-offs for specific AI use cases

Second line: CISO / Risk / Legal

- CISO: Focus on data and AI security, data privacy and governance;
- Risk: Focus on overall risks and compliance with controls
- Legal: Focus on regulatory requirements

Third line: Audit

- Audit: Responsible for internal auditing of AI

Board / C-Suite: Responsible for final accountability

Optro

Common AI Governance failures fall into three categories

Lack of clear responsibilities and accountability

Fragmentation of tools

Lack of continuous visibility

Companies fall into four buckets when it comes to AI Governance maturity

1

Behind

Not using AI or not planning to and/or not thinking about governance at all

2

Starting

Understand the importance of AI governance but are struggling to get started on policies, controls, and responsibilities,

3

Optimizing

Have a governance process in place but are looking to optimize the efficacy and efficiency of their program

4

Leading

Have a robust AI governance program but need to keep up with changing AI technology and risks

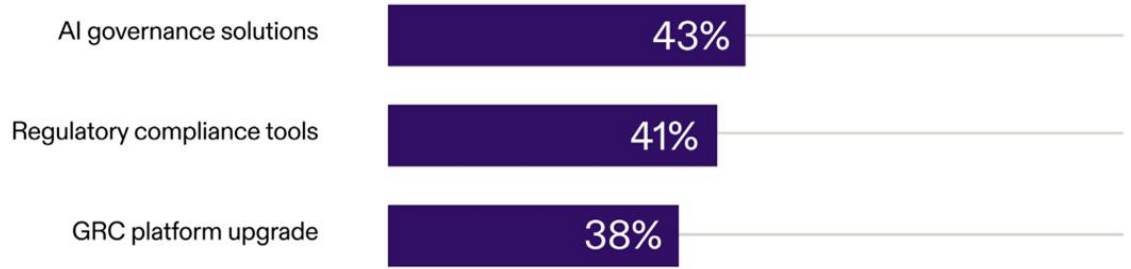
Investment signals

- Budgetary trends: why 72% of organizations are increasing GRC technology spend.
- Top priorities: AI governance solutions, regulatory compliance tools, GRC platform upgrade

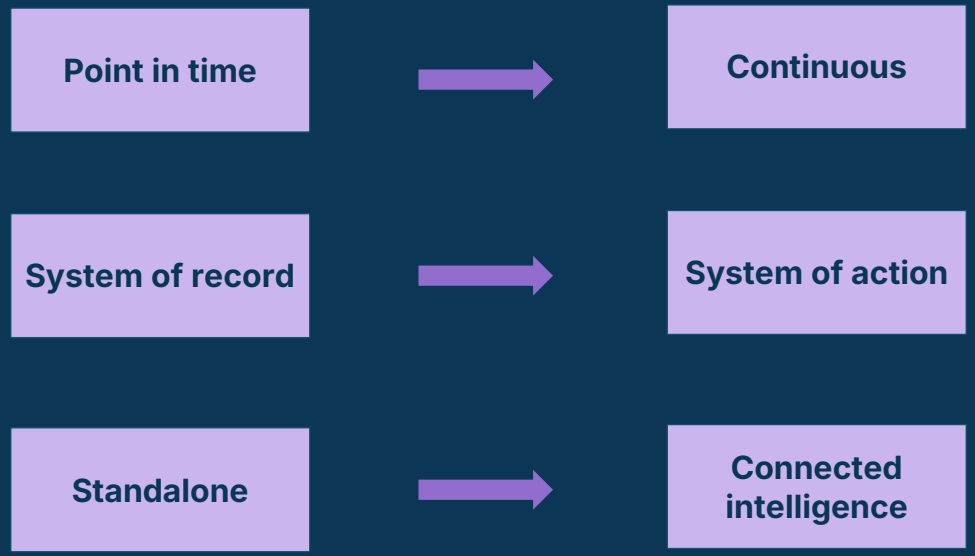
FIGURE 7

72% expect GRC technology budgets to increase

TOP INVESTMENT PRIORITIES



The architectural shift in GRC towards continuous, automated, and connected



Optro

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ8N13

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: livewebconteam@iapp.org