Advisory Council Annual Symposium



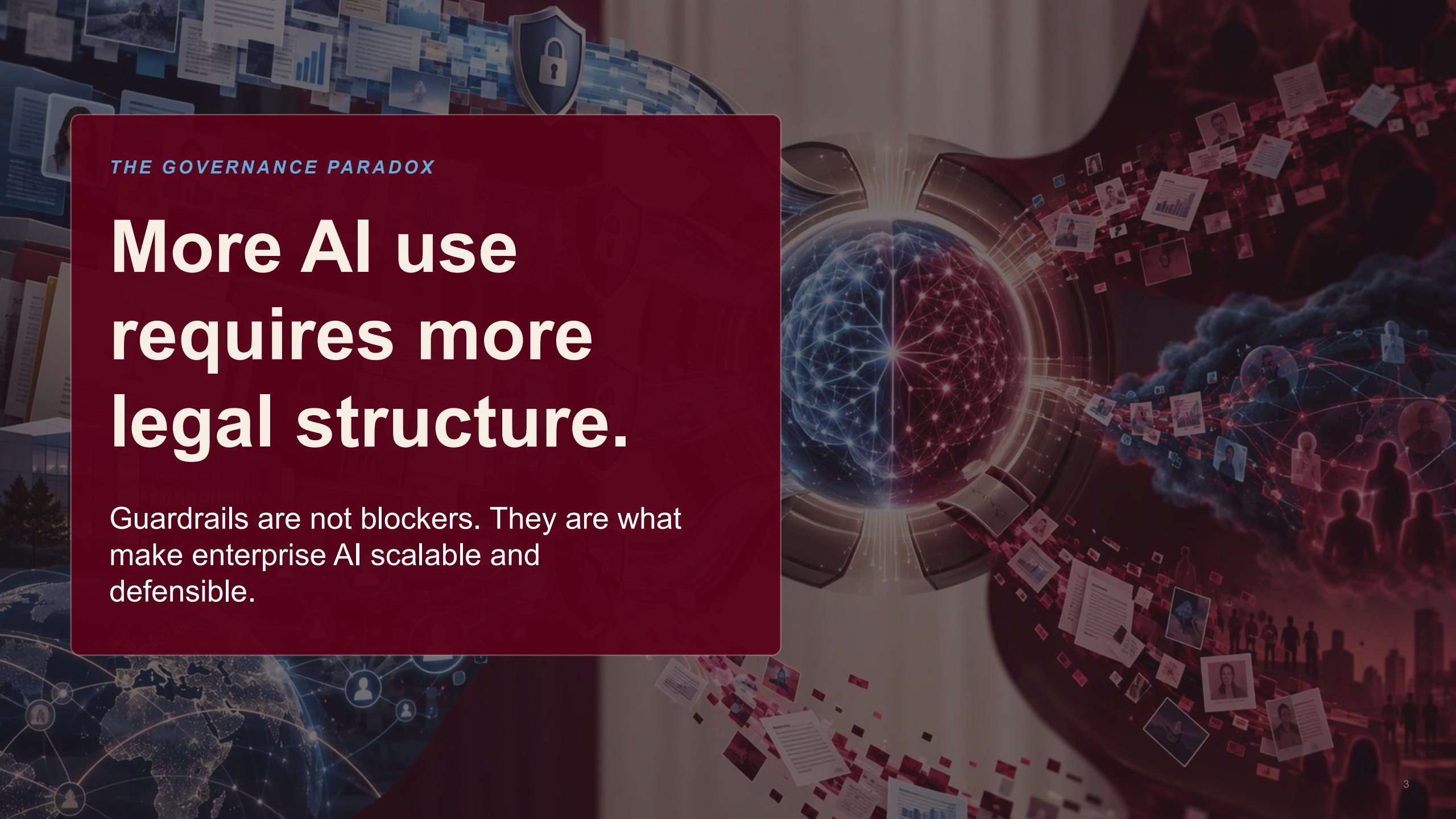
LEGAL CASE FOR RESPONSIBLE AI: MANAGING RISK, PRIVACY & TRUST

UNDERSTAND IT.
GOVERN IT.
USE IT.

Learning Objectives:

- **Explain** why AI governance is essential to responsible adoption.
- **Recognize** how laws and regulations are shaping AI use.
- **Identify** key privacy, accuracy, bias, and trust risks.
- **Apply** practical guardrails for more defensible AI use.
- **Use AI responsibly** while enabling innovation and business value.





THE GOVERNANCE PARADOX

More AI use requires more legal structure.

Guardrails are not blockers. They are what make enterprise AI scalable and defensible.

AI Use Risk Areas

Inaccuracy



Limited Transparency



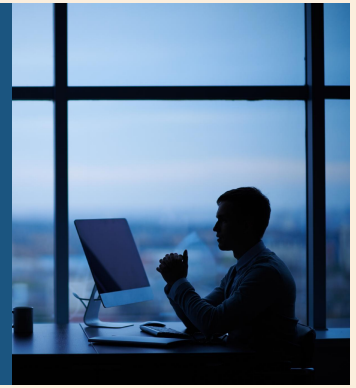
Security Vulnerabilities



Lack of Privacy & Confidentiality



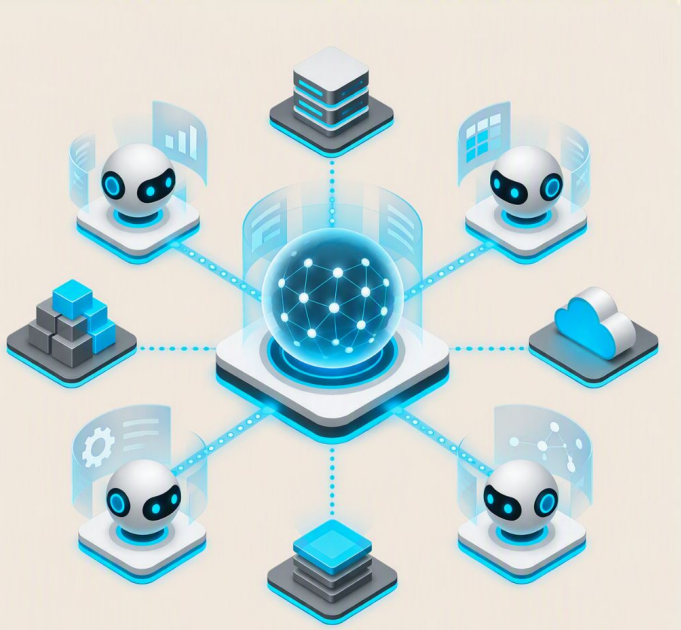
Bias



Intellectual Property Infringement



Agentic AI Amplifies the Risks



- Generative AI primarily produces content. Agentic AI can pursue a goal across multiple steps, use tools, and change systems.
- Errors can compound across steps; delegated permissions can trigger real-world actions; persistent memory and agent-to-agent activity can obscure who authorized what.
- Controls must cover identity, permissions, execution limits, approvals, logging, monitoring, and a reliable stop mechanism.

AI Regulations

No single federal AI statute.
Many enforceable rules.

The federal policy signal is active and contested

Executive Order 14365

The December 11, 2025 order declares a policy of pursuing a minimally burdensome national AI framework and directs federal action addressing state laws viewed as conflicting with that policy.

Operational takeaway: federal policy pressure does not erase state-law compliance duties.

PREEMPTION • PATCHWORK • INNOVATION

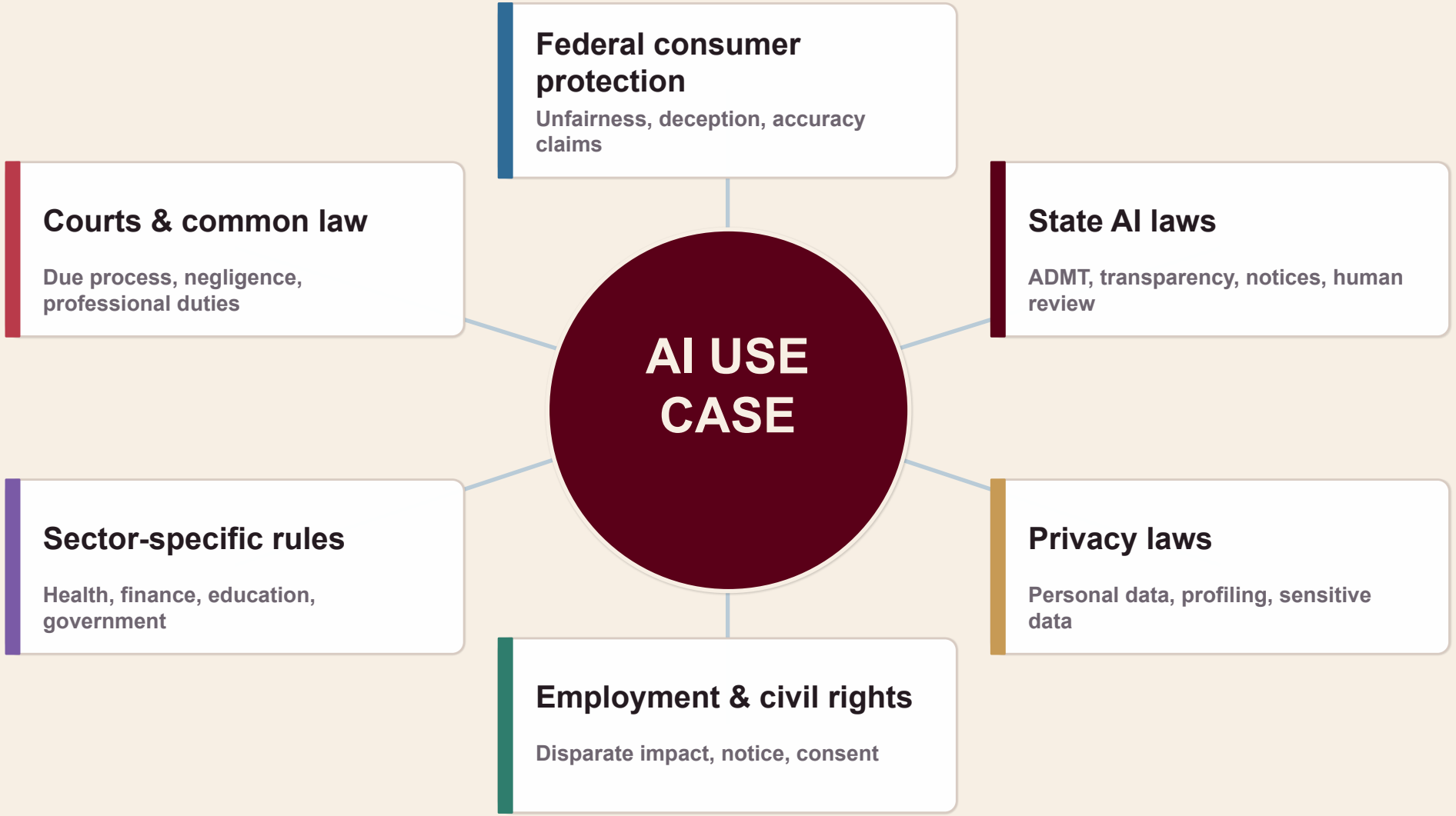
FTC: AI accuracy under Section 5

A July 2026 proposed policy statement focuses on whether AI outputs are steered contrary to reasonable consumer expectations for truthful and accurate performance. The enforcement theory is rooted in unfair or deceptive conduct.

Status matters: proposed policy, not a final rule.

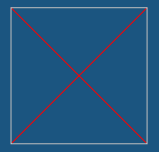
ACCURACY • REPRESENTATIONS • EXPECTATIONS

Legal Landscape Patchwork

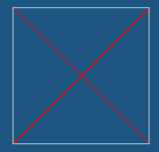


Laws that Regulate AI Use:

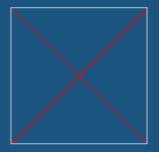
Currently in the U.S., there is no single, comprehensive law that requires companies to implement AI governance controls across all jurisdictions and sectors. While some regions have begun implementing AI-specific regulations, such as the EU AI Act, most jurisdictions are still developing their regulatory approaches.



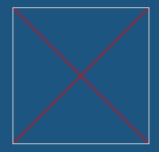
Comprehensive AI Regulations



Data Protection Laws



Narrow Scope AI Laws



General Application Laws applied to AI

(i.e. biometric, anti-discrimination, consumer protection, product liability, intellectual property)

States are the front line of practical compliance

Colorado

SB 26-189 replaces the earlier AI Act with ADMT duties effective for consequential decisions beginning Jan. 1, 2027: notices, explanations, correction, human review, documentation, and records.

California

A layered model: frontier-model transparency, training-data documentation, AI-content transparency, and employment discrimination rules.

Utah & Illinois

Targeted disclosure, consent, and employment-use requirements illustrate narrow, use-case-specific regulation.

Maryland

State AI governance includes a Responsible AI Policy for executive agencies, inventory and assessment, risk management, and prohibited uses.

ACCOUNTABILITY IN ACTION

Case law lessons for AI decision-making

Houston Federation

A public employer's reliance on a proprietary scoring model raised due-process concerns when affected teachers could not meaningfully verify or challenge the score.

EXPLAINABILITY + CONTESTABILITY

State v. Loomis

Algorithmic risk scores may inform a decision only with cautions and cannot substitute for individualized judicial judgment.

LIMITED RELIANCE

Mobley v. Workday

AI screening allegations show that vendors can be drawn into employment discrimination litigation alongside the organizations using their systems.

VENDOR + DEPLOYER RISK

Park / Mata

AI may support legal work, but counsel remains responsible for verifying citations, facts, and filings before submission.

HUMAN VERIFICATION

ENTERPRISE PRINCIPLES, NOT COMPANY RULES

Responsible use standards

Lawful purpose

Use AI consistently with applicable law and policy.

Transparency + accountability

Disclose material AI involvement and assign an accountable owner.

Fairness + human rights

Test for discrimination and protect affected people.

Human judgment

Keep meaningful review for consequential outcomes.

Accuracy + reliability

Set objectives, validate performance, monitor drift.

Privacy + security

Use a legal basis, minimize data, secure inputs and outputs.

Third parties

Diligence vendors, contract for controls, monitor performance.

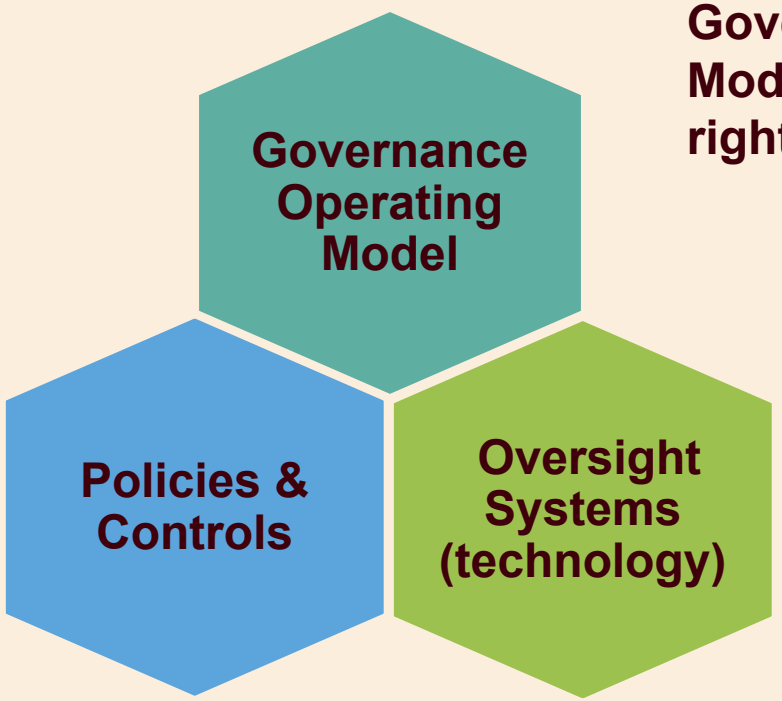
Education

Train users for the tools and decisions they influence.

AI governance is the process of **creating policies,** **assigning decision rights** and **ensuring organizational accountability** for risks and investment decisions in the application and use of artificial intelligence techniques.

AI Governance Overview

Create and Develop AI Governance Operating Model (e.g., teams, decision rights, culture)



Create, Maintain and Enforce AI Governance Policies and Controls

Design, Integrate, and Deploy Governance Technology Oversight Systems

© 2025 Gartner

RISK-BASED UTILIZATION

From prohibition to controlled enablement



CONTROL INTENSITY INCREASES WITH RISK

The control burden should rise with the consequence of the decision, the sensitivity of the data, and the autonomy of the system.

DEFENSIBLE GUARDRAILS

A practical AI life cycle and review process

1	**Approved tools**	Known controls and permitted environments
2	**Use-case classification**	Risk follows purpose, data, and impact
3	**Data controls**	Minimize, classify, restrict, retain
4	**Vendor + contract diligence**	Rights, security, training, audit, liability
5	**Testing + monitoring**	Accuracy, bias, drift, security
6	**Human review + disclosure**	Accountability and meaningful notice
7	**Incident response**	Escalate, contain, correct, learn



EIGHT QUESTIONS BEFORE DEPLOYMENT

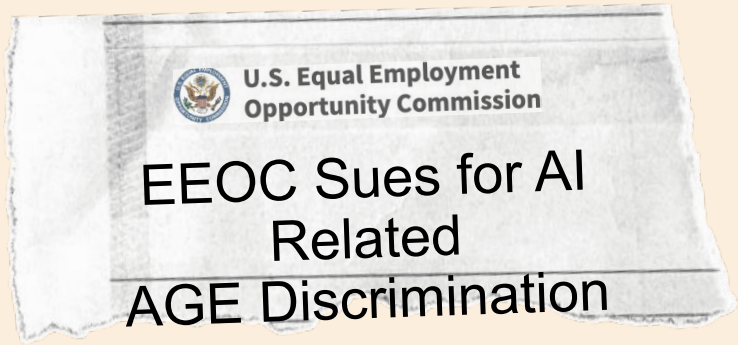
An AI governance defensibility checklist

1. What is the use case?
2. What data is used?
3. What law applies?
4. What vendor terms govern?
5. Who reviews the output?
6. What disclosures and notices are made?
7. How is bias tested?
8. How can a *person* challenge or change the result?

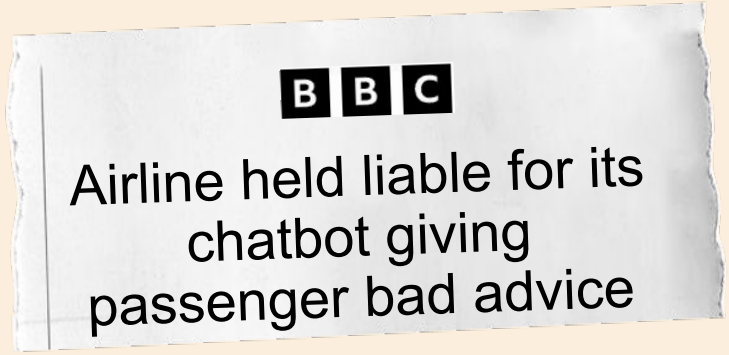
AI Related Incidents Across Industries



McDonald's terminated its AI-powered drive-thru voice ordering system in June 2024 after widespread failures led to customer frustration and reputational damage.

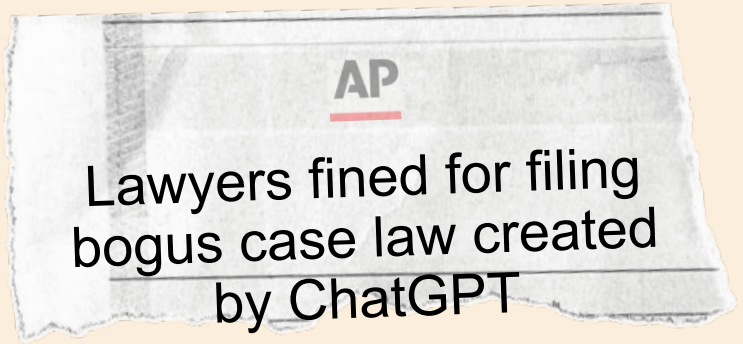


AI hiring system was found to discriminate against older applicants, resulting in a $365,000 settlement and mandatory anti-discrimination reforms—highlighting the legal and ethical risks of biased AI in recruitment.

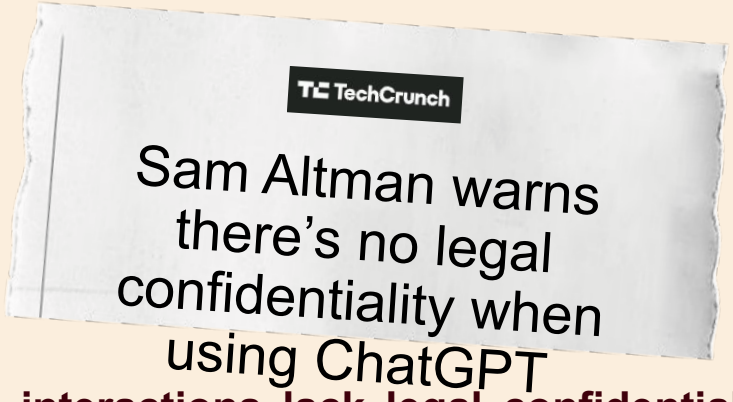


An Air Canada chatbot misinformed a passenger about bereavement fare refunds, leading to a lawsuit where the court ruled in favor of the passenger—highlighting the legal risks of relying on AI for customer service.

AI Precautions for Legal Professionals



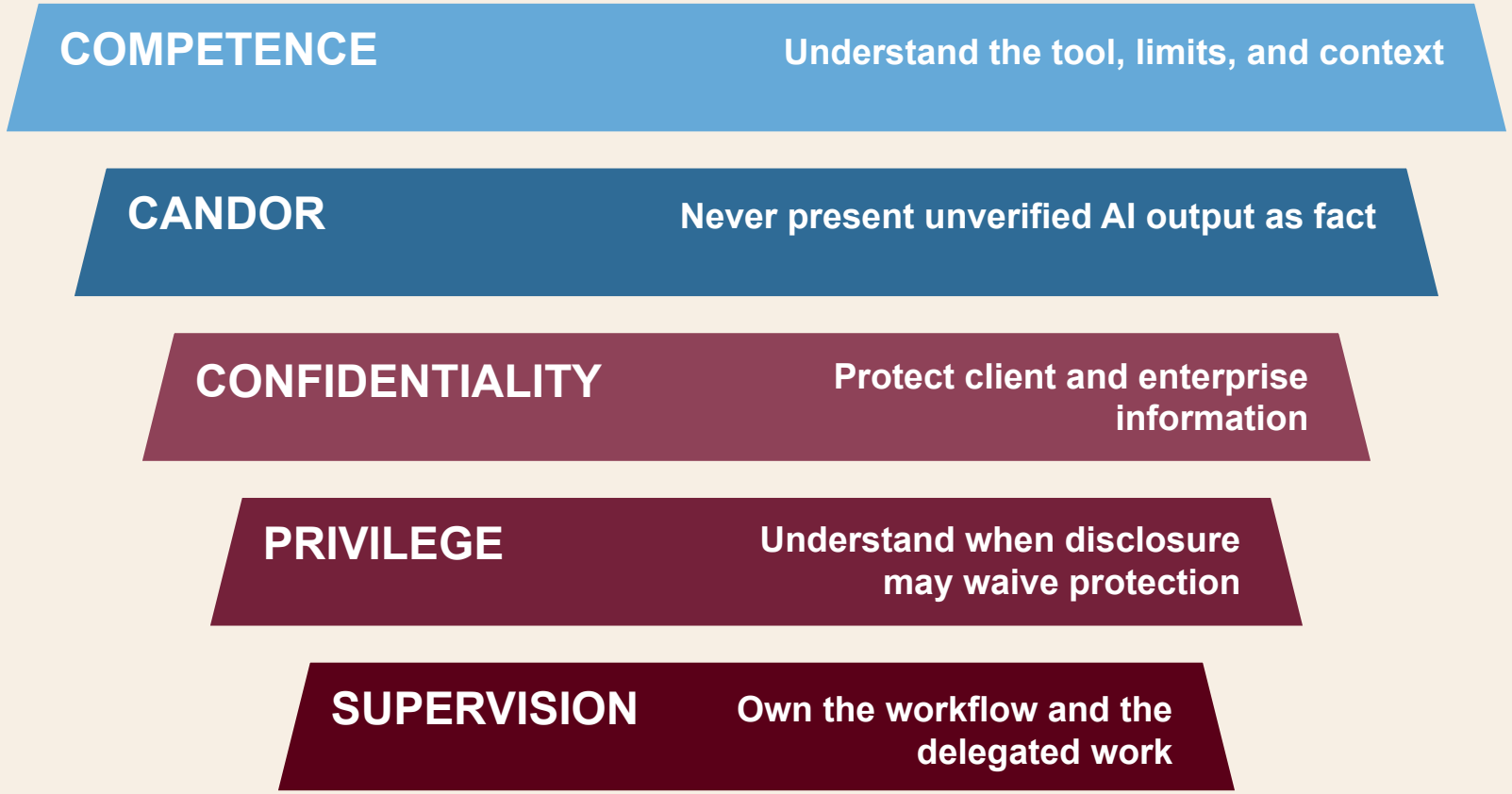
Attorneys were fined after submitting court filings based on fake cases generated by ChatGPT, underscoring the critical responsibility of legal professionals to verify AI outputs and maintain the integrity of legal proceedings.

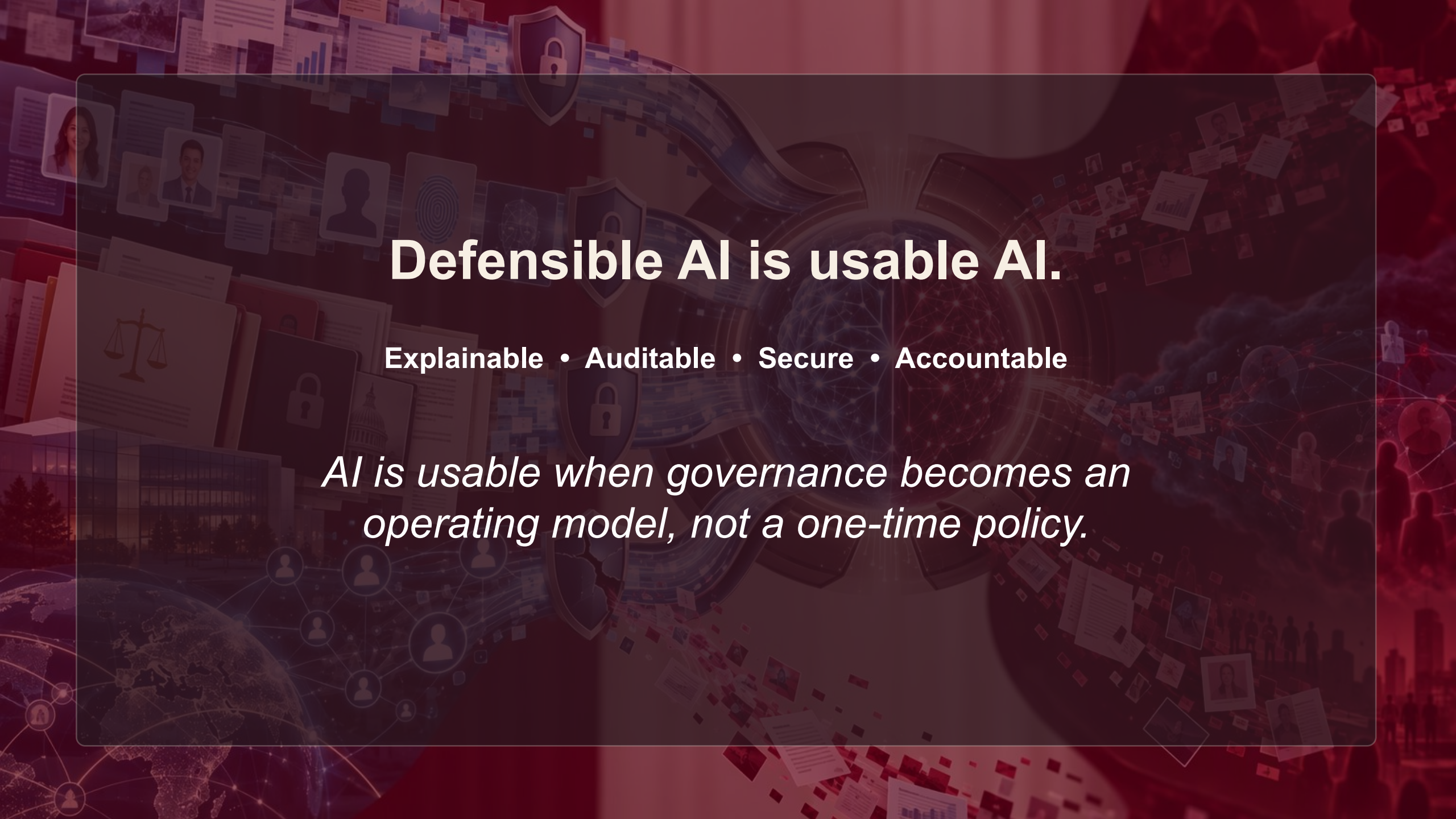


AI interactions lack legal confidentiality protections, making it risky for legal professionals to use tools like ChatGPT for sensitive client-related tasks, as privileged information shared with AI could be exposed in litigation or investigations.

PROFESSIONAL RESPONSIBILITY

The regulatory & legal professional's AI duty stack




Defensible AI is usable AI.
Explainable • Auditable • Secure • Accountable
AI is usable when governance becomes an operating model, not a one-time policy.