From Policy to Practice: AI Compliance that Enables Business

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by Gorodenkoff / *Shutterstock.com*

For most in-house attorneys, artificial intelligence has evolved from experimental technology to business imperative. While business teams using AI tools seek speed and a competitive advantage, in-house legal teams are increasingly accountable for AI risk management. Attorneys drafting comprehensive principles around fairness, transparency, and accountability, may struggle to operationalize these frameworks for daily business use. When AI policies require convoluted approval processes, they effectively halt AI adoption entirely driving innovation underground or grinding it to a halt.

Start with the business use case, not the tool

Anyone that dealt with the EU's General Data Protection Regulation (GDPR) implementation remembers the days of being asked "is your company GDPR compliant?". Rather than reviving an AI version of that inquiry, legal teams should focus on operational context: what business function does this system perform, and where does meaningful risk emerge?

AI applications vary significantly in risk profile. Some tools assist human decision-making, others automate processes entirely. Some rely on sensitive data inputs; others operate on publicly available information. Applying uniform governance across all AI use cases creates unnecessary operational friction.

Legal frameworks should establish initial assessment protocols that distinguish between:

- Assistive AI for content summarization, drafting, or data organization.
- Decision-support AI that informs human judgment while maintaining human oversight.
- Automated AI that drives or materially influences business outcomes.

Legal exposure escalates as AI assumes greater decision-making authority. Governance frameworks should scale proportionally, enabling rapid approval for low-risk applications while implementing rigorous oversight where warranted.

Focus governance on data, not demos

AI risk management aligns closely with established data governance principles. Effective AI oversight centers on three core inquiries:

- Data inputs: What information enters the system?
- Data control: Who maintains oversight of data processing?
- Output utilization: How are AI-generated results deployed?

In-house legal teams deliver maximum value by ensuring business stakeholders understand data provenance, retention requirements, and contractual restrictions on data reuse and model training. This becomes critical when vendors provide AI-enabled solutions that evolve continuously. Risk assessment must consider not only current functionality but potential future applications of client data.

> In-house legal teams deliver maximum value by ensuring business stakeholders understand data provenance, retention requirements, and contractual restrictions on data reuse and model training.

Establishing clear protocols for data inputs, retention periods, secondary use restrictions, and audit rights provides more meaningful risk mitigation than aspirational ethics statements.

Download the **Artificial Intelligence Toolkit for In-house Lawyers, Second Edition**

Build guardrails the business can actually follow

Risk escalates when laws and policies are not intuitive. The objective is not risk elimination but transparent, accountable risk management that executive leadership comprehends and endorses.

Effective operational guardrails demonstrate several characteristics:

- Plain-language documentation accessible to non-legal stakeholders.
- Integration with existing business workflows.
- Clear assignment of ownership beyond the legal department.
- Appropriate discretion for operational judgment.

Practical examples include:

- Mandatory human review for AI-generated content in client-facing or regulated contexts.
- Explicit protocols governing sensitive data usage.
- Streamlined approval processes calibrated to risk levels.
- Designated operational owners for AI tool deployment and monitoring.

Governance is a team sport

In-house legal teams cannot effectively govern AI in isolation. Successful models employ cross-functional frameworks by design. Legal counsel provides risk assessment and regulatory guidance. IT and security teams manage technical controls and system architecture, while business leaders understand operational context and use case requirements.

An effective structure involves an AI governance working group with defined responsibilities:

- Legal establishes risk parameters and escalation protocols.
- IT and security implement technical safeguards and monitoring.
- Business leaders own use case definition and outcome accountability.

This allocation prevents Legal from becoming a default approval bottleneck while maintaining meaningful oversight and accountability.

Choosing when to say no and when to say not yet

One of the most challenging aspects of AI governance involves determining when to decline business requests. In-house legal teams build credibility through selective intervention. Treating every AI initiative as a regulatory emergency erodes legal department influence and business partnership.

> In-house legal teams build credibility through selective intervention.

Rather than defaulting to prohibition, effective legal leaders differentiate between:

- Use cases ready for immediate implementation.
- Use cases requiring modification or additional controls.
- Use cases requiring further development or risk assessment.

Avoiding over-governance

When approval processes become excessively lengthy or opaque, business units inevitably pursue unauthorized alternatives using consumer-grade tools or non-approved vendors. This shadow AI presents far greater risk exposure and management challenges.

A reliable governance indicator is whether employees seek approval before implementation. When they circumvent established processes, governance has become punitive rather than protective. Efficient approval workflows for low-risk applications build institutional trust and encourage transparency in AI adoption.

What good enough governance looks like

In-house attorneys often question whether their AI governance frameworks achieve sufficient maturity. However, AI governance should evolve alongside business requirements and technological capabilities. Perfection is less important than demonstrable progress.

> Perfection is less important than demonstrable progress.

Adequate governance demonstrates these characteristics:

- Business stakeholders understand applicable requirements and processes.
- Executive leadership maintains visibility into risk exposure and mitigation strategies.
- Legal counsel engages early on.

In conclusion, effective AI governance is not about developing the most comprehensive policy framework — it is about making informed risk trade-offs through clear communication and consistent application. When legal teams focus on data governance, decision-making accountability, and operational transparency, they evolve from gatekeepers to strategic business partners. This approach creates governance models that protect enterprise value while enabling innovation.

The most successful in-house counsels recognize that AI governance is ultimately about enabling responsible innovation, not preventing it. By building practical, scalable frameworks that align with business objectives, in-house legal teams position themselves as indispensable partners in their organization's digital transformation.

Join ACC for more AI insights!

Ryan Casey

Chief Legal Officer and Corporate Secretary

Lexitas

Ryan Casey is the Chief Legal Officer and Corporate Secretary at Lexitas, a leading provider of legal services including court reporting, process serving, records retrieval and legal talent sourcing. Previously, as Deputy General Counsel he led a remote, global team responsible for intellectual property, privacy, ESG, Media/AdTech, and M&A. His transactional experience includes dozens of acquisitions, divestitures, and refinancings totaling billions of dollars. In his earlier legal roles, he managed intellectual property portfolios and led due diligence teams. Casey received his J.D. from DePaul University College of Law and currently holds advisory board positions on commercial and nonprofit boards.