What Boards Really Need to Know About AI and Emerging Technology Risk

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by Shutterstock AI / *Shutterstock.com*

Cheat Sheet

- **Focus boards on material risk, not technical detail.** Directors need governance-relevant analysis of risk significance and control effectiveness, not a tour of the technology stack.
- **Use consistent reporting formats over time.** Boards build the comparative judgment that meaningful oversight requires, rather than starting from scratch each cycle.

- **Clarify management responsibility versus board oversight before presenting AI risk to the board.** Accountability for these systems is a governance prerequisite, not a question the board should be asked to resolve.

- **Build a defensible oversight record by documenting the questions asked, the risks identified, and the decisions made.** Regulators and courts focus on evidence of thoughtful process, not flawless outcomes.

The board meeting is in two weeks. The CISO has handed you a forty-slide deck on AI risk, and your job is to figure out what, if anything, belongs in front of the board. That is the governance challenge in miniature. Artificial intelligence, cybersecurity exposure, and data risk have moved from IT line items to boardroom agenda fixtures, and directors, many of whom built their careers long before machine learning entered the corporate vocabulary, are now expected to exercise meaningful fiduciary oversight over risks they may struggle to evaluate. That expectation falls on in-house counsel, who must translate a fast-moving technical landscape into something a board can actually act on, and who will answer for the quality of that translation when regulators, plaintiffs, or shareholders come looking.

Boards aren’t incapable of engaging with technology risk. The issue is that they’re often handed the wrong information at the wrong level of abstraction. A briefing that opens with a technical explanation of large language model architecture will lose most directors before the first recommendation. One that presents only headline metrics without context leaves the board with the appearance of oversight rather than its substance. Either way, the general counsel is exposed when regulators, plaintiffs, or shareholders later ask what the board knew and when it knew it.

The general counsel’s job isn’t to make the board technically literate. It’s to make the board governance ready. Those are two different things entirely.

> The general counsel’s job isn’t to make the board technically literate. It’s to make the board governance ready.

That starts with a clear-eyed answer to one question: what does the board actually need to know? Not everything that’s technically interesting, and certainly not everything the CISO or CTO finds worth reporting. The board’s oversight function runs on material risk, accountability, and control effectiveness. Information delivered to directors should be organized around those same considerations, not around the internal architecture of the company’s technology stack.

Material risk, in this context, is risk that could affect the company’s financial condition, legal liability, regulatory standing, or strategic direction in a way a reasonable investor or regulator would find significant. An algorithmic bias issue that draws adverse regulatory scrutiny is material. A model accuracy rate expressed as a percentage, standing alone, generally isn’t. When general counsels frame technology risk reporting through a materiality lens, the board hears something it can act on: the nature of the risk, its potential magnitude, and the state of the company’s mitigation

efforts. Everything else, the vendor specifications, the infrastructure diagrams, belongs in management-level reporting, not in the board deck.

This framing also disciplines the reporting process itself. Legal, compliance, and technology teams will often push to include more rather than less, on the reasonable assumption that fuller disclosure protects the company. It doesn't always. Directors who receive more information than they can meaningfully process aren't better positioned to exercise fiduciary oversight. They're better positioned to later claim they were overwhelmed and can't be held accountable. The general counsel who designs reporting around materiality and control effectiveness isn't shortchanging the board. That counsel is protecting it.

Format consistency matters as much as content, and it's something in-house counsel tend to underestimate. Boards develop oversight instincts through repetition. When directors see the same reporting structure quarter after quarter, they start building comparative judgment: this risk category was amber last quarter and is now red; that control was still in design six months ago and is now operational. That kind of longitudinal perspective is exactly what real oversight requires. A board that gets a different format, different metrics, or a different framing every cycle is being asked to make comparative judgments without a baseline. That rarely produces useful governance.

The practical implication is that general counsels should invest early in designing a reporting template and then hold the line against the inevitable pressure to refresh or expand it every cycle. The template should capture risk category, current status, trend direction, control maturity, and anything requiring board-level awareness or action. Brief enough that directors read it rather than skim it, stable enough that it builds an institutional record over time. What it shouldn't do is reinvent the narrative every quarter to track the technology team's current preoccupations or the latest industry alarm about AI.

The question of who owns what is where many governance programs quietly break down. Boards oversee risk; management owns it. That distinction is easy to articulate and genuinely hard

to maintain, particularly when AI risk is new, fast-moving, and not yet firmly assigned within the organizational structure. In-house counsel should treat the clarification of management accountability as a prerequisite, not a governance outcome the board is left to sort out. Before the board can exercise meaningful oversight of AI risk, there needs to be a clearly identified management owner, a defined risk appetite, and a framework for reporting performance against that appetite. The general counsel who surfaces the absence of any of those things has done the board a significant service, even when it creates friction with the C-suite.

In-house counsel should treat the clarification of management accountability as a prerequisite, not a governance outcome the board is left to sort out.

The same logic applies to how general counsels should present regulatory and legal risk. The AI regulatory landscape is moving at different speeds across different jurisdictions, and the temptation to hand the board a global regulatory survey is understandable. Resist it. What the board needs is a prioritized view of the regulatory exposures most likely to affect the company's operations, paired with a clear account of what management is doing about them and what escalation looks like if the risk profile shifts. The EU AI Act and sector-specific AI guidance from financial regulators are worth surfacing at the appropriate level of detail. A forty-page comparative analysis spanning sixty countries is a research project, not a governance deliverable.

Running through all of this is a thread general counsels sometimes neglect until it's urgently relevant: documentation. When a regulatory inquiry, shareholder derivative suit, or reputational crisis later focuses attention on what the board knew about AI or cybersecurity risk, the answer will be found in what's written down. Board minutes that capture genuine engagement with technology risk presentations, the questions directors asked, the follow-up they requested, and the management responses they received constitute a defensible record that the board did its job in good faith. General counsels who build that record deliberately from the start are creating a durable institutional asset, not checking a compliance box.

Escalation pathways deserve the same rigor as any other structural element of the governance program. Organizations rarely fail because they lacked rules; they fail because early warning signs didn't reach the right decision makers in time. Legal teams need to define clear triggers that require board or senior management awareness: a regulatory inquiry touching an AI system, systemic errors affecting customer relationships at scale, cross-border compliance concerns, or any situation where an AI system's operation conflicts with stated company values or published commitments. Those thresholds ensure that material risks surface while there's still room to correct them, rather than arriving as crises that require damage control.

Organizations rarely fail because they lacked rules; they fail because early warning signs didn't reach the right decision makers in time.

There's a version of AI governance theater many companies are currently performing. Boards receive impressive-looking technology dashboards, general counsels circulate lengthy AI policies, and everyone proceeds under the comfortable assumption that oversight is happening. It often isn't. Real oversight means directors understand what they're being asked to monitor, management carries actual accountability for the risk being described, and the reporting process is designed to surface problems rather than bury them in complexity. None of that happens by accident, and none of it happens without deliberate design by in-house counsel who understand both the governance

function and the technology landscape well enough to connect them.

The companies that handle AI risk well won't be the ones with the most sophisticated technology or the thickest governance policy. They'll be the ones where someone asked the hard questions early, built a structure that held under pressure, and documented the thinking clearly enough to defend it when scrutiny arrived. That someone is the general counsel. The board doesn't need a technologist. It needs a lawyer who understands that governance isn't a deliverable but a discipline, practiced consistently, adjusted deliberately, and owned completely. In the age of AI, that discipline is the job.

Join ACC for more AI insights!

Alexander Lima

Vice President and Associate General Counsel

Wesco International

Alexander Lima is Vice President and Associate General Counsel at Wesco International, a Fortune 200 company, advising on global transactions, M&A, governance, legal operations, and compliance across over 50 countries. His work spans multibillion-dollar business segments and sectors including infrastructure, AI, and high-growth international markets. Alexander also serves as Board Advisor and Corporate Secretary at Judy Security, a cybersecurity AI firm, and is an Adjunct Professor at the University of Miami School of Law.