Five Things Your Board Needs to Know About AI

Board Governance in the Age of AI

March 2026

R. McConnell Group PLLC

R. McConnell Group PLLC

Fiduciary Duty Landscape for Directors

Post-*Boeing* & *Caremark*: AI as a mission-critical risk

Oversight

Part of duty of care. *Boeing* held the Board liable for failure to monitor mission-critical risk. AI use increasingly qualifies.

Good Faith

Directors must make decisions in the corporation's best interests. Failure to implement AI governance can itself constitute bad faith under *Caremark*.

Disclosure

Directors must communicate honestly with shareholders. AI capabilities and risks are increasingly material to investors and proxy advisors.

Confidentiality

Board communications remain confidential. AI tools that process board materials must maintain enterprise-grade security.

In re Boeing Co. Derivative Litig., C.A. No. 2019-0907-MTZ (Del. Ch. Sept. 7, 2021); *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996)

Five Things Your Board Needs to Know

AI governance is no longer optional — it is a fiduciary obligation

1

Use AI Yourself

You cannot govern what you do not understand

2

Understand Your AI Exposure

Most risk comes through vendors and embedded tools

3

Know What Can Go Wrong

AI hallucinations, bias, IP infringement, noncompliance

4

Shadow AI Is Already Here

80%+ of employees use unapproved AI tools

5

Build the Governance Structure

Clear ownership, training, and documentation

Sources: Deloitte Global Boardroom Program, *Governance of AI* (2025); McKinsey & Company, *The State of AI in 2025* (2025); IBM/Ponemon, *Cost of Data Breach Report 2025* (2025)

1 Use AI Yourself

You cannot govern what you do not use or understand

THE LITERACY GAP

66% of directors report limited or no AI knowledge, yet **88% of organizations** already deploy AI

AI-literate boards outperform peers by 10.9 percentage points in return on equity

Briefings are not enough — directors must interact with AI tools directly to develop the intuition required for oversight

As Manning puts it: "However big you think AI is going to be, it is likely bigger" — dismissing AI is a mistake boards cannot afford

WHAT TO DO

- Schedule hands-on AI sessions using Claude, ChatGPT, and Copilot in guided board settings
- Require management to demonstrate AI systems the company actually uses — not vendor pitches
- Add AI fluency to the board skills matrix and director evaluation criteria
- Think of AI as an intern: good at tasks and being told stuff, but also makes mistakes — rephrase, ask questions, verify (Manning)

Sources: Deloitte Global Boardroom Program, *Governance of AI* (2025); McKinsey & Company, *The State of AI in 2025* (2025); MIT CISR, *Digitally Savvy Boards: AI Update* (2025); Manning & Thamkul, *Stanford Rock Center AI Symposium* (2023)

2 Understand Your AI Exposure

Most AI risk comes through vendors and embedded tools — not just the chatbots employees use

BEYOND CHATBOTS

AI is embedded in your CRM, HR platform, cloud provider, and contract tools — most exposure comes through vendors

A chatbot answers questions; an AI agent sends emails, moves files, and makes decisions — your company may already use both

Free consumer AI tools may store, train on, or expose everything employees input — enterprise platforms keep data within controls

The AI value chain creates downstream liability: components not initially "high risk" can be adapted into high-risk systems (Thamkul)

BOARD ACTION

- Require a complete AI inventory including AI embedded in third-party vendor products
- Classify each system by risk tier: assists employees, informs decisions, makes decisions, or acts autonomously
- Confirm vendor contracts prohibit training on company data and define liability for AI outputs
- Map upstream/downstream AI dependencies — understand where your vendors' AI components come from

Sources: Gartner, *Top 10 Strategic Technology Trends for 2025* (2024); IBM/Ponemon, *Cost of Data Breach Report 2025* (2025); Manning & Thamkul, *Stanford Rock Center AI Symposium* (2023)

3 Know What Can Go Wrong

AI creates new categories of legal exposure — directors must understand the risks

Three Ways to Go Wrong with AI (Manning):

Assume everything it says is correct | Think it's magical | Dismiss it entirely

LIABILITY EXPOSURE

- AI hallucinations produce confident but false outputs — decisions based on fabricated analysis create negligence exposure
- AI hiring/lending tools can discriminate at scale, triggering Title VII, ECOA, and state civil rights claims
- AI-generated content may infringe copyrights — companies face strict liability regardless of intent
- DOJ's ECCP now explicitly evaluates AI governance — prosecutors will ask what the board knew

REGULATORY LANDSCAPE

- EU AI Act (entered into force Aug. 2024; high-risk AI compliance obligations phase in 2026–2027)
- Colorado AI Act: risk management, impact assessments, and disclosure for high-risk AI decisions
- Glass Lewis 2025 guidelines encourage AI oversight disclosure; SEC pursuing "AI washing" enforcement
- Regulation is risk-tiered globally: tougher rules for high-stakes decisions in housing, healthcare, education, criminal justice (Thamkul)

Sources: U.S. Dep't of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs* (2024); EU AI Act (2024); Colo. Rev. Stat. § 6-1-1701 et seq. (2024); SB 24-205, signed May 17, 2024, as amended by SB 25B-004, signed Aug. 28, 2025, eff. June 30, 2026; Glass Lewis, *2025 Benchmark Policy Guidelines* (2025); Manning & Thamkul, *Stanford Rock Center AI Symposium* (2023)

4 Shadow AI Is Already Here

Employees are using AI whether or not the company provides a platform

80%+
of workers use unapproved AI

20%
of breaches involved shadow AI

$670K
added to average breach cost

46%
of violations: source code sharing

GOVERNANCE RESPONSE

- Provide approved AI tools that are better than what employees find on their own — prohibition drives the problem underground
- Audit actual AI usage — what tools, what data, what decisions — not just what was approved
- Establish acceptable use policies by risk: what data can be input, what AI can decide, and what needs human approval
- Every new hire has grown up using AI the way prior generations used Google — banning it is like banning the internet in 2005

Sources: UpGuard, *The State of Shadow AI* (2025); Microsoft & LinkedIn, *Work Trend Index 2024* (2024); IBM/Ponemon Institute, *Cost of a Data Breach Report 2025* (2025); Netskope Threat Labs, *Cloud and Threat Report* (2024)

5 Build the Governance Structure

Clear ownership, structured education, and documentation — not just policies on paper

GOVERNANCE DESIGN

- Assign AI oversight to a specific committee with a defined charter and reporting cadence
- Designate a C-suite AI owner accountable for risk posture, inventory, and incident response
- Establish acceptable use policies by risk tier: what data, what decisions, what requires human approval
- Require quarterly board briefings on AI developments, deployments, incidents, and regulatory changes

TRAINING & DOCUMENTATION

- Start with structured board education, then move to hands-on sessions using the company's actual AI tools
- 47% of Fortune 100 companies cite AI in director qualification descriptions — nearly double the 26% that did so in 2024
- Document all AI training — under *Caremark*, failure to implement reasonable governance constitutes bad faith
- Best practices: ongoing evaluation and testing, security controls, red teaming, vulnerability testing (Thamkul)

Sources: EY Center for Board Matters, *2025 Proxy Season Review* (2025); *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996); Manning & Thamkul, *Stanford Rock Center AI Symposium* (2023)

Five Principles of Trustworthy AI

Any governance framework should address these core principles (Thamkul)

1

Fairness

Minimize harmful bias through data curation, testing, and red teaming

Best Practices:

Data curation; bias evals; terms of use

2

Reliability

Ongoing evaluation, testing, and benchmarking throughout the AI lifecycle

Best Practices:

Security controls; red teaming; vulnerability testing

3

Human Control

Ensure people make critical decisions and can appeal automated outcomes

Best Practices:

Design into the application; in-product controls

4

Transparency

Users must know when AI is used, how it works, and how to interpret outputs

Best Practices:

Model cards; system cards; user guides

5

Privacy & Safety

Proactive risk management for data governance, security, and safety

Best Practices:

Data governance programs; safety evals; bug bounty

Source: Manning & Thamkul, *Stanford Rock Center AI Symposium* (2023)

Evolving Global AI Policy Landscape

Non-binding principles today will become binding laws tomorrow

United States

- EO: Removing Barriers to AI Leadership (2025)
- NIST AI Risk Management Framework
- EO: National AI Policy Framework (Dec. 2025)
- Colorado AI Act (eff. 2026)
- SEC "AI washing" enforcement
- DOJ ECCP AI governance evaluation

Europe

- EU AI Act (entered into force 2024; risk-tiered obligations apply on rolling basis through 2027)
- Risk-tiered compliance obligations
- Human-in-the-loop for high-risk AI
- Transparency & explainability rules
- Data Protection Impact Assessments
- Upstream/downstream provider duties

Global

- G7 Guiding Principles for AI
- Risk-based governance approach
- Testing & mitigation measures
- Transparency on capabilities
- Privacy & security by design
- Regulation segmented by risk level

Sources: Manning & Thamkul, *Stanford Rock Center AI Symposium* (2023); EU AI Act (2024); Colo. Rev. Stat. § 6-1-1701 et seq. (2024); U.S. Dep't of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs* (2024); Exec. Order No. 14,179, 90 Fed. Reg. 8741 (Jan. 23, 2025); Exec. Order No. 14,365, 90 Fed. Reg. 58,499 (Dec. 11, 2025)

Who Owns AI Oversight?

The question has shifted from whether AI matters to who is accountable

BOARD-LEVEL ACCOUNTABILITY

- Full board retains ultimate fiduciary responsibility — *Caremark* failure constitutes bad faith regardless of internal structure
- Designate a specific committee (audit, risk, or technology) with AI explicitly in its charter
- Glass Lewis 2025 guidelines now encourage disclosure of which committee owns AI oversight
- Quarterly reporting to full board on AI risk posture, incidents, and regulatory developments

MANAGEMENT ACCOUNTABILITY

- Designate a C-suite AI owner (CTO, CAIO, or GC) with defined reporting obligations to the board committee
- AI owner maintains inventory, risk tiering, incident response, and regulatory tracking — personally accountable for gaps
- Clear escalation paths: what triggers a board briefing vs. management resolution
- Document every decision — risk management is an ongoing process, not a fixed state (Thamkul)

Sources: *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996); Glass Lewis, *2025 Benchmark Policy Guidelines* (2025); Manning & Thamkul, *Stanford Rock Center AI Symposium* (2023)

Firm Lawyers

Matthew Boyden is a trial lawyer and former federal prosecutor with more than thirty-five years of experience. He represents companies and executives in high-stakes criminal, civil, regulatory, and governance matters. He is regularly engaged where litigation risk, regulatory scrutiny, and institutional exposure intersect. Matthew's practice includes federal criminal defense, complex civil litigation, internal investigations, and board-level advisory work. He has represented clients in matters involving securities fraud, sanctions and trade controls, anti-corruption, anti-money laundering, and financial misconduct, as well as parallel civil and regulatory proceedings. His work frequently involves emerging technology, financial services, and cross-border risk.

Larry Finder is a trial lawyer and former United States Attorney with more than four decades of experience handling complex criminal, civil, and regulatory matters of national significance. He represents individuals, corporations, and boards confronting serious legal, institutional, and reputational risk. Larry began his career as a felony prosecutor in Cook County, Illinois, where he tried major criminal cases early in his career, including serving on the John Wayne Gacy prosecution team. He later joined the U.S. Department of Justice, serving in increasingly senior leadership roles, including Chief of the Criminal Division and First Assistant U.S. Attorney, before being appointed United States Attorney for the Southern District of Texas in 1993. After government service, he was appointed by the U.S. Court of Appeals for the Fifth Circuit to investigate and litigate judicial misconduct by a federal judge, work that resulted in impeachment by the House of Representatives and conviction by the United States Senate.

Ryan McConnell is a former federal prosecutor and trial lawyer who represents companies, boards, and executives in high-stakes criminal, civil, and governance matters. He is called when litigation risk, regulatory exposure, and institutional credibility intersect. Ryan has tried nearly twenty federal jury trials and conducted hundreds of investigations involving complex fraud, cross-border enforcement, and sensitive regulatory issues. His practice focuses on federal criminal defense, complex civil litigation, internal investigations, and advising boards and senior executives on governance issues and matters requiring judgment under pressure. Ryan served as lead trial counsel in *U.S. v. Rovirosa*, a federal criminal prosecution brought by the Department of Justice's Fraud Section under the Foreign Corrupt Practices Act. Before founding his firm, Ryan was a partner at three international law firms, where he handled a broad range of complex civil and criminal litigation and led internal investigations across industries and jurisdictions. His civil litigation experience includes civil fraud, antitrust, securities, and derivative litigation; D&O and fiduciary-duty matters; shareholder and partnership disputes; and complex commercial litigation in state and federal courts nationwide.