Key Questions that General Counsels Should be Asking Themselves with Respect to AI

The General Counsel of a company plays uniquely critical roles—all of which are directly implicated by the adoption and use of AI. There are a number of key, practical questions GCs should be asking themselves. In no particular order:

1. Have I briefed the board or relevant committee(s) on the legal and governance implications of our use of AI?
2. Do we have a formal structure or policy for board-level oversight of AI risk and opportunity?
3. For Delaware corporations, will our AI-related activities expose directors and/or officers to Caremark oversight claims?
4. Do our board minutes and materials reflect a clear record of AI risk awareness and monitoring?
5. Do I understand where and how AI is being used across the company—in products, operations, disclosures, or customer interactions?
6. Are AI-related risks, including discrimination, hallucination, and IP infringement, formally integrated into our ERM framework?
7. Do we have policies in place to govern employee use of AI tools, particularly generative AI?
8. Are we monitoring relevant regulatory developments (EU, US Federal and state, FTC, DOJ, EEOC, other global AI laws)?
9. Could our use of AI give rise to material litigation, regulatory investigation, or enforcement?
10. Are we taking reasonable steps to prevent unlawful bias, data misuse, or consumer deception from AI outputs?
11. Are our AI-related public statements (in product information, press releases, earnings calls, 10-Qs and Ks, investor decks) accurate and not misleading?
12. Do I understand whether AI-generated content is used in disclosures, scripts, or investor communications?
13. Have I coordinated with finance and compliance to assess whether AI systems impact internal controls over financial reporting or disclosure controls?
14. Have we reviewed our contracts with AI vendors for:
    - IP ownership and indemnity?
    - Security standards?
    - Disclaimers of responsibility for outputs?
15. Are we conducting AI-specific diligence for material third-party software, tools, or APIs?
16. Are our data privacy practices sufficient for how we use or train AI systems?
17. Do we know whether training data contains sensitive or personally identifiable information?
18. Have we assessed the cyber risk implications of generative AI (e.g., prompt injection, model exfiltration)?
19. Are we prepared to defend how our AI models work in the event of litigation or regulatory inquiry?
20. Do we have appropriate documentation and explainability protocols for any high-risk or regulated AI applications?
21. Have I partnered with HR, compliance, and IT to implement training and usage guardrails for employees?
22. Am I fostering a culture of responsible innovation—balancing legal caution with business enablement?
23. Am I thinking ahead about potential AI-related disclosures, akin to the evolution of cybersecurity and sustainability?
24. Do we have a plan in place for AI-specific disclosure mandates?
25. Am I actively engaged with external networks to stay ahead of legal AI developments (Weil, CLEs, think tanks)?

* * *

If you have questions concerning the contents of this list, or would like more information on our webinar, please speak to your regular contact at Weil or to any of the following authors:

Authors

Howard Dicker	View Bio	howard.dicker@weil.com	+1 212 310 8858
Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
Olivia Greer	View Bio	olivia.greer@weil.com	+1 212 310 8815
Adé Heyliger	View Bio	ade.heyliger@weil.com	+1 202 682 7095