

AI preparedness checklist

What every company should be doing now

In the absence of clear AI-specific legislation or regulation in the United States, companies should neither heedlessly charge ahead nor timidly wait for greater clarity. Rather, as regulators use existing authorities and private litigants use old laws to bring suits centered on the newest technologies, companies should strongly consider establishing a written internal AI self-governance framework. This framework would institutionalize a focus on accountability, accuracy, compliance, fairness, security and other principles while developing or integrating AI tools, and it should include clear contracting guidelines. Through effective governance and responsible practices, companies can leverage AI's potential while greatly mitigating class action and regulatory risks.

- Establish a high-level AI Policy or AI Code of Conduct. Tone from the top matters. AI strategy and governance should be periodically discussed with the board of directors and senior management. Determine whether you are going to align with a particular framework such as the NIST AI Risk Management Framework or the NAIC Model Bulletin on AI Systems.
- Identify your cross-functional AI governance team, including legal, compliance, IT and business leads for AI matters. Consider including outside counsel and technology consultants with experience conducting AI impact assessments and bias testing on the company team.
- Review existing written information security, privacy and risk management policies and procedures with the team to ensure they reflect risks related to AI and current regulatory requirements governing AI, data security, privacy, and contractual obligations. Assign and document roles and responsibilities for compliance. Determine if your policies align with the company's business goals and practices. Link to your business continuity plan.
 - Ensure all applicable regulatory requirements have been built into company procedures. Confirm that the company has adequate compliance testing procedures in place and establish a schedule for testing.
- Know what and where your AI systems are. Ask each business unit how AI systems are used and what processes they impact. Consider that some AI systems may reside outside of the corporate data center(s), including on vendor systems or in the cloud.
- Develop an enterprise-level risk appetite statement and a detailed AI impact assessment process. These should be reviewed and updated regularly as new AI systems are developed and deployed and AI laws and regulations continue to evolve.
- Review your AI governance model and risk profile with executive management and the board of directors to ensure the board and management are adequately informed about the company's use and deployment of AI and have established satisfactory internal controls and governance structures.
- Risk management principles apply to artificial intelligence systems. Conduct periodic risk assessments to identify risks associated with AI systems and the potential business consequences of these risks. Common AI risks include bias, hallucinations, lack of transparency and explainability, and security vulnerabilities. What are the potential operational, legal and regulatory consequences if an AI system is biased, unfair or inaccurate?
- Establish AI information sharing processes across the company and with vendors. This should include any updates to company policies, procedures or risk assessment processes, as well as information on new laws, regulations and industry standards applicable to AI.
- Assess and document employees, contractors and consultants who have oversight responsibilities for AI systems, and periodically review their training and qualifications to confirm that their oversight roles are assigned appropriately. Document the training, qualifications and periodic reviews of all individuals responsible for developing, deploying or overseeing AI systems.

- Understand how your vendors, subcontractors and other third-party service providers are using AI. Ask about the external data sets used to train the AI system and assess the third party's ability to satisfy requirements for accuracy, security, transparency and explainability, and fairness.
- Update third-party contracts to require representations and warranties regarding the use and deployment of AI systems and adequate controls (including documented policies and procedures, training, risk assessments, and subcontractor requirements). Require periodic security certifications or conduct routine periodic compliance audits on these vendors.
- Verify that third-party service providers have sufficient insurance coverage and update third-party contracts to include language that contractually obligates vendors to maintain such insurance coverage.
- Ensure that your insurance coverage is adequate to protect against potential losses arising from the use of AI systems. Review with key business unit leaders the coverage and exclusion terms of the company's insurance for such losses. Determine whether the terms are appropriate for the nature of the company's business and the likely risks your company may face.
- Conduct regular training of employees and vendors in your AI system governance, procedures and responsibilities. Keep current the content of your privacy and information security training programs. Ensure that employees are trained in data protection measures and that procurement and marketing teams are required to vet their purchases through legal and compliance for AI system risks.

Eversheds Sutherland's Artificial Intelligence Practice

Eversheds Sutherland brings deep legal experience in technology, data privacy and corporate governance. We can provide essential guidance supporting compliance with applicable laws, regulations and industry standards. We are currently managing such projects for numerous Fortune 500 clients, including insurers, and we help them navigate issues particular to AI on a daily basis, such as data protection, consumer privacy, model governance, risk assessments and compliance with existing laws and anticipated future laws and regulations. We deliver high-quality, project-managed, seamless service to meet our clients' specific needs.

AI technology can introduce new risks, such as bias, discrimination, inaccurate and unreliable results, consumer privacy challenges and the need for executive or Board oversight and establishing ethical boundaries; we help clients identify and mitigate these challenges by formulating sound policies and legal strategies. Certain industries, such as financial services and healthcare, are heavily regulated, and using AI requires compliance with evolving laws and regulations in multiple jurisdictions. Companies need counsel with an established presence and deep experience with technology. We can help your company understand the evolving regulatory landscape and achieve compliance while simultaneously reducing potential risks of regulatory enforcement. In addition, Eversheds Sutherland has significant litigation capabilities in the event of disputes or legal challenges related to AI.

We have more than 3,000 lawyers operating in over 70 offices and more than 150 in various practices who are primarily serving insurance clients. We appreciate this opportunity to present our capabilities and discuss how we can work with you and your member companies to help you achieve your commercial objectives, including across the US and, where relevant, global borders.

Contact

For questions about AI preparedness, contact:

Cynthia M. Krus, *Partner*

Washington, DC: +1 202 383 0218

cynthiakrus@eversheds-sutherland.com

Rachel M. Reid, *Partner*

Atlanta: +1 404 853 8134

rachelreid@eversheds-sutherland.com

Cynthia R. Shoss, *Partner*

New York: +1 212 389 5012

cynthiashoss@eversheds-sutherland.com

Mary Jane Wilson-Bilik, *Partner*

Washington, DC: +1 202 383 0660

mjwilson-bilik@eversheds-sutherland.com

eversheds-sutherland.com

© Eversheds Sutherland Ltd. 2023. All rights are reserved to their respective owners.

Eversheds Sutherland (International) LLP and Eversheds Sutherland (US) LLP are part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, visit eversheds-sutherland.com. US42609_092623