



Artificial Intelligence Update

April 2024

Critical Components of AI Governance Programs

Over the past several decades, businesses have embraced varied technologies to accelerate growth. Navigating the doomsday headlines surrounding the latest hot technology—AI, and in particular, generative AI—while keeping pace with the rapidly evolving landscape of generative AI technology and its associated risks can feel overwhelming, even for the most seasoned professional. Yes, the human + machine model that generative AI promises is here to stay, as generative AI grows in prevalence and potential use cases. Fostering a culture of human oversight from the outset of developing and integrating AI and generative AI will help companies more successfully navigate and manage the risks inherent in this technology. In this alert, we outline some critical components companies should consider when establishing and evolving an AI governance program.

Establish A Cross-Functional AI Oversight Committee

Whether structured formally or informally, establishing a well-represented AI oversight committee forms the cornerstone of an effective AI governance program. The committee will be responsible for establishing the company's overarching relationship with AI and generative AI and will oversee decisions on establishing a governance framework, including approving and restricting use cases, to support the company's growth and strategic advantages in utilizing AI while mitigating risks. The committee should comprise diverse individuals from across the company, tasked with identifying and understanding potential use cases for AI and generative AI, as well as pinpointing associated risks that proposed use cases may pose. An AI

oversight committee typically includes leaders from IT, security, legal and representatives from core groups within the business (e.g., business-line leaders, HR, marketing/sales).

Creating and Maintaining a Generative AI Policy

Most companies already have an acceptable use policy (AUP) that governs the use of technology internally, including AI technology that the company has been using for years. However, the evolving risks presented by generative AI, namely AI technology that creates new content (e.g., texts, images, code, videos), often are not sufficiently covered by existing AUPs. Thus, AI governance programs should include a generative AI policy (either as a standalone or updated within an AUP) that establishes governing principles for building and using generative AI, including approved and prohibited use cases, restrictions on types of data that can train and be used as inputs in generative AI technology and parameters for utilizing outputs that are created by generative AI tools. Once the policy is established, consider creating guidelines with specific details on how to apply the policy to key groups within the business (e.g., engineering, sales/marketing, HR). The policy should be revisited regularly to consider the evolving generative AI technology and its associated risks, as well as the company's growth objectives.

Establishing Processes for Incorporating and Monitoring AI

Effective AI governance programs should identify processes

that need to be established or existing processes that can be utilized to vet AI use cases to obtain and maintain visibility into the company's development and use of AI.

Third-Party AI Tools

Many organizations already have a vendor management or procurement program that includes security, legal and leadership reviews for third-party software procurement. Revising existing programs to incorporate checks for standalone AI technology as well as AI components/functions within the software will help ensure that a proper level of evaluation of the tool occurs and that they adhere to the company's AI preferences.

While the standalone AI software can be monitored traditionally, monitoring AI embedded within the software is more challenging. Creating processes to identify AI components within existing and new software subscriptions will help companies understand their ability to control availability or monitor usage of such features (e.g., a generative AI feature that creates a summary of meetings built into video conferencing software).

Additionally, while specific technology or services being procured might not include AI technology, the provider's supply chain may still encompass AI; therefore, processes should also entail asking vendors about their use of third-party technology and any AI they utilize.

Development of AI and Generative AI Tools

Many organizations already have development cycles with specific checkpoints at different stages throughout the process. Companies should examine their development cycles to ensure that there are built-in evaluation points throughout the cycle to ensure alignment with their AI and generative AI preferences.

Like the "privacy by design" concept, companies can consider building a culture of compliance through an "ethical AI by design" program. Checkpoints in the development of AI and generative AI technology should be considered at the initiation and concept stage, design stage, development and training stage, and continue through the operational and maintenance stages.

Educate and Train Your Workforce

A comprehensive AI governance program will include an education component, as an informed workforce is more likely to uphold and adhere to a company's approach to AI and generative AI. Much like the policy conversation above, companies should be mindful of creating a program that takes a realistic and grounded approach to this technology. If companies move too slowly or are too restrictive in their approach, employees will likely find creative, and often less secure, ways to circumvent the policies. Instead of simply establishing new rules to follow, companies should educate and train their employees about the organizational risks that AI and generative AI can pose, and tailor training to their specific industry and illustrate the most likely use cases. Educating employees on potential risks will help employees learn the "why" behind policy decisions. Doing so also enables employees to better identify and mitigate risks while also identifying opportunities for the use and development of AI and generative AI to align with the company's preferences.

Additional Resources

Similar to the principles of information governance and data governance, a strong AI governance program should be holistic, multi-disciplinary and leverage ongoing learning to constantly adapt and effectively safeguard the organization. In establishing an AI governance program, some helpful resources to consider are the [NIST AI Risk Management Framework](#), [the White House Executive Order on AI](#), including [the Office of Management and Budget's recently provided memorandum regarding Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence](#), and the [EU AI Act regulatory framework](#).

FOR MORE INFORMATION

For more information, please contact:

Julie D. Honor

312.998.4246

Julie.Honor@ThompsonHine.com

Will M. Henry

216.566.7077

William.Henry@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel. This document may be considered attorney advertising in some jurisdictions.

© 2024 THOMPSON HINE LLP. ALL RIGHTS RESERVED.