MUNCK WILSON MANDALA

Client Alerts

Why AI Governance Should Align with AI Development

February 17, 2025 | (Time to read: 3 minutes)

By Daniel E. Venglarik

Recent months have seen exponential growth in artificial intelligence (AI) tools. Among new models, OpenAI successively released multiple new variants culminating with GPT-4o and o3-mini; DeepSeek released its comparable model R1; and Google released Gemini 2.0 Flash. Among AI agents and AI assistants, Microsoft and Mistral each released iOS and Android apps for Copilot and Le Chat, respectively.

This pace of development creates challenges for AI governance and enterprise risk management. Three areas that warrant accelerated cycle times are AI acceptable use policy updates, AI risk assessments, and data security. These areas require proactive updates to maintain compliance, protect sensitive information, and mitigate risks associated with AI deployment in business and personal contexts.

AI Acceptable Use Policies

The flurry of activity surrounding AI tools suggests that AI acceptable use policies must keep pace. Organizations need to establish clear guidelines for employees and stakeholders regarding the use of AI tools in professional settings.

Well-written AI acceptable use policies typically specify at least the following:

- **Approved AI Tools**: Specific identification of AI tools that employees are permitted to use for work, along with conditions governing such use such as device restrictions, approved datasets, and compliance requirements.
- **Permissible Uses**: Guidelines on how AI can be used within the organization, including acceptable tasks such as drafting content, generating reports, or analyzing data.
- **Prohibited Practices**: Restrictions on AI tools and use for sensitive activities, such as handling personally identifiable information (PII) or other confidential data, or engaging in certain types of decision-making.

To keep acceptable use policies relevant, organizations should match the speed of new AI developments to reflect emerging trends. Concomitant training and other informative communications to ensure that employees understand and adhere to policy updates should also be considered.

AI Risk Assessments

Risk assessments are foundational to governance and risk management, but are typically conducted with long iteration windows that range from quarters to multiple years. As new AI tools become available for potential integration into daily workflows, more frequent and focused “mini” risk assessments should be conducted to evaluate the potential impacts on business operations and compliance.

One key area that might be inadvertently overlooked between scheduled risk assessments is operational risks: As an enterprise workflow increasingly relies on an AI tool outside of enterprise control, how disruptive to business operations could service downtime become, and what fallback procedures are being maintained to mitigate such disruption?

Another risk – one that is relatively unique to AI – is output verification. Different reasoning models have different degrees of sophistication in drawing inferences and presenting results, and different vendors follow distinct practices regarding making the model's reasoning visible to the user. "Trust but verify" procedures can ensure that practices are merely AI-assisted, with ultimate decision-making being human.

A responsive approach to AI risk assessment enables organizations to identify vulnerabilities and implement safeguards before AI-related risks escalate.

Data Security and BYOD Policies

Stark contrasts exist between the terms regarding data ownership, privacy, and use and retention for different models. User ability to opt out of specific practices relating to (for example) monitoring by the vendor varies.

Because AI models rely on vast datasets to function, AI governance must address data security—both directly and through Bring Your Own Device (BYOD) policy updates. Key considerations include:

- **Device Security**: Implementing encryption and multi-factor authentication to secure AI-related activities on personal and enterprise devices.
- **Compliance Measures**: Ensuring AI usage aligns with data protection regulations such as GDPR, CCPA, and industry-specific guidelines.

By proactively adapting governance frameworks, organizations can harness the power of AI while minimizing associated risks. AI governance should evolve in lockstep with AI development to ensure responsible, ethical, and secure implementation.

Related People

- Daniel E. Venglarik