# Navigating the challenges of generative AI and shadow AI in organisations



In recent years, the emergence of Generative AI (GenAI) tools has been heralded as the most disruptive technological advancement since the rise of the internet. This seismic shift began with the launch of the highly popular Large Language Model, ChatGPT, two years ago, fundamentally transforming how businesses and individuals consume information, create content, and analyse data.

The rapid evolution of these AI technologies has led many organisations to grapple with the challenges associated with their regulation and governance. Consequently, a phenomenon known as ‘Shadow AI’ has surfaced, as employees often utilise personal AI tools without the knowledge or approval of their employers. According to research conducted by Microsoft, a staggering 78% of knowledge workers regularly employ their own AI platforms to facilitate work processes, yet 52% of these individuals do not disclose this information to their employers. This presents a considerable risk, as companies face potential data breaches, compliance violations, and various security threats.

To effectively manage these challenges, organisations must adopt a comprehensive strategy that encompasses robust governance, clear communication, and adaptable monitoring and management of AI tools. Adam Wignall, General Manager at Kolekti, commented on the significance of establishing trust in these dynamics. He notes that “employees will use GenAI tools, whether their employer mandates it or not,” underscoring the difficulties associated with outright bans. Research indicates that 46% of employees would refuse to stop using AI tools even if prohibited.

GenAI technology offers accessible solutions that can significantly improve efficiency and address skill deficiencies within the workforce. Employers are thus encouraged to set clear guidelines regarding acceptable AI usage, which must be comprehensive enough to clarify both the permissible and prohibited applications of these tools. To this end, providing thorough training is vital to help employees navigate the complexities of safely and ethically utilising AI. Such training should encompass not only technical skills but also an understanding of the potential risks related to privacy, intellectual property, and compliance with regulations such as GDPR.

Another critical aspect is defining distinct use cases for AI within organisations. Many employees may currently refrain from using AI due to a lack of clarity on its application. A study indicates that 20% of staff do not utilise AI tools simply because they are unsure how to do so. By fostering awareness and understanding of these tools, organisations can mitigate risk while capitalising on the benefits that AI offers.

Additionally, organisations face the challenge of employees adopting unauthorised AI solutions that circumvent IT departments. The flexibility of many AI platforms can inadvertently contribute to the proliferation of tools that may not comply with necessary corporate policies or security standards. One proposed solution is robust API management, which allows companies to control how both internal and external AI tools integrate with their existing systems. This approach enables businesses to oversee data access, monitor interactions, and ensure that AI applications operate securely.

Despite the advantages of API management, it is crucial to avoid excessive surveillance practices that could push employees back towards shadow usage. Instead, setting up sensitive alerts to detect the improper handling of confidential information can serve as a preventive measure. For instance, AI tools might be configured to alert employees when personal data or proprietary information is at risk of being mishandled. These proactive measures can substantially reduce the likelihood of security incidents.

By constructing a solid governance framework, clarifying the acceptable use cases for AI, and employing adaptable API management procedures, organisations can find a viable balance between productivity and protection in the face of the challenges posed by Shadow AI. This strategy will enable businesses to leverage the full potential of GenAI tools while safeguarding data and adhering to internal policies. As enterprises continue to navigate the evolving landscape of AI technologies, fostering a culture of trust and transparency remains essential for driving innovation and ensuring compliance on all fronts.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier> - Corroborates the economic potential of generative AI, its impact on productivity, and the significant value it can add across various business functions.
* <https://wan-ifra.org/2024/11/two-years-later-taking-stock-of-chatgpts-impact-on-the-news-media/> - Provides details on the transformative impact of ChatGPT on various industries, including its rapid adoption and integration into workflows.
* <https://lpsonline.sas.upenn.edu/features/how-organizations-can-leverage-generative-ai-efficiency-and-help-employees-thrive> - Supports the benefits of generative AI in automating repetitive tasks, enhancing productivity, and improving decision-making across different industries.
* <https://masterofcode.com/blog/chatgpt-statistics> - Offers statistics on the widespread adoption of ChatGPT, its usage in various professions, and the potential benefits and risks associated with its use.
* <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier> - Highlights the potential for generative AI to automate a significant portion of employees' time and its impact on industries like banking, life sciences, and high tech.
* <https://lpsonline.sas.upenn.edu/features/how-organizations-can-leverage-generative-ai-efficiency-and-help-employees-thrive> - Emphasizes the importance of transparency, communication, and training in the implementation of generative AI tools to ensure safe and ethical use.
* <https://masterofcode.com/blog/chatgpt-statistics> - Provides data on the prevalence of employees using personal AI tools without employer knowledge, and the risks associated with such practices.
* <https://wan-ifra.org/2024/11/two-years-later-taking-stock-of-chatgpts-impact-on-the-news-media/> - Illustrates how AI tools like ChatGPT are being used in various professional settings, including journalism and software development, without always being disclosed to employers.
* <https://lpsonline.sas.upenn.edu/features/how-organizations-can-leverage-generative-ai-efficiency-and-help-employees-thrive> - Discusses the need for clear guidelines and training to help employees understand the permissible and prohibited applications of AI tools.
* <https://masterofcode.com/blog/chatgpt-statistics> - Supports the idea that employees may continue using AI tools even if prohibited, highlighting the need for a balanced approach to governance and trust.