Management of Shadow AI in the US

Ankita Varma

Department of Information Technology and Management, Illinois Tech

ITMS 578: Cyber Security Management

Professor Thomas Johnson

4/30/2025

Management of Shadow AI in the US

Artificial Intelligence (AI) is everywhere. It is present in phones, home smart devices and appliances, vehicle CarPlay, and any automatic system we interact with. However it is not always apparent that AI is a part of our daily lives with recommendations for YouTube videos, places to visit on Google Maps, shopping options on Amazon and restaurant recommendations for tonight in OpenTable in regular use. If we tried to define AI, then we would encounter a variety of definitions debated across disciplines. Despite this lack of consensus, everyone accepts it affects many aspects of people's lives in many different ways. One formal definition by the U.S. federal government in the National Artificial Intelligence Initiative Act of 2020 (2020) defined AI as:

> "The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—
>
> (A) perceive real and virtual environments;
>
> (B) abstract such perceptions into models through analysis in an automated manner; and
>
> (C) use model inference to formulate options for information or action." (§3)

The broad spectrum of applications and varying levels of integration and autonomy allow AI to be used in a variety of ways in multiple industries. For example, AI is embedded in almost every vehicle but the extent of autonomy differs between a Toyota RAV4 with smart safety features versus a Tesla with driving and parking autopilot capabilities. The Toyota has sensors and AI to inform the driver of the surroundings while the Tesla will interpret those inputs and

make driving decisions when in autopilot driving mode. This contrast illustrates different levels of AI autonomy. Similarly, smart home devices often use AI, typically integrated through a centralized control system that manages devices via commands such as a voice-activated light switch that turns a lamp on or off. In this case the AI device has high integration but low autonomy. More familiar AI use cases range from predictive typing in text messages to virtual assistants like Siri processing verbal input, and Google Translate processing images for language translation. These applications have significantly enhanced the accessibility of AI for consumers and reduced adoption hesitancy, making a notable departure from the apocalyptic representations of AI frequently depicted in science-fiction narratives. The growing ease of accomplishing everyday tasks through AI has opened the door to new use cases. These applications have embedded themselves into daily tasks and habits such that consumers have become dependent on their use. The benefits consumers enjoy in their personal life from AI leads to eagerness to use AI for their work related tasks. In the workplace, when users are using unsanctioned AI tools without the governance or visibility from IT and security teams, it creates the issue of Shadow AI. Shadow AI presents significant risks to companies and must be addressed through governance, training, and awareness to ensure employees understand the associated risks and acceptable use cases.

Due to the large amount of data in the world and on the internet now, people need help processing and understanding it to get out of analysis-paralysis. AI is facilitating the consumption of data and assisting consumers to identify important information for the task at hand. Offloading daily tasks to AI has freed up mental capacity to do more within the same 8-hour workday. Recent years have introduced agile methodology as a productivity booster, and now with AI tools, consumers can increase their performance at work, practitioners can improve

provided services in healthcare, and writers can beat writer's block. Software engineers often use GitHub Copilot as a coding assistant, physicians are using AI to develop treatment plans (Alowais et al., 2023), and students on PackBack are using AI to vet their logical constructs for cohesive discussions. Until now, AI outputs were used to guide consumers or nudge them towards specific actions, now the consumers can use AI for their own applications. Thus, turning the application use on its head, where consumers will be providers of input to the AI systems and interact with them in a hands-on way, whereas in the past, they were just consuming the output of the AI systems.

Shadow AI has evolved from an older problem: Shadow IT

Before discussing this latest workplace problem, we need to look back in history to find an example of a similar problem to give us lessons learned and ideas on what works to tackle the Shadow AI problem. We can refer back to Shadow IT for this. Shadow IT is the introduction of software or tools into a technological environment without the knowledge of or alignment with governing IT teams (Klotz et al., 2019). Shadow IT can happen for a multitude of factors. Klotz et al. discussed some factors including, but not limited to, the following:

- IT system shortcomings - IT system shortcomings are functional deficiencies that inhibit users from completing tasks effectively. These deficiencies may include systems containing incorrect data (Bob-Jones et al., 2008), lacking sufficient mobility, or being fundamentally ineffective (Kent et al., 2013). When current systems fail to adequately address the needs of end users, these users often resort to creating improvised solutions, which introduce new risks into organizational processes. While these solutions may address immediate needs, they exacerbate issues related to stability and scalability. For instance, Excel is frequently

employed to circumvent traditional IT systems, resulting in the creation of shadow IT systems (Silic & Back, 2014). Excel workbooks may interface with multiple systems, process data, and return it to databases. This practice introduces numerous points of failure, such as incorrect formula updates, insecure handling of database passwords, and the departure of key personnel, which complicates the maintenance of tools that the organization has become reliant upon.

- IT organization slowness - IT organization slowness can occur due to a lack of agility within the IT organization (Beimborn & Palitza, 2013), improper prioritization of change requests (Chua et al., 2014), and procurement and implementation processes that exceed task deadlines (Klotz et al., 2019). Agility within the IT organization is crucial for addressing the needs of the business. Ultimately, IT organizations exist to support the business in creating value, and when IT organization slowness starts hindering value creation, shadow IT systems emerge. Businesses often react to market changes and need to adapt quickly to remain competitive. If the IT systems they rely on cannot offer the necessary flexibility, they turn to solutions with less governance and more adaptability. For example, a business teams seeking greater flexibility in managing its workflow may find the pace of updating IT-sanctioned Jira too slow. Consequently, business teams may replace it with customizable cloud-based applications such as Monday.com to manage workflow outside of the IT systems.
- Lack of employee awareness of policies – Many employees are not aware of company policies and therefore contribute to shadow IT in the process of trying to complete their tasks. Even if they know the policies exist, they don’t know the policy content and consequences of not following those policies. A 2015 research found that 80% of employees

that violated IT policies, did so unknowingly (Dittes et al., 2015). Both the use of Excel workbooks to automate tasks and the adoption of cloud-based platforms to manage workflows often stem from a lack of employee awareness. When organizations fail to effectively communicate the risks associated with using unsanctioned tools and the potential consequences, employees tend to prioritize task completion without considering the unintended repercussions.

Unlike shadow IT which has been around for a while, shadow AI is newer and faster paced because AI products are evolving quickly and are useful for a wide range of applications to the wider public. Shadow IT required a more specialized skill set and technical know-how to find tools, install them and use them, whereas shadow AI is much more accessible and portable. AI is now accessible across employee devices - including smartphones, tablets, and laptops - regardless of location, facilitated by the widespread availability of high-speed internet connectivity.

For example, ChatGPT can be accessed through any web browser on any internet connected device and requiring minimal technical proficiency to use. Any user, of any skill level and any age can interact with ChatGPT about anything as long as they are able to input prompts. A young child with access to the internet can use voice search to access ChatGPT benefits even before they can read or write. Apple's integration of ChatGPT into Apple Intelligence now allows Siri to provide results via voice as well (Apple, 2024). In cases where employees are restricted from accessing ChatGPT or other AI tools on corporate devices, personal devices often serve as alternatives. The revolution of consumer technology and specifically the rapid expansion and adoption of personal devices has significantly expanded public access to the internet. As a result, approximately 8 out of 10 employees use non-corporate issued devices for work-related tasks

(Kolmar, 2022). Similarly, around 80% of companies have implemented some form of Bring Your Own Device (BYOD) policy (Kolmar, 2022). While many benefits were realized due to BYOD, it also exacerbated the problem of Shadow IT. The normalization of BYOD culture has contributed to the emergence of a parallel trend: Bring Your Own AI (BYOAI). In this context, every device is an opportunity to access AI tools, unsanctioned and untracked by the IT organization. The ease of use and broad applicability of these AI tools on personal devices to achieve performance and productivity goals increases the chances of applying AI tools to everyday tasks. When surveyed, 75% of knowledge workers are using AI and more than 50% of them are using personal or non-corporate devices to do so (Software AG, 2024). Even in these cases, personal devices can constitute shadow IT and their use of AI tools represents shadow AI. This evolution of shadow AI has significantly transformed the technological landscape of the workplace and presents critical challenges that must be addressed.

Motivations of Shadow AI

The underlying motivations behind shadow IT and shadow AI are very similar: IT system shortcomings, IT organization slowness, and lack of employee awareness. People are trying to fulfill their professional responsibilities while navigating workplace challenges to ensure timely completion of tasks and the delivery of high-quality work. Shadow AI can be discussed in a similar pattern:

IT system shortcomings

As discussed in the Shadow IT section, end users prioritize completing their tasks as efficiently as possible. When the current system does not facilitate this, users seek alternatives.

In the case of shadow AI, IT system shortcomings manifest in several scenarios, such as developers wanting to use coding assistants for help with code documentation, code generation, and code refactoring, as illustrated in Figure 1 (Deniz et al., 2023). AI assistants, such as GitHub Copilot, can write detailed code documentation and comments based on reading the source code. They can generate code for repetitive tasks, such as accessing a library or looking up specific syntax, and even write unit tests for small software programs. Code refactoring involves maintaining legacy code through regular updates to accommodate new scenarios or incorporate changes to essential library packages, ensuring these modifications are propagated throughout the program. These are challenging tasks, and AI assistants help navigate the complexities by acting as a developer's pair programmer. When the corporate IT organization fails to provide tools for these purposes, developers are compelled to seek alternatives, often resorting to publicly accessible free platforms such as ChatGPT. In a GitHub survey (Figure 2), 60% of developers who used AI assistants reported feeling more job fulfillment, 77% spent less time searching, and 96% were faster at repetitive tasks (Kalliamvakou, 2022).

IT organization slowness

Shadow AI also occurs due to IT organization slowness in procurement, change request processing, and lack of organizational agility. This is especially apparent in the rapid innovation of AI technology. AI is widely marketed and frequently highlighted on social media for its benefits. This has created champions throughout companies, pushing for adoption. With new technologies such as ChatGPT and AI agents being introduced in recent years, companies have struggled to keep pace with adoption. The ease of access to AI tools through cloud-based systems has made unsanctioned use of AI increasingly common. According to Deloitte (2024), 46% of companies are giving access to AI tools to 20% or less of their employees. This

staggeringly low number is driven by the disconnect in how employers and employees view the immediate AI adoption timeline. While employees are eager to use the new tools available to them, the organization doesn't see the urgency to implement the changes as illustrated by Figure 3 (Mayer et al., 2025). For example, employees are 3 times more likely to be using AI tools in their daily tasks compared to their leadership's expectations. Another indicator of slow adoption is that approximately 75% of companies do not have a comprehensive roadmap for their AI tool strategies as shown in Figure 4.

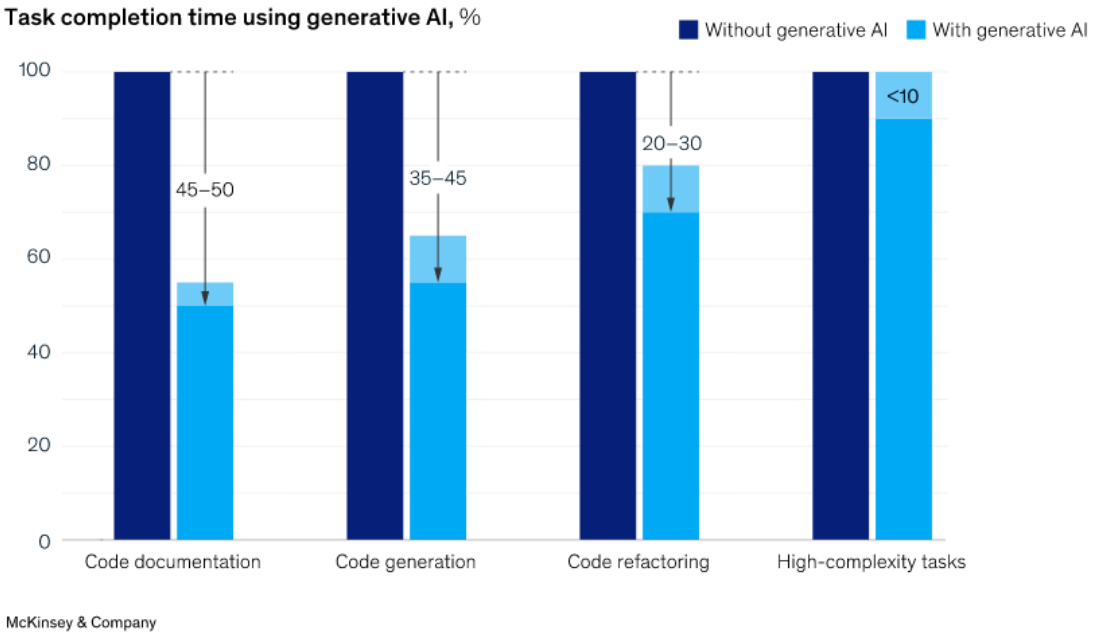
Lack of employee awareness

Lastly, and potentially a significant contributor to the rise of shadow AI, is employees' lack of policy awareness. Employees are unaware of the existence and content of policies and therefore do not know the consequences of not following them. According to a survey from The Conference Board (2023), 17% of employees don't know if their company has an AI policy. One contributing factor is the limited visibility that managers have into their employees' use of AI tools. As a result, organizational leaders often lack a comprehensive understanding of the extent to which AI is being utilized across the company. This lack of insight frequently leads to the absence of formal AI policies, or when such policies do exist, to a failure in effectively communicating them to the broader workforce. At the same time, many employees, recognizing the growing relevance of AI in their daily tasks, are eager for formalized training and guidance. As illustrated in Figure 5, 48% of US employees are eager for formal training from the organization on the usage of AI and 41% wish for better access to AI tools at work (Mayer et al., 2025). Employees within organizations have an appetite for learning and adopting new AI tools, particularly when their use is formally authorized and supported by organizational leadership. Consequently, when organizations take the initiative to establish clear policies for AI tool usage,

such efforts are likely to be well received and embraced by employees. These policies should be accompanied by comprehensive training and awareness programs to ensure that employees are properly informed about the organization's position on AI and its appropriate use within the business context. Furthermore, we see that currently only 29% of US employees perceive full support from their organizations on the usage of AI, increasing to merely 31% in the next 3 years. Organizational support for employee use of AI can significantly enhance authorization processes, promote acceptable usage practices, and improve governance visibility, each of which is essential for securing an organization's assets.

Figure 1

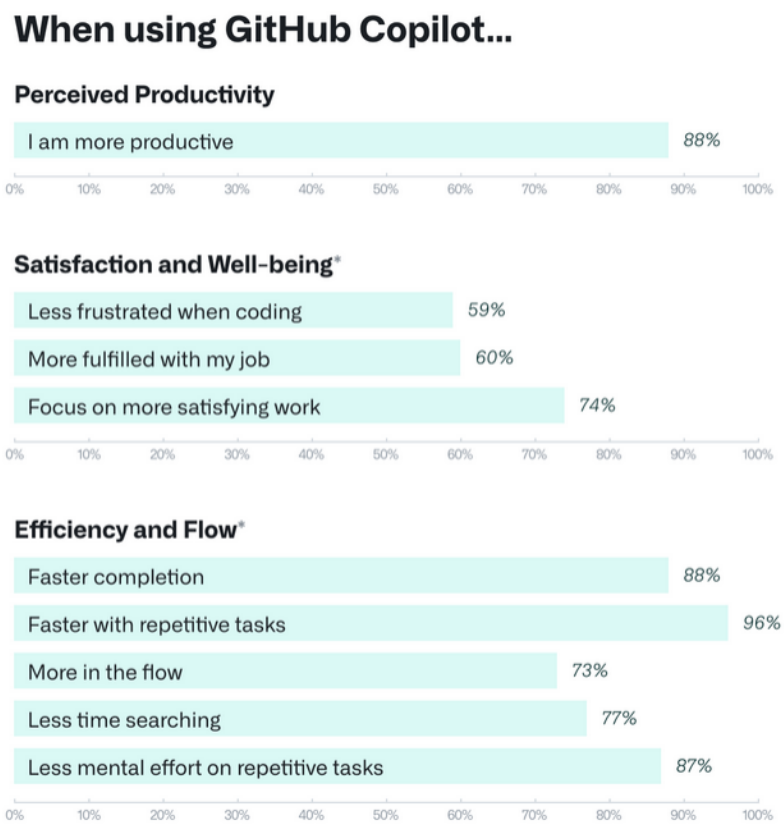
Developer task completion time with and without generative AI for code documentation, code generation, code refactoring and high-complexity tasks.



Note. This research was performed by McKinsey and the figure has been adapted from their report *Unleash developer productivity with generative AI* (Deniz et al., 2023)

Figure 2

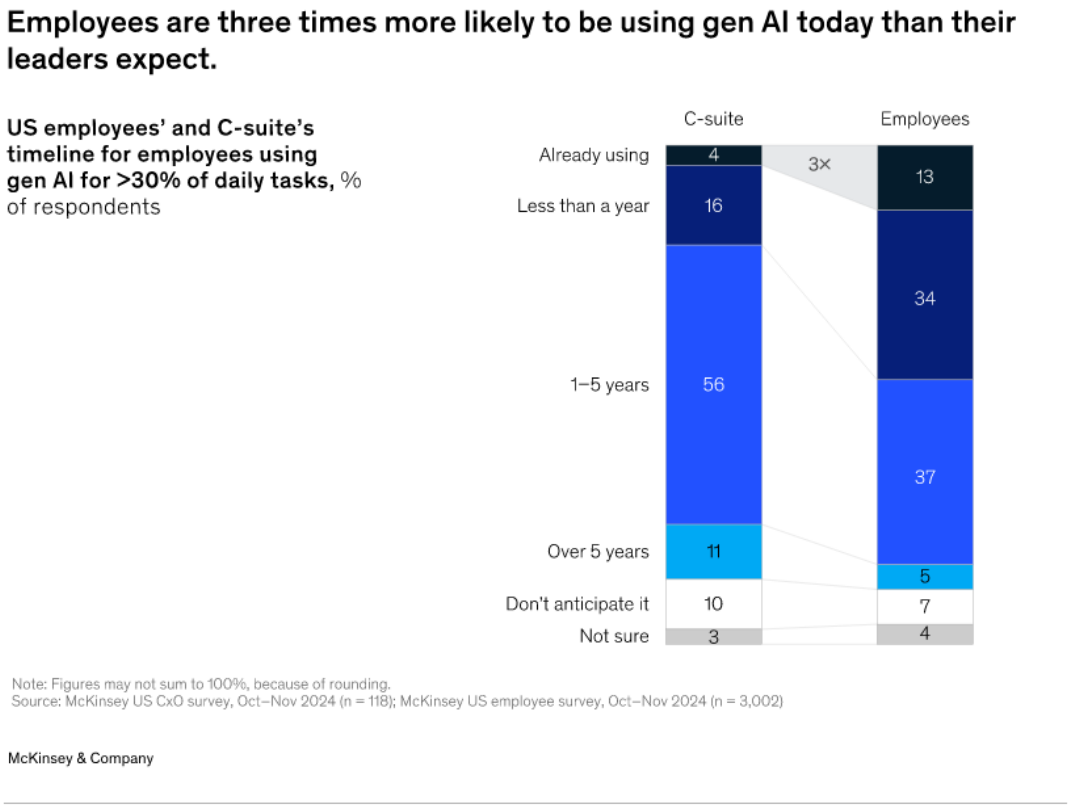
Survey of Developer reactions to using GitHub Copilot



Note. GitHub performed a study to understand the impact of GitHub Copilot on developers. Adapted from *Research: quantifying GitHub Copilot's impact on developer productivity and happiness* (Kalliamvakou, 2022)

Figure 3

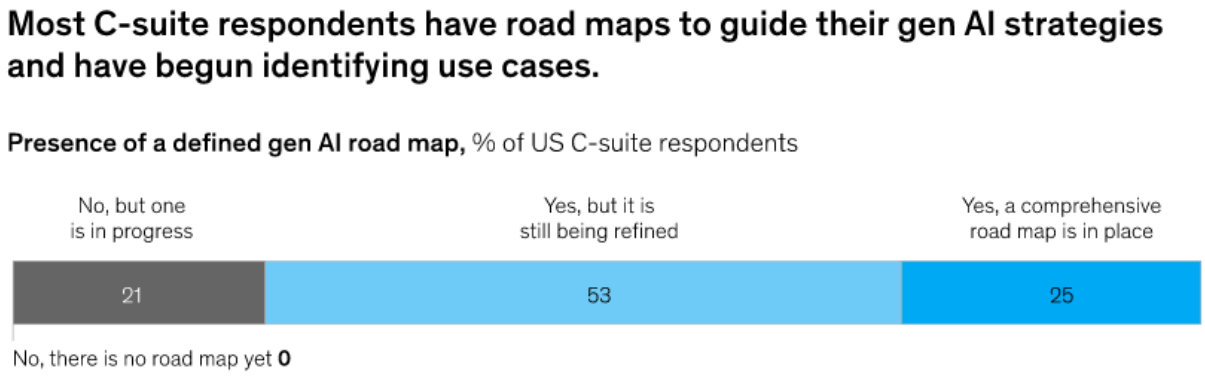
Employer and employee perspective of usage of Generative AI



Note. McKinsey & Company report performed a survey for both C-suite leaders and employees to understand the difference in expectations around AI use. This has been adapted from *Superagency in the workplace: Empowering people to unlock AI's full potential* (Mayer et al., 2025)

Figure 4

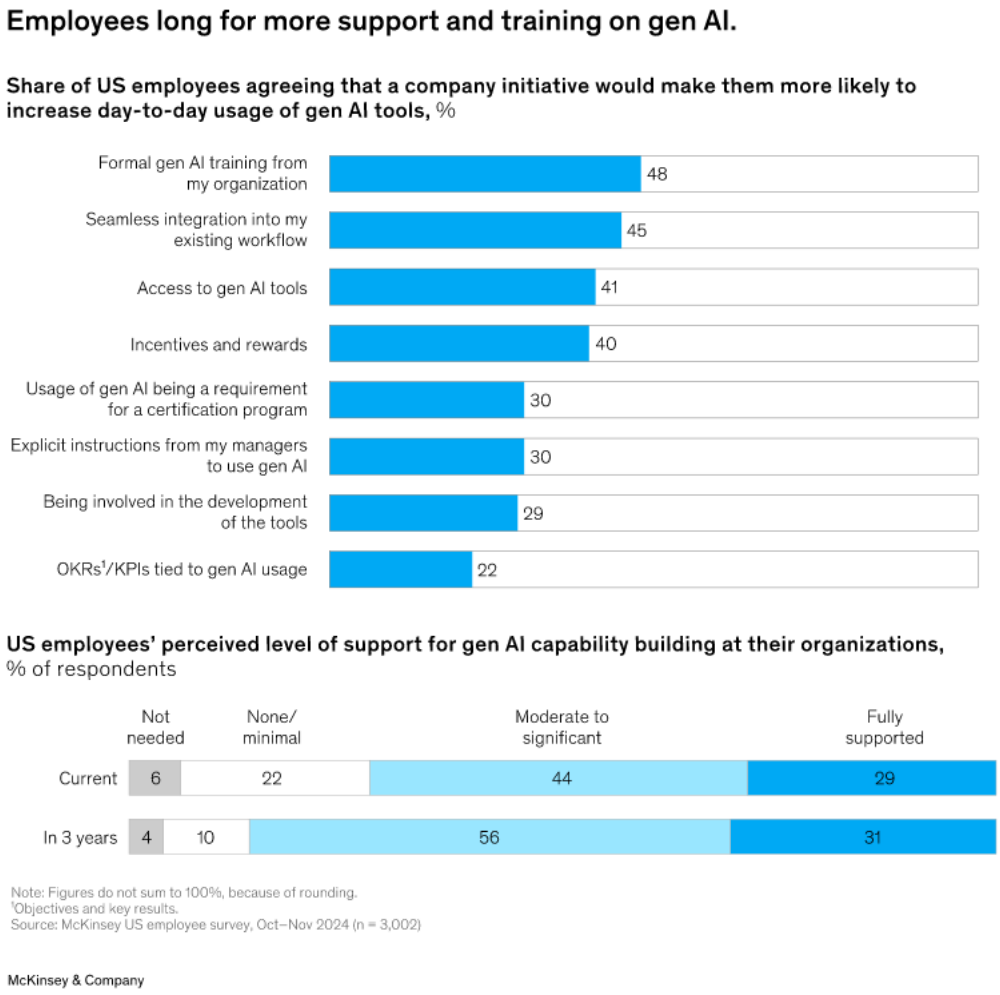
Survey of C-suite leaders about presence of a defined AI road map.



Note. McKinsey & Company report performed a survey for both C-suite leaders to understand where they believe their company is in terms of defining an AI road map. This has been adapted from *Superagency in the workplace: Empowering people to unlock AI's full potential* (Mayer et al., 2025)

Figure 5

Survey of employees to understand AI adoption and level of support from their company.



Note. This has been adapted from *Superagency in the workplace: Empowering people to unlock AI's full potential* (Mayer et al., 2025)

Given the unaddressed demand for AI tools in the workplace, employees are introducing shadow AI by independently procuring AI tools outside of the IT organization. Companies, however, are not equipped to handle shadow AI. They are struggling with users adopting the technology faster than they can understand it and figure out what to do about it. In a survey by Deloitte (2024), 45% of executives claim that AI is not on board agendas, while 79% admit that knowledge of AI is limited or less at the board level. In a survey by Gartner (2024), 88% of companies indicate that their AI leader is not at C-suite level and does not have sufficient authority. Without understanding the technology, organizations are unable to govern, take a stance on the changes, or educate their workforce. Consequently, they are delaying addressing AI within the organization because they are either unaware of its widespread use, in denial of the technology and its effects on their business or struggling to comprehend how it can benefit their business. Therefore, management is unsure what position or direction they should take with this technology for their business. Unlike shadow AI, introducing shadow IT systems requires a highly technical skillset and therefore was limited to a smaller group of employees. Consequently, companies had more time to educate themselves, make decisions, and enforce governance policies within their organization. The ability to control network traffic and enforce stricter administrative controls on corporate devices gave employers time to decide and govern the workplace according to their policies. On the contrary, shadow AI has a lower technical bar, a larger advocacy group, and high accessibility, giving company decision-makers less time to pivot and adapt to the new technology landscape within their companies.

There are risks associated with this slow-moving decision process, as employees begin using AI tools without any administrative oversight, organizational visibility, or governance structure. Consequently, companies need to proactively address AI with their workforce. To

mitigate these risks, decision-making needs to be expedited by increasing visibility into company operations, particularly understanding the extent of shadow AI exposure before an incident occurs. For instance, 15% of employees put company data in ChatGPT regularly, and one-third of these employees are entering sensitive data such as source code, internal business information, and personal identifiable information (LayerX, 2023). A notable example occurred in 2023, when Samsung experienced a data leak after an employee input sensitive source code into ChatGPT. In response, Samsung banned the use of AI tools such as ChatGPT and began developing their own internal assistant for company use (Petkauskas, 2023). However, measuring a company's exposure to shadow AI can be difficult, as employees fear sounding replaceable if they admit to using AI in their daily work. This fear can lead to an understatement of the actual exposure a company may have to shadow AI. Companies also need to consider other types of risks including non-compliance with industry standards and policies, for example a GDPR violation can cost up to 20 million euros (TeamViewer, 2024).

Addressing shadow AI

Considering the widespread use of AI tools and the growing presence of shadow AI within companies, it is necessary to address shadow AI. Before solutioning, the most important task is to understand the company's exposure to AI. To do this, it is essential to take an inventory of the AI usage throughout the company. This increases the visibility of technology infiltration within the organization to the leaders and decision makers within the organization. Also, this highlights the potential risks associated with the implementation of AI in various initiatives within the organization. This not only provides awareness of exposure to the leadership team, but also sets up the organization for upcoming changes by facilitating discussions at all levels of the company

during the discovery process. Once we have an AI inventory, we recommend these three pillars to address shadow AI:

Establish Trust in AI tools

First and foremost, trust in AI tools is a prerequisite for their adoption within an organization. According to Stradtman et al. (2024) , trust in AI is influenced by factors such as bias, hallucination, privacy violations, malicious intent, and IP infringement. Therefore, an organization must first believe that the tool is trustworthy enough to join the organization's trust circle, much like the process to hire any new employee. Once the level of trust is determined and any gaps identified, the full analysis must be documented. If trust is lacking, this must also be clearly documented for the organization. Hence, action rather than inaction is required in these uncertain situations to guide the whole organization. Moreover, trust in the output of the AI systems being used is just as important as the tool itself. Rigorous testing and verification of the tools are required to ensure that they meet the necessary standards of trust. Even if an AI tool is found to be useful to the business, its reliability and trust must be determined before establishing clear usage guidelines within an organization. The adoption of an AI tool with full faith in the input and output towards achieving the organization's vision, mission, goals, and values is important. Much like the organization vets and approves the skills and quality of decision making of new hires, it should do the same on its tools to create the trust required to effectively use the tools within the organization and maintain trust with their customers.

Establish a Governance Strategy

It is imperative to identify the appropriate people and define a governance strategy for the organization. To develop an effective governance strategy, it is essential to get representation

from both interested and impacted parties, as well as define clear roles and responsibilities for those involved. The completed AI inventory helps identify the right parties to involve in this step of the process. This should not be a small group behind closed-doors creating a strategy in a vacuum; instead, inputs from a wide range of knowledgeable and impacted persons should be incorporated. In this step, the roles and responsibilities of all those involved in decision-making and the decision hierarchy must be determined. It should also include various persons of authority for sponsorship and enforcement of the decisions.

This group needs to establish a governance framework by first defining the technology and acceptable usage for the organization. Followed by inspecting the impacts, strengthening governance and enforcement, and aligning on potential risks internal and external to the organization related to the adoption of AI. This should also take into account external upstream dependencies and downstream integrations with other software systems. Additionally, it should consider how people use the outputs from these systems in their decision-making processes.

The U.S. Department of Commerce established the National Institute of Standards and Technology (NIST) which regularly publishes standards, frameworks and guidelines for other professionals working in the science and technology sectors. This is especially important for companies or institutions that work with the U.S. federal government's departments and agencies which are required to be NIST compliant. Of particular note is the NIST AI Risk Management Framework NIST AI 600-1, released in July 2024. The Framework specifically addresses risks and proposes actions for managing these risks in conjunction with supplementary material such as the AI Risk Management Framework (AI RMF) (Tabassi, 2023). In NIST AI 600-1(2024), they suggest mitigating the risks and potential impacts of AI in many ways. For example, organizations must:

1) Establish governance in the form of terms of use and terms of service

2) Involve relevant individuals in the risk identification process

3) Verify that the downstream impacts are included in the identification and mitigation process

4) Establish policies, procedures, and processes for a safety-first mindset and minimizing negative impacts

5) Expand training material to include the safe handling of digital content and assessing content trustworthiness

The AI RMF provides an organizational structure of activities to carry out effective risk management and mitigation as seen in Figure 6. For example, in the process of adopting the AI RMF into their business, IBM used a 3-step process to adoption:

1) study the published AI RMF and associated playbook to understand the format and requirements and prepare themselves with a defined approach and scope out the next analysis phases,

2) map each part of the framework to IBM's internal policies, procedures, and design and discuss with leadership for buy-in

3) systematic analysis (Domin & Glaubitz, 2023)

As highlighted in the AI RMF, through the Map, Measure, Manage and Govern activities, companies will identify, set measurements and ensure that the risks applicable to their organizations are properly handled.

As an outcome of the governance strategy, the governance team should propose AI governance policies. These policies should be tied into the existing policies as much as possible. By linking new and old together, the enforcement and familiarity of policies allows for faster

adoption and employees are more receptive to the changes. This allows the alignment of people, processes and technologies within the organization towards adopting the new technology (Markham, 2024).

Figure 6

The AI Risk Management Framework's four core functions.

Note. Adapted from *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Tabassi, 2023)

Establish AI Leadership and Training

Lastly, companies need to step up and start addressing shadow AI and not ignore it or use the wait-and-see approach. An MIT study in 2022 found that 84% of executives are driven to adopt AI but only 19% are confident in leading their company to that point (Stackpole, 2022). Jason Wingard (2025) says that appointing AI leadership with C-suite authority and providing executives with AI education are key factors in successfully integrating AI.

By requiring leaders to get educated on the AI technologies available to their workers and in the public domain, leaders can understand the benefits and impacts on their businesses. Leaders can make informed decisions for the best direction for their company setting the stage for determining the course of action best suited for their company. By appointing a Chief AI Officer with C-suite authority, companies can ensure effective leadership of AI initiatives. This role focuses on both current and future implementations, as well as assessing the associated risks and benefits for the organization. The C-suite authority will ensure that AI within the organization receives the appropriate visibility within the long-term roadmap of the company and enforce the governance most aligned with the company's vision, mission and values.

Prior defined governance policies should outline acceptable use cases and establish company policies for the application of AI technology within the organization to provide employees with proper guidance. Once these are in place, then training programs should be developed for disseminating information on proper usage of AI technologies in the workplace. Training users on good and bad habits such as intellectual property risks and industry specific concerns will increase employee policy awareness and contribute to better educated workers. As mentioned earlier, nearly 80% of employees violated IT policies unknowingly in 2015 (Dittes et al., 2015). As Mayer et al. (2025) illustrates in Figure 5, employees want more formal training

and better integration of AI tools within the organization, with only 29% feeling fully supported by their organization. Bringing shadow AI out of the shadows into the light is possible given nearly half of US employees look forward to a company led formal training program and 41% are eager to gain access to company authorized AI tools (Figure 5). The formal training program would also include the organization's stance on the security, and appropriate use of AI tools within the business context. Thereby enforcing the business' best interests and educating employees on the safety and risks of technology.

Conclusion

Shadow AI tools will increase risk exposure if left unchecked especially through inaction or indecision of the company leaders. The new generation of AI tools are easy to access and offer increased productivity gains for employees, but at the same time increase risks to companies. Various factors, including lengthy IT approval processes, have led employees to find their own solutions to immediate issues. Thus shadow IT has transformed into shadow AI exposing companies to data leaks and many more risks in this information age. The widespread use and targeted advertising of AI tools towards the public has led to increased general adoption of the technology and calls for more sanctioned use of AI tools within the workplace. Employees are looking for guidelines, policies, and approved usage of the tools to boost performance at a rate faster than companies can decide what to do about them. The quicker organizations address this technology through training, governance, and awareness of risks, the sooner those risks can be mitigated, users can be informed, and governance can be implemented effectively. Users often are not aware of how much risk to the business there is for every AI interaction. As the technological landscape evolves, the companies need to establish and adopt a framework that is

flexible and addresses the ever-evolving risks. Governance, training, and awareness initiatives are essential for addressing Shadow AI effectively by educating employees about associated risks, acceptable use cases, and mitigating potential risks to the company. Appointing a strong AI leader is a crucial step in successfully implementing these strategies. As we advance into an era increasingly dominated by AI, the strategic steps outlined in this paper provide a roadmap for organizations to harness the full potential of AI while mitigating associated risks, thus paving the way for a future marked by technological excellence and business innovation.

References

Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., Aldairem, A., Alrashed, M., Bin Saleh, K., Badreldin, H. A., Al Yami, M. S., Al Harbi, S., & Albekairy, A. M. (2023). Revolutionizing healthcare: The role of artificial intelligence in clinical practice. *BMC Medical Education*, *23*(1), 689. https://doi.org/10.1186/s12909-023-04698-z

Apple. (2024, June 10). *Introducing Apple Intelligence for iPhone, iPad, and Mac*. Apple Newsroom. https://www.apple.com/newsroom/2024/06/introducing-apple-intelligence-for-iphone-ipad-and-mac/

Beimborn, D., & Palitza, M. (2013). Enterprise App Stores for Mobile Applications—Development of a Benefits Framework. *Proceedings of the Nineteenth Americas Conference on Information Systems*.

Bob-Jones, B., Newman, M., & Lyytinen, K. (2008). Picking Up the Pieces After a "Successful" Implementation: Networks, Coalitions and ERP Systems. *Proceedings of the Fourteenth Americas Conference on Information Systems*.

Chua, C. E. H., Storey, V. C., & Chen, L. (2014). Central IT or Shadow IT? Factors Shaping Users' Decision To Go Rogue With IT. *Thirty Fifth International Conference on Information Systems*.

Deloitte. (2024, October 8). *Deloitte: AI Slow to Gain Prominence in the Boardroom*. PR News Wire. https://www.prnewswire.com/news-releases/deloitte-ai-slow-to-gain-prominence-in-the-boardroom-302269876.html

Deniz, B. K., Gnanasambandam, C., Harrysson, M., Hussin, A., & Srivastava, S. (2023, June 27). *Unleash developer productivity with generative AI*. McKinsey.

https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/unleashing-developer-productivity-with-generative-ai

Dittes, S., Urbach, N., Ahlemann, F., Smolnik, S., & Müller, T. (2015). Why don't you stick to them? Understanding Factors influencing and Counter-Measures to combat deviant Behavior towards organizational IT standards. *Proceedings of the 12th International Conference*.

Domin, H., & Glaubitz, A. (2023, September 26). *IBM's Approach to Implementing the NIST AI RMF*. IBM. https://www.ibm.com/policy/blog/ibms-approach-to-implementing-the-nist-ai-rmf

Gartner. (2024, June 26). *Gartner Poll Finds 55% of Organizations Have an AI Board*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2024-06-26-gartner-poll-finds-55-percent-of-organizations-have-an-ai-board

Kalliamvakou, E. (2022, September 7). *Research: Quantifying GitHub Copilot's impact on developer productivity and happiness*. GitHub Blog. https://github.blog/news-insights/research/research-quantifying-github-copilots-impact-on-developer-productivity-and-happiness/

Kent, S., Houghton, L., & Kerr, D. V. (2013). *Affective Events Theory, Institutional Theory and feral Systems: How do they all Fit? 27*.

Klotz, S., Kopper, A., Westner, M., & Strahringer, S. (2019). Causing factors, outcomes, and governance of Shadow IT and business-managed IT: A systematic literature review. *International Journal of Information Systems and Project Management*, *7*(1), 15–43.

Kolmar, C. (2022, October 17). 26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace. *Zippia*. https://www.zippia.com/advice/byod-statistics/

LayerX. (2023). *Revealing the True Genai Data Exposure Risk*. https://go.layerxsecurity.com/hubfs/Research-Revealing-the-True-GenAI-Data-Exposure-Risk.pdf

Markham, I. (2024, November 15). Shadow AI Could Be Lurking in Your Enterprise. Here's What to Do About It. *The Wall Street Journal*. https://deloitte.wsj.com/riskandcompliance/shadow-ai-could-be-lurking-in-your-enterprise-heres-what-to-do-about-it-aef1a78d

Mayer, H., Yee, L., Chui, M., & Roberts, R. (2025, January 28). *Superagency in the workplace: Empowering people to unlock AI's full potential*. McKinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work

Mittal, N., Perricos, C., Schmidt, K., Sniderman, B., & Jarvis, D. (2024). *State of Generative AI in the Enterprise 2024* (pp. 1–31). https://www2.deloitte.com/us/en/pages/consulting/articles/state-of-generative-ai-in-enterprise.html

National Artificial Intelligence Initiative Act of 2020, 15 U.S.C. § 9401(3) (2020). https://www.congress.gov/bill/116th-congress/house-bill/6216

National Institute of Standards and Technology. (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (No. NIST AI 600-1; pp. 1–64). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

Petkauskas, V. (2023, May 8). *Lessons learned from ChatGPT's Samsung leak*. Cybernews. https://cybernews.com/security/chatgpt-samsung-leak-explained-lessons/

Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers & Security, 45*, 274–283. https://doi.org/10.1016/j.cose.2014.06.007

Software AG. (2024). *Chasing Shadows: Understanding and Managing Shadow AI* (pp. 1–8). Software AG.

Stackpole, B. (2022, October 5). *New report documents the business benefits of 'responsible AI.'* MIT Sloan School of Management. https://mitsloan.mit.edu/ideas-made-to-matter/new-report-documents-business-benefits-responsible-ai

Stradtman, B., Snaidauf, D., & Conti, J. (2024). *Trustworthy AI Services from Deloitte and IBM* (pp. 1–3). Deloitte & IBM.

Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (No. NIST AI 100-1; p. NIST AI 100-1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.AI.100-1

TeamViewer. (2024, February 6). *A closer look at the difference between shadow AI and shadow IT*. TeamViewer. https://www.teamviewer.com/en-us/insights/difference-between-shadow-ai-and-shadow-it/

The Conference Board. (2023, September 13). *Majority of US Workers Are Already Using Generative AI Tools*. The Conference Board. https://www.conference-board.org/press/us-workers-and-generative-ai

Wingard, J. (2025, February 18). *Leaders Don't Get AI: 3 Ways To Close The Gap*. Forbes. https://www.forbes.com/sites/jasonwingard/2025/02/18/leaders-dont-get-ai--3-ways-to-close-the-gap/