Maximize The Benefits Of AI While Minimizing The Risks

FEATURING RESEARCH FROM FORRESTER

Bring-Your-Own-AI Hits The Enterprise

MAXIMIZE THE BENEFITS OF AI WHILE MINIMIZING THE RISKS

Rapidly rapidly develop and expand your AI/ML models with open source

Welcome/introduction

"Bring your own AI"(BYOAI) has been identified as the next big BYO IT topic by Forrester Research. It refers to employees' use of external AI resources, including generative AI such as ChatGPT, AI-infused software, AI-creation tools, and cloud-based APIs, that your business doesn't own to accomplish company-related business.

BYOAI introduces regulatory, governance, privacy, third-party vendor, and security challenges that businesses must now manage to maximize the benefits of AI while limiting unapproved usage, known as "shadow AI".

IN THIS DOCUMENT

Maximize The Benefits Of AI While Minimizing The Risks

Research From Forrester: Bring-Your-Own-AI Hits The Enterprise

About Red Hat

The "Bring Your Own AI hits the enterprise" report from Forrester Research outlines best practices to help CIOs effectively manage it at scale. It covers:

- Challenges BYOAI brings to the traditional CIO approach to BYO.
- How to craft a modern BYOAI management policy.

Red Hat® OpenShift® AI is designed to help. It provides an open source platform for building, training, testing and serving models for your own AI-enabled applications. With it, organizations can rapidly develop their AI/ML models, expanding further by adding open source tools and Red Hat technology partner solutions.

BEST PRACTICE REPORT

Bring-Your-Own-AI Hits The Enterprise

Key Policies To Maximize The Benefit Of Bring-Your-Own-AI While Minimizing The Risks

September 11, 2023

By Andrew Hewitt, John Brand with Matthew Guarini, J. P. Gownder, Jeff Pollard, Enza Iannopollo, Michele Goetz, Anna Synakh, Ian McPherson

FORRESTER®

Summary

The next wave of “bring-your-own” has arrived, and its name is bring-your-own-AI (BYOAI). Whether it’s generative AI tools like ChatGPT, AI-infused software, or AI-creation tools, employees are already using consumer AI services that your business doesn’t own. CIOs and other business leaders must develop a management strategy that maximizes the benefits and limits the risks of BYOAI. This report outlines best practices for CIOs overseeing BYOAI to help your technology organization effectively manage it at scale.

Additional resources are available in the online version of this report.

BYOAI Challenges The Traditional CIO Approach To "Bring-Your-Own"

AI is the most transformative technology to hit the enterprise since mobile. While AI has steadily evolved for decades, the astronomic rise of generative AI — ChatGPT gained 1 billion page views in just four months — is accelerating AI's impact on the future of work. Employees of all kinds are already experimenting with generative AI: from developers to visual designers to sales teams and marketers. While companies like Bain & Company, Buzzfeed, and Coca-Cola are aggressively integrating ChatGPT into key services, much of today's AI usage happens on publicly available consumer services — like ChatGPT, DALL-E2, and Midjourney. However, employees won't just bring generative AI to work, they'll also use other forms of AI, such as AI-infused software, AI-creation tools, and cloud-based APIs, all of which fall under the purview of BYOAI. We define BYOAI as:

An employee using any form of external AI service to accomplish company-related business regardless of whether it's sanctioned by the business.

The rise of BYOAI introduces regulatory, governance, privacy, third-party vendor, and security challenges that businesses must now manage. While some companies like Amazon, Apple, Citigroup, and Samsung announced restricted or outright bans of ChatGPT, BYOAI will become as ubiquitous as computers, mobile, and cloud are today (see Figure 1 and see Figure 2). As a Biden administration senior official recently commented, "AI is coming into virtually every part of the public mission." CIOs and other leaders must create a formal BYOAI management strategy to maximize the benefits of AI while limiting unapproved usage, also known as shadow AI. While many are accustomed to enforcing usage policies for BYOD, managing BYOAI risk will prove especially difficult. Why?

- **The CIO does not fully own AI.** While the CIO remains wholly responsible for employee smartphones and mobile apps, data science teams and chief AI officers have driven AI strategy to date. As AI becomes more mainstream, CIOs, CTOs, and EA pros will be responsible for AI enablement and management, but with close collaboration with HR, security and risk, data science, and other leaders to develop use cases, enforce proper usage, deliver business outcomes, and update BYOAI policies and guidelines.
- **BYOAI is much riskier.** Managing BYOD requires a usage policy and technical controls, but BYOAI carries more risk. Just 19% of AI decision-makers indicate they are less concerned about employees using unsanctioned AI in their work,

according to Forrester's July 2023 Artificial Intelligence Pulse Survey. BYOAI attempts to harness new forms of intelligence to augment employee skills, while BYOD is primarily concerned with enabling employees to use a personal device securely for work. This introduces multiple, complex risks that simply don't exist for BYOD, including ethical AI usage, AI literacy challenges, and data poisoning, among others.

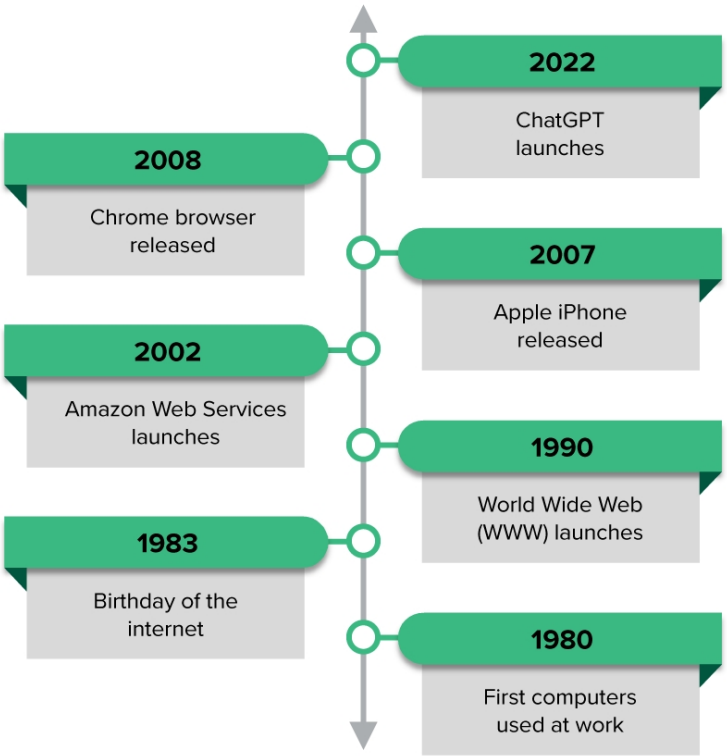
- **Security tools and practices around AI are immature.** A plethora of mature tools exist today to effectively manage the risk of BYOD, from mobile device management to mobile threat defense. While some controls such as API security, privacy, and governance technologies are starting to appear to manage generative AI, many organizations lack the vendor relationships, technologies, and skills to manage BYOAI effectively. Most security tools also lack sophisticated observability, management, and monitoring capabilities for BYOAI solutions, a major gap that needs to close before security and risk management teams feel comfortable with employees using AI.
- **BYOAI is widely (and often freely) available and evolving quickly.** The early days of mobile featured two dominant operating systems (OS) and thousands of mobile apps — all of which have standard management frameworks. Because AI is accessible across multiple OS, devices, browsers, APIs, and app stores, a network ban will be ineffective, complicating management for CIOs. Bans also cost technology teams valuable data, because it forces use "underground," which eliminates opportunities to learn about potential use cases. Vendors may also enlighten third-party consumer and business apps with AI features, which means currently deployed — and any personally owned preapproved apps — in use will now expose the enterprise to more risk.
- **The CIO is now responsible for digital employee experience.** CIOs during the mobile era were primarily concerned with IT management, security, and cost. This is no longer true. According to Forrester's Future Fit Survey, 2023, 62% of CIO business and technology decision-makers indicate that improving IT capabilities to improve employee experience is a high priority IT objective over the next 12 months. While the CIO is responsible for enabling BYOAI, they must cede control of the user experience to a consumer service that they can't influence. Ensuring a strong DEX will require CIOs to thoroughly investigate how and if consumer AI services support approved enterprise use cases and DEX initiatives, which is not an easy task.

Figure 1

AI Will Become A Staple Of The Modern Work Life

Fast-forward to 2022:

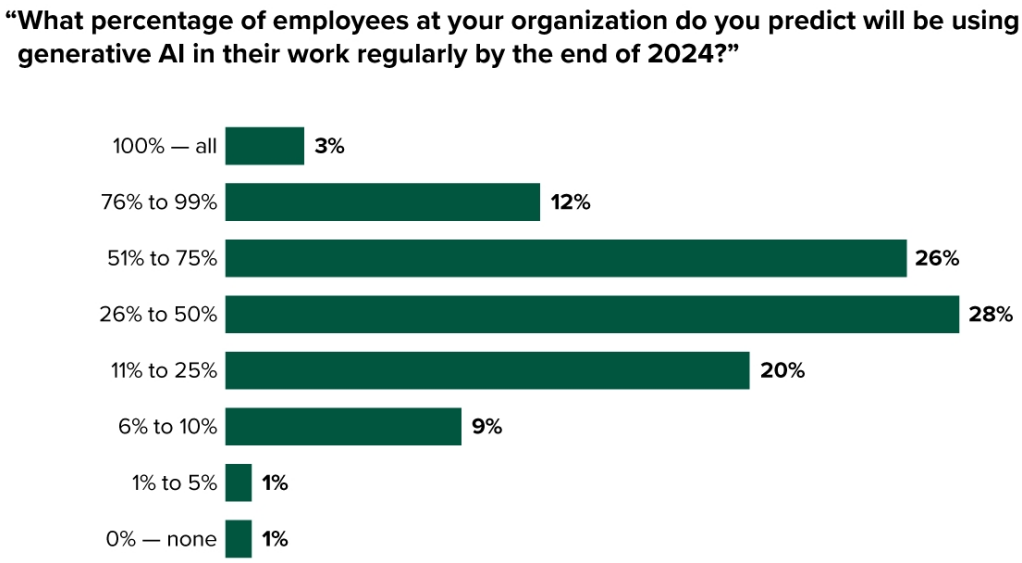
89% use a computer at least weekly for work[1]
22% agree that their organization tracks, monitors, or logs how they use the internet[2]
55% say the smartphone they use for work is personally owned[3]
53% say their most frequently used browser for work is Google Chrome[4]
82% of enterprise cloud decision-makers are adopting public cloud[5]



1. Base: 5,606 global respondents employed full time
2. Base: 4,974 global respondents full/part time who use a computer at least weekly for work
3. Base: 3,417 global respondents employee full time/part time whose organization supports a BYOD policy. Source: Forrester's Workforce Survey, 2023
4. Base: 9,213 global respondents employee full time/part time who use a computer at least weekly for work. Source: Forrester's Workforce Survey, 2022
5. Base: 2,162 global enterprise cloud decision-makers. Source: Forrester's Infrastructure Cloud Survey, 2022

Figure 2

Many Employees Will Use Generative AI By The End Of 2024



Base: 269 global AI decision-makers
Source: Forrester's July 2023 Artificial Intelligence Pulse Survey

Craft A Modern Bring-Your-Own-AI Management Policy

Given the risks associated with BYOAI, most companies are updating policies for generative AI while they build their own corporate-approved AI capabilities, also known as a "two-track strategy" (see Figure 3). Why? 1) The inherent risks of BYOAI make enterprise AI more attractive, and 2) policies don't have a track record of success. Acceptable usage documents are often too techy, draconian, and devoid of business context. To test our theory, we asked ChatGPT to craft a policy for BYOAI usage. While it successfully produced a policy template, it followed an old-school approach to policy development, missing a few key elements, such as AI literacy, use cases, and a focus on employee experience.

Given that BYOD policies were historically ineffective, does that mean CIOs should do nothing to address BYOAI? No, because employees will still use BYOAI regardless — 10% of workers who use a computer at least weekly for work purposes admit they

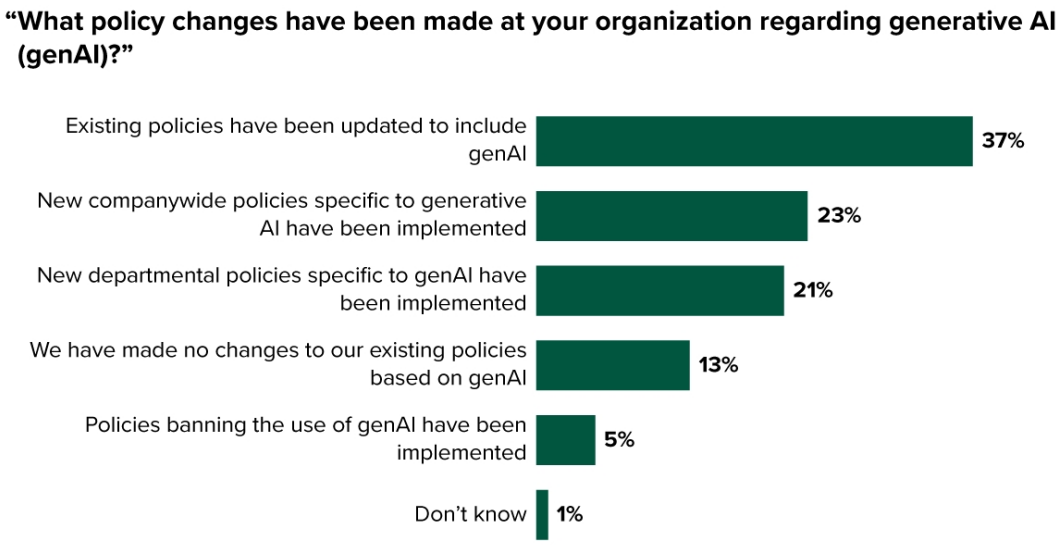
would circumvent IT security policies if they knew how to do it, according to Forrester's 2023 data. With limited security controls available today, it's not a question of *if* employees will BYOAI, but *when* and *how*. While policies are still necessary, CIOs must modernize them for BYOAI. This modern BYOAI policy should (see Figure 4):

- **Align with AI governance efforts.** Forrester's official AI governance model is built upon four pillars: purpose, culture, action, and assessment. The CIO should work closely with the AI governance professionals to apply this framework to the BYOAI policy. This includes ethical as well as security, regulatory, training, and commercial considerations. For example, common goals of AI governance are to "do no harm" and "ensure that AI is always under supervisory control." CIOs can include this type of language upfront in their BYOAI policy documents to draw a connection to responsible AI usage.
- **Outline key employee use cases in an empathetic tone.** Prior BYOD policies failed because they lacked employee empathy. Most overly focused on restrictions without helping employees answer the question: "How can this policy benefit me?" BYOAI policies should include a list of approved use cases and roles that ground the policy within a clear business context while inspiring specific roles to reimagine how they accomplish their work. As one Forrester IT leader put it, "We need to become the department of 'know,' not 'no.'"
- **List proscriptions and enforcement actions.** Create a list of restrictions that clearly define what employees can and cannot do with AI. Offer an example for each restriction outlined. These policies should cover four areas: security and privacy, literacy, usage, and support (see Figure 5 and see Figure 6). Companies can use tools like Credo AI to help generate AI policies and controls to mitigate risk.
- **Offer non-punitive guidelines.** In contrast to the restrictions, guidelines carry no penalty for noncompliance. They help inform and educate employees about making better work and life choices with BYOAI. These guidelines should reiterate and closely align with cultural goals of the AI governance framework. For example, the city of Boston's AI policy provides guidelines such as, "Think about how racial and ethnic minorities, women, nonbinary, people with disability or others could be portrayed or impacted by the content [that AI produces]."
- **Provide links to training and development resources.** Because CIOs play such an important role in supporting the digital employee experience, they must take a more proactive role in helping employees to develop a higher robotics quotient (RQ), a key requirement for augmenting human skills with AI. CIOs should lean on

Forrester's RQ framework and DEX teams to lead change management, develop training and certifications, offer workshops, and measure satisfaction.

Figure 3

Organizations Are Addressing GenAI Policy In Numerous Ways



Base: 275 global AI decision-makers
Source: Forrester's July 2023 Artificial Intelligence Pulse Survey

Figure 4

Twelve BYOAI Policy Sections, According To ChatGPT

Bring-your-own-AI policy
1. Purpose
2. Scope
3. Eligibility
4. Data security and privacy
5. Compliance
6. Data backup and recovery
7. Training and support
8. Conflicts of interest
9. Termination of use
10. Liability
11. Policy violations
12. Policy review

By implementing this bring-your-own-AI policy, your business aims to strike a balance between enabling employees to leverage their AI tools effectively while safeguarding data, maintaining compliance, and promoting a secure work environment.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 5

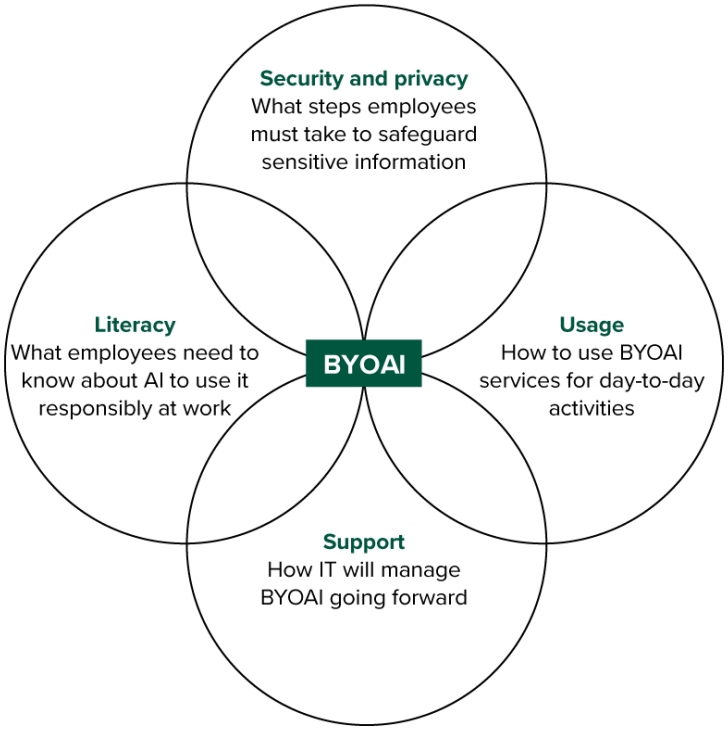
Core Elements Of A BYOAI Usage Policy

Overview	Policy details	Guidelines	Enforcement
Mission statement	Security	Recommendations	Noncompliance
Scope	Literacy	Training support	Whistleblower
Eligibility	Usage		Liability
Continuous improvement	Support		Ongoing management

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 6

BYOAI Policy Details Should Cover Four Key Areas



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

CIOs Must Lead The Effort To Drive Adoption Of BYOAI Policies

Writing a bring-your-own policy is only one step — communicating its value, enforcing compliance, and revising it as necessary is equally important. To effectively balance BYOAI adoption, CIOs should:

- **Focus heavily on communication.** Communication must be clear, empathetic, and reinforced regularly. Most importantly, CIOs must remain highly visible in these discussions and not hide behind corporate policy statements. CIOs should lean heavily on internal communications teams to ensure employees understand the BYOAI policy, feel they can provide feedback on it, and receive relevant updates. CIOs should use a mix of communication metrics to gauge BYOAI awareness, including viewership, adoption, usage patterns, and external benchmarks.
- **Emphasize the balance between AI opportunity and threat.** CIOs must effectively communicate the benefits and risks of BYOAI to the workforce. Like the early days of BYOD, what works best is framing the benefits and risks from the perspective of the employee. Employees need to know: "Why does this matter to me?" From a benefits perspective, that could be enabling a marketer to write copy at twice the speed. From a risk perspective, that could be a coworker sharing your personal details on a BYOAI service, compromising your own privacy.
- **Actively review and refine BYOAI policies.** Working closely with AI governance pros, employees, and other business leaders, assess and review BYOAI policies in response to new consumer AI releases, enterprise AI development, evolving AI regulations, employee feedback, observability metrics, and predefined business outcomes. Continual assessment is one of the four key pillars of effective AI governance, and that applies to the CIO's office as well. For example, the city of Seattle's CTO Jim Loter released the city's interim policy in April 2023, with plans to revise the policy by October 31, 2023.
- **Pay special attention to privacy risk.** Privacy is the number one concern of leaders when using artificial intelligence. AI systems can potentially interact with sensitive information in three ways: in the training model itself, in corporate data sets, and in the output. All of these are potential risks in a BYOAI program. Forrester's A Privacy Primer On Generative AI Governance suggests giving employees a refresher on personal or sensitive data categories to help them better manage the risk.
- **Without forgetting about the larger risk landscape.** Security, financial and regulatory risks will continue to develop as BYOAI becomes more mainstream. Each will require its own auditing and observability capabilities to monitor

effectively. Continue to survey the security landscape for tools that will provide better telemetry and observability, while interfacing with governance, risk, and compliance leaders to respond to changing regulations.

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER




Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

ABOUT RED HAT

We're the world's leading provider of enterprise open source solutions—including Linux, cloud, container, and Kubernetes. We deliver hardened solutions that make it easier for enterprises to work across platforms and environments, from the core datacenter to the network edge.

Red Hat® OpenShift® AI is an AI-focused portfolio that provides tools to train, tune, serve, monitor, and manage AI/ML experiments and models on Red Hat OpenShift. Bring data scientists, developers, and IT together on a unified platform to deliver AI-enabled applications faster.