LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

BRING YOUR OWN AI (BYOAI) IN THE WORKPLACE: PATTERNS, PITFALLS, AND THE BYOAI-GOV™ FRAMEWORK FOR BEHAVIOR-AWARE GOVERNANCE

Thamburaj Anthuvan*, Dr. Sunitha Prabhuram[2], Ganesh Raju[3], Dr. Kajal Maheshwari[4], Aditya Mishra[5]

[1]PCET's S.B. Patil Institute of Management, Pune, Maharashtra, India
[2]School of Business, Manipal Academy of Higher Education
[3]Akshaya Emerging Technologies (industry affiliation)
[4]PCET's S.B. Patil Institute of Management, Pune, Maharashtra, India
[5]Indian Institute of Management Calcutta (IIM Calcutta), Kolkata, West Bengal, India

Abstract : The informal use of generative artificial intelligence (AI) tools such as ChatGPT, Copilot, and Gemini is spreading rapidly across workplaces, outpacing institutional governance. This trend—known as Bring Your Own AI (BYOAI)—creates tensions between innovation, trust, and regulatory oversight. This study examines how organizations can manage unsanctioned AI use through a two-phase approach: a systematic review of 45 peer-reviewed studies and a multi-region survey of 345 professionals across business, healthcare, education, and government sectors. Findings reveal six behavioral user archetypes and four organizational governance postures shaped by risk perception and task sensitivity. The paper proposes the BYOAI-Gov™ framework, a behavior-aware model that integrates task-risk zoning (Enable, Regulate, Restrict) with a four-level maturity scale. It reframes informal AI use as a governable organizational behavior and provides practical guidance for balancing innovation with accountability and ethical assurance in decentralized digital workplaces.

Keywords : BYOAI, generative AI, workplace governance, organizational behavior, governance framework

1. Introduction

The adoption of tools like ChatGPT, Copilot, and Gemini is no longer driven solely by formal IT rollouts. Increasingly, employees are using these tools independently—logging in via personal accounts, often on personal devices, to complete work tasks. This rising trend, referred to as Bring Your Own AI (BYOAI), echoes the earlier BYOD movement but introduces new complexities around control, trust, and accountability (Raju, 2024; van der Meulen & Wixom, 2024). Unlike sanctioned enterprise deployments, BYOAI infiltrates the workplace informally—manifesting in slide decks, draft emails, reports, or code snippets—frequently without institutional oversight or disclosure.

A parallel phenomenon, Shadow AI, further deepens these concerns. It includes unauthorized scripts, APIs, or third-party plugins that bypass official IT channels altogether (Chin et al., 2025; Puthal et al., 2025). Together, these behaviors are not isolated anomalies but indicators of a structural shift in how work is performed—and they raise urgent questions about ethics, risk, and governance (Dwivedi et al., 2019; Wang et al., 2023). Why is this happening? Many employees seek to work smarter, circumvent slow processes, or compensate for vague AI guidelines. Often, they act quietly—not out of rebellion, but necessity. Others hesitate, uncertain of what is permitted or safe. This mix of quiet adoption and silent resistance signals a deeper misalignment: traditional top-down governance models fail to reflect the lived realities of AI use in the workplace (Morley et al., 2023; Ghosh, Saini, & Barad, 2025).

While earlier frameworks such as AI-C2C (Anthuvan & Maheshwari, 2025) and AI4People (Floridi et al., 2018) provide valuable normative direction, they are typically policy-heavy and overlook decentralized, behavior-driven adoption. Similarly, foundational theories such as the Unified Theory of Acceptance and Use of Technology (UTAUT; Venkatesh, Morris, Davis, & Davis, 2003) and structuration theory

(Orlikowski, 2000) illuminate individual–technology interactions but rarely address governance under conditions of informal, user-initiated tool use. This paper addresses that conceptual gap by applying a bottom-up lens—one that values experimentation, recognizes uncertainty, and emphasizes psychological safety and trust. Specifically, it aims to:

- Understand how employees adopt or avoid generative AI tools at work.
- Identify the behavioral archetypes and organizational postures shaping this engagement.
- Propose a behavior-sensitive governance model that enables responsible use through segmentation, practical enablement, and contextual oversight.

In doing so, this work repositions BYOAI not as a compliance threat but as a governable phenomenon—one that demands graduated, behavior-aware frameworks attuned to the hybrid realities of digital work.

2. Theoretical and Conceptual Foundations

Understanding the informal spread of generative AI tools like ChatGPT or Copilot requires a behavioral lens that accounts for how and why employees adopt, avoid, or bypass formal systems. The Unified Theory of Acceptance and Use of Technology (UTAUT) offers a foundational explanation for informal GenAI use by highlighting constructs such as performance expectancy, effort expectancy, and facilitating conditions (Orlikowski, 2000). In practice, our respondents cited ease of use, peer modeling, and lack of access to sanctioned tools as key drivers, consistent with recent findings on technology adoption in loosely governed environments (Jain, Garg, & Khera, 2022). Extensions of UTAUT further suggest that trust mediates adoption, especially when institutional direction is unclear (Korzyński, Costa e Silva, Górska, & Mazurek, 2024). This explains why certain users ("AI Champions") act with confidence while others ("Silent Starters") proceed with caution. Simultaneously, Shadow IT theory situates BYOAI within a broader pattern of user-driven innovation in response to bureaucratic inertia. Employees bypass formal channels not out of defiance, but to close usability gaps or overcome restrictions (Silic & Back, 2014). However, GenAI tools amplify latent risks—hallucinations, data leakage, or flawed content—that can undermine trust and decision-making in ways traditional IT governance has not accounted for (Chin et al., 2025; Puthal et al., 2025; Zhao, Dai, & Jun, 2025).

Rather than viewing such behaviors as violations, human capital theory helps recast BYOAI as a form of informal upskilling. Employees are not merely seeking shortcuts—they are often engaging in self-initiated learning, adapting to technological shifts, and striving to stay professionally agile (Deci & Ryan, 2000; Yusuf et al., 2024). Many users treat GenAI tools as co-pilots for learning, enhancing fluency through experimentation, particularly in the absence of formal training (Jaiswal, Arun, & Varma, 2021; Morandini et al., 2023). This framing is crucial as it surfaces the disconnect between traditional control-oriented governance and the lived realities of decentralized AI use. The BYOAI phenomenon is not random; it reflects a behavioral logic shaped by opportunity, psychological safety, and evolving norms (Edmondson & Lei, 2014; Bankins et al., 2023). Accordingly, governance models must evolve—moving beyond rigid compliance to embrace segmentation, enablement, and trust-building. This theoretical scaffolding directly informs the behavior-aware governance framework presented in this study.

3. Methodology

To address the behavioral, organizational, and governance dimensions of informal generative AI adoption in the workplace, this study adopted a multi-method design comprising a systematic literature review (SLR) and a multi-region survey. This design ensured both conceptual depth and empirical breadth, aligning with recommendations for governance-model development in socio-technical contexts (Gregor, 2006; Vom Brocke et al., 2015). Each component contributed to a layered understanding of BYOAI behavior and informed the structure of the proposed BYOAI-Gov™ (Bring Your Own AI Governance) framework—hereafter referred to as BYOAI-Gov.

3.1 Systematic Literature Review

The SLR followed PRISMA 2020 guidelines (Page et al., 2021) and adhered to methodological standards in information systems and digital governance research (Vom Brocke et al., 2015). Four databases—Scopus, Web of Science, IEEE Xplore, and Google Scholar—were queried using Boolean combinations of terms including "Bring Your Own AI," "shadow AI," "unsanctioned AI," "informal technology adoption," and "AI governance." The search was limited to peer-reviewed articles published between January 2019 and March 2025 in English. After removing duplicates, all titles and abstracts were screened, followed by full-text assessment based on predefined inclusion and exclusion criteria.

Inclusion criteria:

- Empirical or conceptual studies focused on workplace settings
- Studies examining informal or unauthorized use of AI or digital tools
- Articles addressing governance, adoption behavior, or risk frameworks

Exclusion criteria:

- Non-workplace contexts (e.g., K–12 education, consumer-only applications)
- Studies focused solely on technical performance or algorithm design
- Commentaries, editorials, and non-peer-reviewed literature

Following this process, 45 eligible studies were retained and coded. These were grouped into six thematic clusters: governance gaps, access pathways, behavioral dynamics, risk perception, policy responses, and trust models. The synthesis approach combined deductive theory-based coding (drawing on UTAUT, structuration theory, and responsible innovation) with inductive clustering to surface new governance-relevant constructs. This dual-mode synthesis enabled theoretical triangulation with primary survey data. The screening and inclusion flow is detailed in Figure 1 (PRISMA diagram).

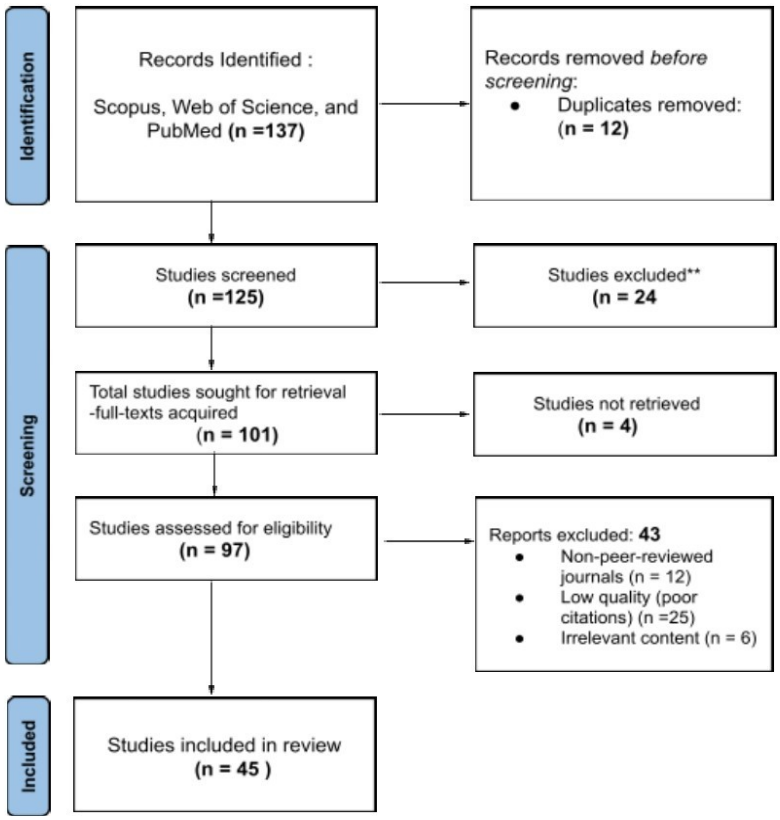

Figure 1. PRISMA Flowchart of BYOAI Literature Review
This diagram illustrates the identification, screening, and inclusion of 45 studies from 137 records, based on PRISMA 2020 guidelines.

3.2 Survey Design, Deployment, and Analysis

To complement the literature synthesis and capture real-world insights into BYOAI behavior, a 15-item structured survey instrument was developed. Its design was anchored in the theoretical constructs of the Unified Theory of Acceptance and Use of Technology (Orlikowski, 2000), Shadow IT behavior (Silic & Back, 2014), and contemporary digital governance frameworks (Morley et al., 2023; Organisation for Economic Co-operation and Development [OECD], 2019). Demographic segmentation followed ESOMAR standards (ESOMAR, 2023) and global role-taxonomy guidelines (Advance CTE, 2024; United Nations, 2024). Content and face validity were established through iterative reviews by five domain experts in AI policy, organizational behavior, and ethics. A pilot test with 50 participants confirmed item clarity, logical flow, and internal reliability (Cronbach's alpha > 0.70), with minor refinements applied prior to deployment.

The finalized survey was disseminated online using convenience and snowball sampling techniques between March and May 2025. A total of 345 valid responses were collected across four regions—India, the United States, South Africa, and the United Kingdom—spanning key sectors such as healthcare, information technology, academia, government, and finance. Participation was voluntary, anonymous, and non-incentivized to reduce bias and encourage openness. Data analysis was conducted using Python (v3.10) and R (v4.2), incorporating both descriptive and inferential statistics. Key metrics included adoption frequency, access pathways, and perceived governance gaps. Non-parametric tests (Kruskal–Wallis and Wilcoxon rank-sum) were used to assess group-level differences in risk perception. A binomial logistic regression model was applied to identify predictors of tool avoidance. Open-text responses were processed using VADER sentiment analysis to

capture emotional tone, while cross-tabulations revealed patterns across roles, domains, and governance expectations.

3.3 Framework Synthesis

The BYOAI-Gov Framework was developed through a three-stage synthesis process combining descriptive coding, analytical abstraction, and thematic integration—aligned with constructivist model-building practices (Gregor, 2006; Noblit & Hare, 1988). Descriptive coding captured patterns across both the literature and survey—such as informal access norms, usage motivations, and governance expectations. Analytical coding then examined underlying tensions, particularly between control and enablement, drawing on sociotechnical perspectives (Scott, 2013; Pavlou & El Sawy, 2010). This dual-mode approach yielded seven core governance pillars: leadership, trust, skills, transparency, participation, contextual fit, and continuous oversight. These pillars reflect both individual-level behavior and institutional responses, offering a flexible framework grounded in task-risk alignment and behavioral segmentation. Unlike traditional compliance-centric models, BYOAI-Gov emphasizes adaptive, trust-centered oversight aligned with contemporary digital-governance thinking (Yeung, 2018).

4. Results

The findings are presented in two integrated parts, aligned with the study's mixed-method design. The first synthesizes insights from the systematic literature review, uncovering behavioral drivers and governance gaps surrounding BYOAI. The second analyzes data from a multi-region survey, offering empirical insights into employee usage patterns, risk perceptions, and organizational responses. Together, these complementary strands inform the design and logic of the proposed BYOAI-Gov framework.

4.1 Insights from the Systematic Literature Review

The systematic literature review identified 45 peer-reviewed studies across management, public policy, and information systems, revealing distinct but interlinked insights about the rise of BYOAI. Rather than treating themes in isolation, the findings were interpreted through a behavioral-governance lens to surface deeper systemic patterns.

First, multiple studies emphasized the mismatch between rapid tool adoption and slow policy adaptation (Dwivedi et al., 2019; Roberts & Oosterom, 2024). Informal GenAI use was driven largely by perceived productivity gains and lack of accessible alternatives—reflecting UTAUT's constructs of performance expectancy and facilitating conditions (Orlikowski, 2000; Jain, Garg, & Khera, 2022). However, such use often occurred without organizational clarity, creating ambiguity about what constitutes acceptable experimentation versus risky overreach (Morley et al., 2023; Korzyński, Costa e Silva, Górska, & Mazurek, 2024). Second, a recurring insight across governance-focused papers was the absence of segmentation in enterprise risk strategies. Most models were designed for formalized AI systems—not adaptive responses to employee-level tool experimentation. This created regulatory blind spots and left organizations with either excessive restrictions or passive tolerance (Ghosh, Saini, & Barad, 2025; Organisation for Economic Co-operation and Development [OECD], 2019). Trust, transparency, and contextual fit emerged as under-addressed dimensions.

Together, the literature signals a shift from purely technical oversight to behavior-aware governance—a view that treats informal AI adoption not as deviance but as a coping mechanism within structurally misaligned systems (Silic & Back, 2014; Edmondson & Lei, 2014). These insights directly informed the behavioral segmentation and task-risk stratification embedded in the BYOAI-Gov Framework.

4.2 Insights from the Multi-Region Survey:

Building on the survey methodology detailed in Section 3.2, this section presents the results of a structured 15-item instrument deployed across four countries (n = 345). The

survey aimed to examine how professionals access and use generative AI (GenAI) tools in the workplace, the extent of informal or unsanctioned use (BYOAI), perceived risks, and expectations from governance systems. Analysis was grounded in three key theoretical lenses—Shadow IT theory (Silic & Back, 2014), structuration theory (Orlikowski, 2000), and the Unified Theory of Acceptance and Use of Technology (UTAUT; Venkatesh, Morris, Davis, & Davis, 2003). Findings are presented in four interlinked parts: (i) behavioral user archetypes; (ii) organizational governance postures; (iii) risk perception and avoidance behavior; and (iv) demand for support structures. Each subsection triangulates descriptive statistics, inferential testing, and theory-informed interpretation. Tables and figures referenced below reflect both structured responses and open-text thematic coding.

4.2.1 Respondent Profile and Contextual Validity

To ensure contextual relevance, the study targeted digitally active professionals across sectors where generative AI integration is most salient. The final sample (n = 345) included participants from India, the United States, South Africa, and the United Kingdom—regions that together accounted for over 90% of responses. The cohort was primarily composed of mid-to-senior professionals in AI-adjacent domains such as marketing, IT, HR, and sales, with a dominant age range of 35–54 years. While gender distribution was male-skewed, it remained broadly reflective of enterprise leadership demographics. These respondent characteristics provide a valid foundation for interpreting behavioral patterns around GenAI adoption and governance preferences in real-world enterprise contexts. A summary of the demographic distribution is presented in Table 1.

Table 1. Summary Demographic Profile of Survey Respondents (n = 345)

Variable	**Top Categories**	**% of Respondents**
Geography	India, United States, South Africa, United Kingdom	Top 4 = 90.2%
Age Group	25–34, 35–44, 45–54	35–54 = 58.6%
Gender	Male, Female	Male = 69.6%
Role Level	Mid- to Senior-Level Professionals	~80%
Function	Marketing, IT, HR, Sales	Top 4 = 52.5%

Note: IT = Information Technology; HR = Human Resources.

4.2.2 Patterns of AI Use

The survey reveals widespread informal adoption of generative AI tools within enterprise contexts, often occurring outside official IT channels. A substantial majority of respondents accessed AI platforms via personal or mixed accounts, with only a minority operating exclusively through organization-provided access. This highlights the porous boundary between sanctioned and unsanctioned technology use in daily workflows. Usage was not limited to a single platform—respondents reported employing a range of tools, led by ChatGPT, followed by Google Gemini and Microsoft Copilot. This reflects an emerging multitool environment shaped by functional preferences and user familiarity with large language models. Notably, AI applications extended well beyond content generation. Tasks such as email drafting, presentation design, summarization, ideation, data analysis, and even coding point to a transition from exploratory use to strategic task alignment. These patterns suggest that GenAI tools are being embedded into both creative and operational dimensions of work. Table 2 summarizes respondents' access modes, tool preferences, and task-specific usage, laying the foundation for the behavioral archetypes analyzed in the next section.

Table 2. AI Access Modes, Tool Usage, and Supported Task Types (n = 345)

A. Access Method		
Access Method	**No. of Respondents**	**% of Respondents**
Personal account (unreimbursed)	143	41.40%
Both official and personal accounts	93	27.00%
Organization-provided official access	91	26.40%
Prefer not to disclose	13	3.80%
Personally paid, later reimbursed by organization	5	1.40%
B. AI Tools Used Most Frequently		
AI Tool	**No. of Respondents**	**% of Respondents**
ChatGPT	304	88.10%
Google Gemini	173	50.10%
Microsoft Copilot	128	37.10%
Others	70	20.30%
DeepSeek	69	20.00%
GitHub Copilot	31	9.00%
Notion AI	20	5.80%
Prefer not to say	1	0.30%
C. Tasks Typically Supported by AI		
Task Type	**No. of Respondents**	**% of Respondents**
Writing/email drafting	253	73.30%
Presentation / Slide design	179	51.90%
Research / Reporting / Summarization	173	50.10%
Brainstorming/Ideation	161	46.70%
Data analysis / Excel assistance	141	40.90%
Meeting summaries/transcriptions	110	31.90%
Image/video generation	102	29.60%
Language translation/localization	72	20.90%
Dynamic reporting/dashboards	52	15.10%
Customer response generation	50	14.50%
Coding/Automation	54	15.70%
Others	31	9.00%
Prefer not to say	3	0.90%

Note: AI = Artificial Intelligence; reimbursement refers to initially paying for the tool or service and later receiving compensation from the organization.

4.2.3 Risk Perception, Policy Gaps, and AI Tool Avoidance

Despite the growing prevalence of generative AI tools, nearly a quarter of respondents (24.1%) reported intentionally avoiding their use in the workplace. This behavior appears to be driven more by psychological and reputational concerns than by technical limitations or access issues. Notably, while 42% of respondents expressed moderate to

high concern over risks such as data leakage and AI hallucinations, only 24.9% reported having access to a formal organizational policy on AI use. The remainder either lacked clear guidance or operated under informal norms, indicating a widespread governance vacuum. To examine drivers of avoidance behavior, a logistic regression model was employed. As shown in Table 3, risk perception emerged as the sole statistically significant predictor ($p < 0.001$), whereas neither policy awareness nor hierarchical role level had any meaningful effect. A Kruskal–Wallis test further revealed no significant regional variation in perceived risk, underscoring the global nature of user anxieties. These findings suggest that governance strategies should prioritize psychological safety and behavioral reassurance, rather than relying solely on formal policy dissemination.

Table 3. Logistic regression model identifying predictors of AI tool avoidance (n = 345)

Predictor	**Estimate (β)**	**Std. Error**	**z-value**	**p-value**	**Interpretation**
(Intercept)	-3.3732	0.774	-4.358	< 0.001 ***	Baseline probability
Policy Awareness (X1)	0.2095	0.1745	1.201	0.23	Not significant
Role Level (X2)	-0.1059	0.1527	-0.694	0.488	Not significant
Risk Perception (X3)	0.8073	0.1439	5.612	< 0.001 **	Significant predictor

**Note: Std. Error = Standard Error; AIC = Akaike Information Criterion; df = degrees of freedom; ***p < 0.001, *p < 0.01. Model: Avoidance = Policy Awareness + Role Level + Risk Perception.*

4.2.4 Governance Support Needs

Despite the informal nature of GenAI adoption, survey respondents expressed a clear preference for structured governance support. Notably, 69% of participants favored clear usage guidelines, 67% sought structured awareness programs, and 62.3% supported having a vetted list of approved tools. These preferences held consistently across geographies, role levels, and usage frequency. Importantly, high-frequency users were just as likely to request formal guidance, indicating that governance is not seen merely as a compliance mechanism but as a confidence enabler. Figure 2 summarizes these preferences across six key categories. These findings suggest a demand for modular, enablement-oriented governance—including onboarding support, pre-built policy templates, and tool curation—rather than rigid, top-down control. Organizations appear best positioned to build trust by offering guardrails that balance autonomy with clarity.

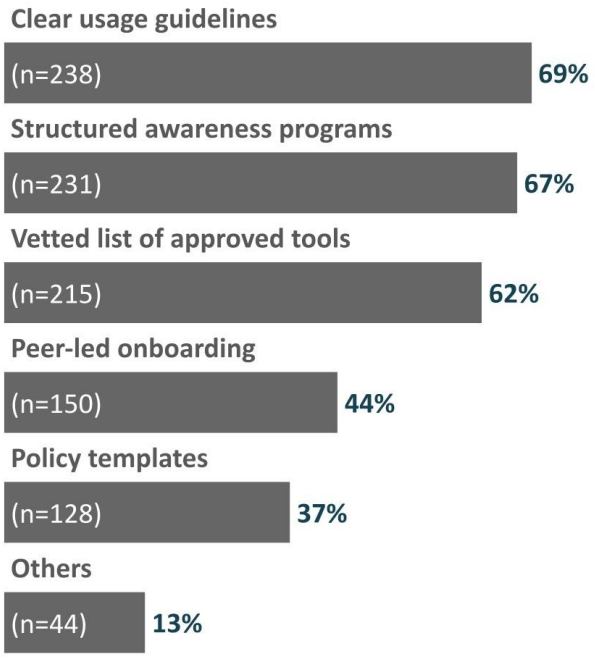

Figure 2. Preferred Governance Support Measures for Workplace AI Use
Author-created figure based on survey responses (n = 345).

4.2.5 Archetyped Employee Behaviors in BYOAI Engagement

Employee use of GenAI tools varies widely across capability, disclosure, and risk tolerance. Based on survey responses and open-text coding, six behavioral archetypes were derived to capture these differences. These profiles support personalized governance strategies and are summarized in Table 4.

Table 4. Workplace AI user archetypes based on behavior, risk tolerance, and disclosure

Archetype	Description	% (Approx.)
AI Champion	Enthusiastically promotes AI adoption, mentors peers, and influences team behavior.	14%
Expert Explorer	Highly capable and independent user; experiments ahead of formal guidance.	17%
Cautious Observer	Open to AI but refrains from use due to ambiguity or perceived risks; waits for clarity.	21%
Silent Starter	Uses AI quietly without disclosing usage; risk-aware but efficiency-driven.	18%
Passive User	Disengaged or unaware of GenAI tools; lacks exposure or sees limited relevance.	20%
Rule Bender	Actively bypasses guidance or restrictions to use unsanctioned tools.	10%

Note: Percentages are approximate, based on structured survey responses and qualitative coding of open-text feedback. Archetypes reflect relative behavioral trends and are not mutually exclusive.

This typology shows that effective governance must be personalized. Silent Starters, for instance, may need trust-building and safe disclosure templates, while Rule Benders require structured restrictions and targeted oversight. These archetypes serve as design anchors for behavior-aware governance.

4.2.6 Archetyped Organizations and Governance Postures Toward BYOAI

Organizational responses to BYOAI vary in structure, intent, and support. Drawing on reported policy access and qualitative feedback, four governance archetypes were identified—ranging from fully structured models to passive or uninformed tolerance. These categories help explain how institutional context shapes user behavior. Table 5 outlines these archetypes and their approximate distribution.

Table 5. Organizational archetypes based on BYOAI governance posture

Organizational Archetype	**Description**	**Approx. %**
Structured Enablers	Have formal policies, approved tools, training modules, and disclosure pathways.	24.90%
Silent Permitters	No formal governance, but BYOAI is allowed or tolerated without resistance.	~19.4%
Unaware Tolerators	Lacking both policy and awareness, usage occurs without any oversight.	~43.2%
Conditional Supporters	Provide selective support—typically limited to core teams or tech functions.	~12.5%*

Note: BYOAI = Bring Your Own AI. Percentages are approximate. Conditional supporters were identified through indirect indicators and open-text responses.

These governance postures influence employee engagement. For instance, a cautious observer may feel supported in a structured enabler context but remain disengaged under an unaware tolerator. Recognizing this interaction between user type and organizational environment is critical for designing governance systems that are adaptive, behavior-aware, and psychologically safe.

4.3 The BYOAI-Gov™ framework: Behavior-Aware, Risk-Tiered AI Governance

The adoption of generative AI (GenAI) tools in the workplace reveals substantial variability across both user behavior and organizational response. This asymmetry—ranging from covert, informal use by individuals to complete absence of formal policies at the institutional level—necessitates a governance model that is both flexible and grounded in behavioral realities. The BYOAI-Gov framework responds to this need. It offers a modular, empirically derived framework that moves beyond one-size-fits-all compliance models. Built from a synthesis of systematic literature and multi-region survey findings, the framework is designed to align oversight with task sensitivity, user archetypes, and institutional maturity.

4.3.1 Structure of the BYOAI-Govframework

The BYOAI-Gov framework offers a modular governance framework integrating behavioral segmentation, task sensitivity, and organizational maturity. Developed through a three-phase synthesis of empirical and literature-based insights, its structure reflects real-world AI usage rather than abstract control models. The framework comprises three interlinked modules: task-risk zoning (Enable, Regulate, Restrict), behavior-anchored interventions tied to user archetypes, and a four-stage organizational maturity overlay. Together, these modules support phased, context-aware governance aligned with institutional readiness. Table 6 summarizes the framework's core components.

Table 6. Key components of the BYOAI-Gov framework

What It Includes	What It Does
Behavioral Personas	Classifies employee behavior into types like Innovators, Cautious Users, and Avoiders—so governance can be tailored.
Task Sensitivity Tiers	Groups GenAI usage by risk levels: T1 (low-risk), T2 (moderate), and T3 (high-risk tasks).
Governance Levers	Combines policies, access controls, training, and psychological safety levers—mapped to personas and risk tiers.
Maturity Levels	Offers a four-level roadmap: Passive → Reactive → Structured → Strategic, showing how governance can evolve.
Global Benchmarking	Aligns the framework with trusted standards: OECD AI Principles, UNESCO AI Ethics, AI4People, and the EU AI Act.

Note: BYOAI = Bring Your Own AI; GenAI = Generative Artificial Intelligence; SLR = Systematic Literature Review. Framework components are synthesized from SLR and survey insights and designed to align behavioral governance with international AI ethics frameworks.

4.3.2 framework Design Methodology

The BYOAI-Gov framework was developed through a staged, evidence-driven process focused on contextual fit and behavioral realism. Inputs were drawn from a systematic review (Section 4.1) of 45 peer-reviewed studies and a multi-region survey of 345 professionals, revealing gaps in governance and diverse usage behaviors. User and organizational archetypes were distilled from these findings and mapped to practical governance needs using a 70:20:10 task-risk segmentation. This informed a conceptual model linking behavioral patterns to oversight levers such as disclosure pathways, tool registries, and sandbox environments. Framework components were modularly designed for operational relevance and refined through expert feedback. Final validation aligned the framework with global AI ethics standards. Figure 3 summarizes this seven-stage development process.

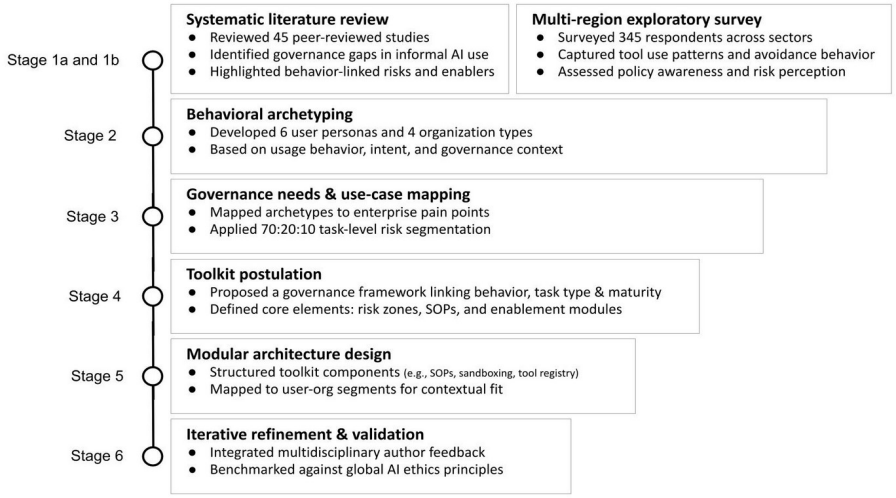

Figure 3. Research-Informed Development Process of the BYOAI-Gov framework

A six-stage development funnel illustrating the progression from literature synthesis and survey insights to behavioral archetyping, governance need mapping, framework design, modular architecture, and expert validation. Author-generated visual based on primary research inputs.

4.3.3 The BYOAI-Gov framework: Structure, Segments, and Application Logic

A central feature of the BYOAI-Gov framework is its task-centric, risk-tiered governance structure that classifies generative AI activities into three distinct zones—Enable (70%), Regulate (20%), and Restrict (10%). Rather than focusing on specific tools, this model emphasizes the nature of the task and its contextual risk as the basis for oversight. The indicative 70:20:10 segmentation reflects real-world usage trends and risk perceptions observed in the empirical data.

- Enable (70%) encompasses low-risk, individual productivity tasks—such as note summarization, rewriting internal content, or generating non-client-facing drafts. These activities typically require minimal oversight and can be supported through awareness-building initiatives, safe-use templates, and onboarding materials. Employees operating in this space often align with archetypes like *Quiet Enablers* and *Tool Evangelists*.
- Regulate (20%) includes moderate-risk, team-oriented, or semi-automated tasks —such as internal reporting, prompt-based synthesis, or collaborative content creation. These require contextual oversight through conditional approvals, department-level playbooks, and usage disclaimers. This zone frequently includes *power users* and *rule benders* who push boundaries within perceived grey zones.
- Restrict (10%) covers high-risk or externally sensitive applications—ranging from legal or compliance content generation to the use of client data or submission of AI-generated proposals. Activities in this segment warrant restrictive controls, including task prohibitions, formal review pathways, and secure alternatives. User archetypes here often include *Shadow Scripters* or high-autonomy actors operating with elevated risk exposure.

Figure 4 presents a visual depiction of these zones, associated task types, and recommended governance responses.

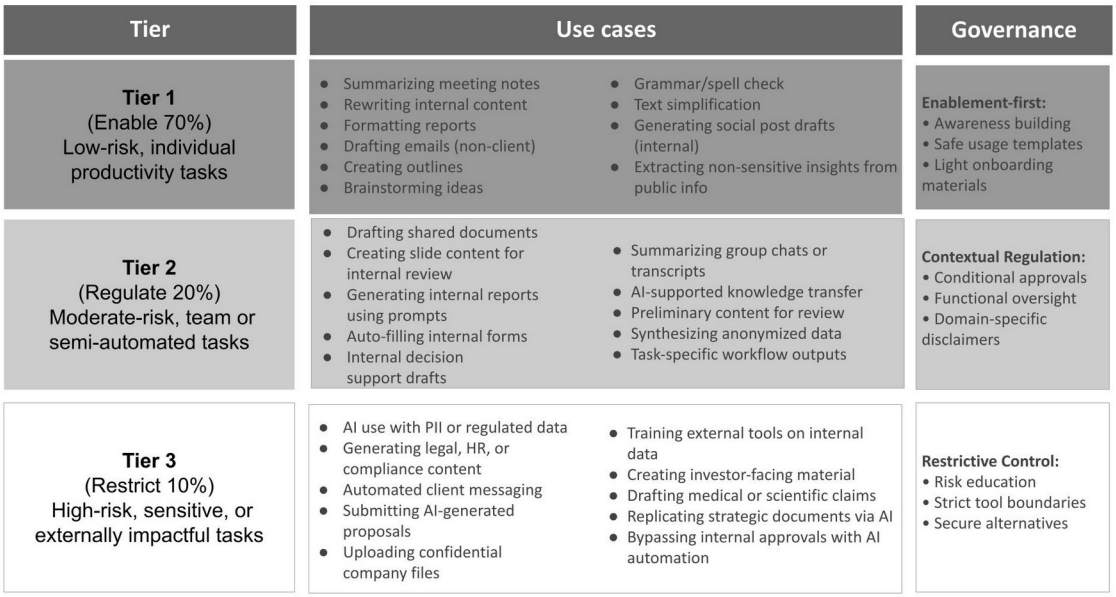

Figure 4. BYOAI-Gov™ framework: Tiered Governance Model

A tiered model classifying GenAI use into Enable, Regulate, and Restrict zones based on risk intensity and task sensitivity. Use cases and governance strategies are mapped accordingly. Author-generated figure based on empirical data and framework synthesis.

4.3.4 Operationalizing the BYOAI-Gov Framework: Mechanisms and Modularity

To enable practical implementation, the BYOAI-Gov framework includes seven modular components that connect strategic principles with day-to-day governance actions. These tools support varying organizational postures by linking behavioral profiles and task risk tiers to specific interventions. For example, the AI Tool Registry and Risk Litmus Sheet assist in contextual risk assessment, while the Ethics-Onboarding Card and Disclosure Template promote transparency and psychological safety. Designed for progressive adoption, these modules allow phased integration across maturity levels. Table 7 outlines each component and its intended function.

Table 7. Core components of the BYOAI-Gov framework and their intended functions

Framework Component	**What It Covers**
AI Tool Registry	A living database of tools mapped to green, amber, and red zones based on task risk and data exposure. Includes usage notes, update protocols, and contact points for tool escalation.
Disclosure Template	A one-page self-declaration form for employees to disclose AI tools used outside formal approvals. Includes optional fields for task type, data type, and frequency of use.
Ethics-Onboarding Card	A visually engaging one-pager summarizing responsible AI use. Covers hallucination risk, AI bias awareness, input limitations, and red flag examples.
Risk Litmus Sheet	A short checklist for team leads or function heads to assess whether a given task–tool pair is appropriate. Includes green–amber–red indicators based on context, content, and consequences.
Function-Level Playbooks	Customizable guides for departments (e.g., HR, marketing, analytics) detailing relevant use cases, safe tool usage, red zones to avoid, and escalation mechanisms.
Anonymous Survey Pulse	A lightweight, repeatable survey format to gather feedback on AI adoption comfort, psychological safety, governance clarity, and perceived value. Meant for biannual deployment.
Framework Ownership Role	Role definition for a departmental AI champion. Includes a sample JD (job description), escalation protocols, peer training duties, and engagement in governance updates.

Note: Components are derived from the literature, survey responses, and expert consultations to ensure practical and contextual governance alignment. Abbreviations: AI – Artificial Intelligence; JD – Job Description; SME – Subject-Matter Expert; BYOAI – Bring Your Own AI

This modular architecture supports flexible rollout pathways. Organizations in early stages may prioritize lightweight, trust-building tools, while more advanced settings can deploy structured playbooks and defined oversight roles. Governance adaptation is guided by a four-level maturity model—Passive, Reactive, Structured, Strategic—as illustrated in Figure 5, enabling alignment with institutional capability and user behavior over time.

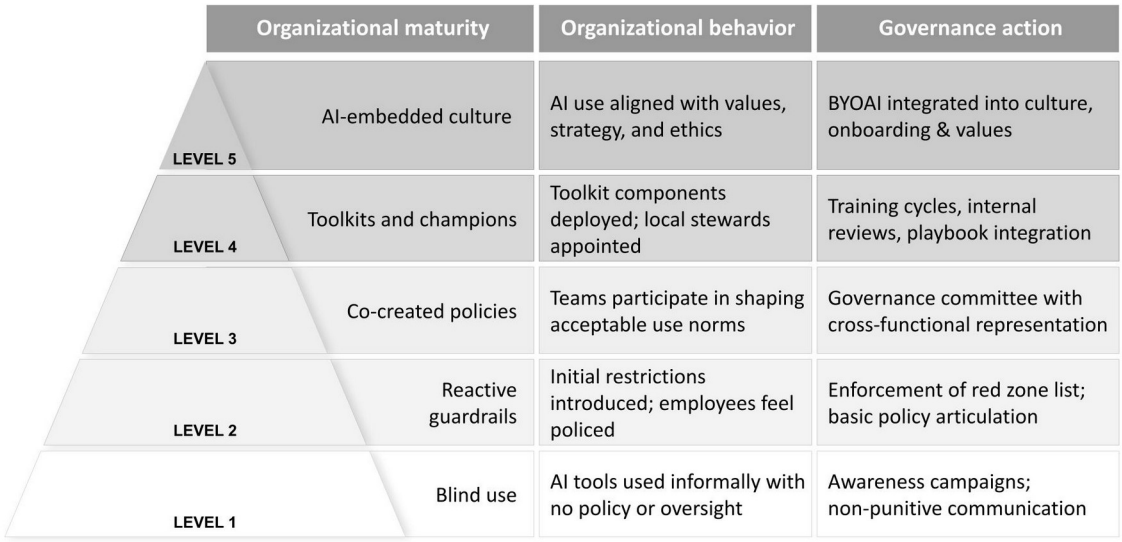

Figure 5. BYOAI-Gov framework: Governance Maturity Model
A progressive model outlining enterprise readiness stages: Passive → Reactive → Structured → Strategic. Author-generated visual informed by multi-source insights.

4.3.5 Integrative Summary

The BYOAI-Gov framework offers a cohesive model for managing unsanctioned AI use through modular, context-sensitive governance. It integrates behavioral archetypes, task-risk segmentation (70:20:10), and enterprise maturity stages to deliver personalized oversight strategies. With tools ranging from disclosure forms to departmental playbooks, the framework supports organizations across adoption curves. Fundamentally, this framework recognizes that governance must be behavior-aware, risk-aligned, and evolution-ready—grounded in lived user dynamics rather than idealized compliance structures.

5. Discussion

This study examined the increasing normalization of unsanctioned generative AI (GenAI) use within enterprise settings and proposed the BYOAI-Gov framework—an adaptive, behavior-sensitive governance model. Through a mixed-methods approach combining systematic literature synthesis and a multi-region survey (n = 345), the research revealed significant gaps between user behavior and formal policy, underscoring the need for governance frameworks that reflect actual usage contexts rather than enforcing rigid controls. The findings challenge traditional top-down approaches and advocate for an integrative ethos of psychological safety, proportional oversight, and co-created guardrails.

5.1 From Shadow to Strategy: Closing the Governance Gap in BYOAI

Bring Your Own AI (BYOAI) has moved from the margins to the mainstream. In this study, 42% of respondents reported accessing GenAI tools through personal accounts, while only 26.6% used exclusively sanctioned platforms (Brynjolfsson, Li, & Raymond, 2023). This grassroots adoption cuts across departments and roles, driven more by task-specific needs than organizational hierarchy (Yusuf et al., 2024). However, only 25% reported access to a formal AI policy, indicating a persistent gap between usage realities and institutional oversight.

Rather than an act of defiance, this pattern reflects unmet needs within the workforce. Employees turn to generative AI tools to improve efficiency and ease workload, yet often operate in a vacuum of guidance. Traditional compliance-driven policies cannot cope

with such decentralized and spontaneous use. In most cases, BYOAI represents a search for productivity—not a breach of policy (Zirar, Ali, & Islam, 2023; Chowdhury, Budhwar, Jeyaraman, Pereira, & Tarba, 2022). Psychological safety and autonomy, as highlighted by Edmondson and Lei (2014), are essential for innovation to thrive. When rules are ambiguous or punitive, employees either hide their use of AI or disengage altogether, stifling creativity and experimentation. Top-down governance frameworks such as those advanced by UNESCO, the OECD, and AI4People (Anthuvan & Maheshwari, 2025; Organisation for Economic Co-operation and Development [OECD], 2019) rightly stress transparency and accountability but assume centralized control over AI systems. In reality, our findings show that 60% of generative AI use occurs without formal oversight, while 24% of users abstain completely for fear of sanctions or unclear rules. This echoes the notion of "unethical pro-organizational behavior" (Tang, Yam, & Koopman, 2020), where well-intentioned employees bend rules in pursuit of efficiency, inadvertently creating hidden risks.

Comparable trends are visible beyond the enterprise. In higher-education settings, students' independent adoption of AI tools has outpaced institutional preparedness, underscoring the urgency for diagnostic and governance frameworks that enable responsible use (Anthuvan, Prabhuram, Wankhade, & Maheshwari, 2025). Likewise, research on large technology firms reveals a similar pattern of bottom-up diffusion, where generative AI spreads through early adopters and "spreaders" rather than through managerial directives (Rowe, Suire, Raymond, & Jacob, 2024).

5.2 Archetypes, Risk Perception, and Psychological Safety

GenAI use in the workplace reflects behavioral diversity rather than uniform adoption. This study identified six user archetypes that differ in disclosure practices, risk perception, and AI engagement intent. These profiles offer a foundation for risk-calibrated, psychologically safe governance responses. Table 8 presents the archetypes alongside targeted interventions designed to align with their behavioral and organizational impact.

Table 8. BYOAI user archetypes and recommended governance responses

Archetype	Typical Behavior	Perceived Risk	Recommended Governance Response
Shadow Scripter	Runs unapproved automations or scripts; bypasses policy	High	Flag for risk review; offer secure alternatives
Power User	Relies heavily on AI across functions and workflows	Medium	Provide training; whitelist safe, approved tools
Tool Evangelist	Actively promotes AI use within team/peer networks	Medium	Onboard as internal champions with guidelines
Quiet Enabler	Uses personal AI for simple tasks; avoids formal disclosure	Low	Normalize use; encourage voluntary disclosures
Avoider	Avoids AI due to unclear rules or fear of judgment	Low	Address via psychological safety and role clarity
Unaware User	Uses embedded AI features unknowingly (e.g., autocomplete)	Low	Awareness campaigns build foundational knowledge

Note: Archetypes are derived from survey behavior patterns; governance responses are aligned with risk levels and disclosure behaviors.

Psychological safety significantly shaped how employees engaged with GenAI tools. While some users reported open, responsible usage, others avoided or concealed their use due to fear of judgment or ambiguous policies—consistent with prior research on the inhibitory effects of low-trust environments (Edmondson & Lei, 2014; Newman, Round, Bhattacharya, & Roy, 2017; Tarafdar, Cooper, & Stich, 2019). As summarized in Table 9, varying levels of psychological safety mapped directly to distinct usage behaviors, underscoring the need for emotionally attuned governance strategies.

Table 9. Psychological safety and its influence on AI usage behavior

Psychological Environment	**Observed Behavior**	**Governance Need**
High psychological safety	Responsible use, voluntary disclosure	Encourage, guide, and celebrate usage
Moderate psychological safety	Hesitant use, limited experimentation	Clarify policies and provide training
Low psychological safety	Covert use, complete avoidance	Build trust and safe experimentation zones

Note: Patterns are derived from user-reported behaviors and correlated with levels of psychological safety in workplace environments.

These dynamics validate the behavioral design of the BYOAI-Gov framework. By linking interventions to user types and ensuring psychological safety, the framework promotes open, responsible adoption rather than reliance on restrictive controls. Cross-tabulations by role, age group, and function further support the value of segmentation. This is consistent with prior literature demonstrating that psychological safety, performance expectancy, and peer influence positively affect technology adoption, while job insecurity and algorithmic aversion serve as barriers—even in innovation-focused settings (Jain, Garg, & Khera, 2022; Edmondson & Lei, 2014; Park & Park, 2024; Cao, Duan, Edwards, & Dwivedi, 2021).

5.3 Theoretical Triangulation: Bridging UTAUT, Shadow IT, and Human Capital

The behavioral insights from this study align with three complementary theoretical lenses. UTAUT explains GenAI adoption as driven by perceived efficiency and peer validation, with barriers like policy ambiguity and inadequate support dampening use (Orlikowski, 2000; Korzyński, Costa e Silva, Górska, & Mazurek, 2024). Shadow IT theory situates BYOAI as a workaround to institutional gaps—motivated by autonomy, speed, or unmet functional needs (Silic & Back, 2014; Zhao, Dai, & Jun, 2025). Human capital theory reframes such behavior as self-directed learning, with users adopting AI tools to enhance personal capability and relevance in a changing work landscape (Deci & Ryan, 2000; Morandini et al., 2023). Together, these frameworks position BYOAI not as mere rule-breaking, but as an indicator of engagement and adaptability. Table 10 links key user motivations to targeted governance responses that foster responsible innovation and skills development.

Table 10. Upskilling-driven BYOAI behaviors and governance opportunities

Employee Motivation	Typical BYOAI Behavior	Governance Opportunity
Desire for efficiency	Using AI for repetitive task automation	Provide curated frameworks with job-specific examples
Learning by doing	Experimenting with prompt design	Enablement zones and self-paced training modules
Staying competitive	Leveraging AI to augment skill sets	Recognize AI fluency in performance reviews

Rather than viewing BYOAI as a form of deviance or policy breach, these behaviors can be reframed as strategic signals of workforce engagement and adaptability. When appropriately governed, BYOAI becomes not a liability but a lever for individual growth and organizational innovation.

5.4 framework Validation and Global Alignment

The BYOAI-Gov framework demonstrates strong alignment with leading international AI governance frameworks, including the OECD AI Principles (Organisation for Economic Co-operation and Development [OECD], 2019), the AI4People guidelines (Anthuvan & Maheshwari, 2025), UNESCO's *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021), and the emerging EU AI Act (European Commission, 2021). These frameworks emphasize core governance principles such as human agency, proportionality, transparency, and contextual oversight—values that are inherently embedded within the framework's design. Specifically, the framework's archetype-based governance supports inclusivity and human-centric oversight by addressing diverse user motivations and psychological needs. The 70:20:10 task zoning model operationalizes proportionality by calibrating governance intensity to task sensitivity, while the accompanying maturity ladder enables phased deployment aligned with organizational readiness. In terms of accountability and explainability, the framework includes practical components like tool registries, disclosure templates, and departmental playbooks that promote visibility and institutional learning. Furthermore, the emphasis on upskilling and capacity building—through enablement zones, HR–L&D levers, and self-paced training modules—addresses global calls for enhancing digital literacy and workforce preparedness. Overall, the BYOAI-Gov framework offers a modular, behavior-sensitive approach that meets global standards while remaining adaptable across enterprise types and geographies.

5.5 Organizational Maturity and Governance Scalability

The successful adoption of BYOAI governance hinges on an organization's digital maturity, behavioral dynamics, and risk sensitivity. The BYOAI-Gov maturity model outlines a five-stage progression—Awareness, Reactive, Structured, Strategic, and Embedded Governance—illustrating how oversight mechanisms can evolve as GenAI usage matures across enterprise functions. In early phases, where informal experimentation prevails and policies are either absent or unclear, organizations benefit from soft-enablement tools such as awareness campaigns, disclosure templates, and ethical onboarding aids. As maturity increases, governance can incorporate structured interventions like function-specific playbooks, task-risk matrices, and usage vetting protocols. At the highest level, BYOAI oversight becomes embedded in daily operations through defined roles (e.g., AI Champions), audit trails, and continuous learning programs. This graduated approach is supported by research emphasizing that psychological enablers—such as autonomy, competence, and trust—foster responsible

digital experimentation (Weritz, Wache, & Honigsberg, 2024). Rather than enforcing rigid compliance, the model promotes behavioral governance that adapts to evolving organizational realities and user needs. Comparable readiness frameworks are emerging in other domains as well. For instance, Re Cecconi, Khodabakhshian, and Rampini (2025) proposed an AI-readiness metric for the construction sector, emphasizing sustainability and ethical integration—paralleling the governance maturity logic of the BYOAI-Gov™ framework. Similar readiness and governance concerns are emerging in healthcare, where AI-capable organizations are being defined by their infrastructure, ethical oversight, and ability to manage Bring Your Own AI behaviors responsibly (Arnaout, 2025).

5.6 From Policy to Practice: Societal Relevance and a New Governance Ethos

The BYOAI-Gov framework is designed not just for internal enterprise governance but also for wider societal applications. Unlike static, principle-based frameworks (Cath, Wachter, Mittelstadt, Taddeo, & Floridi, 2018; Whittlestone, Nyrup, Alexandrova, & Cave, 2019), it offers a modular, context-aware structure that adapts to local needs—suitable for AI governance in sensitive sectors like finance, healthcare, and education (Whittlestone et al., 2019; Jia, 2020). Its design aligns with current calls for multi-level, inclusive governance (Bankins, Ocampo, Marrone, Restubog, & Woo, 2023), enabling regulators and policymakers to conduct audits, run sandbox trials, and assess readiness beyond mere compliance—bridging the gap in fast-changing GenAI environments (Winfield & Jirotka, 2018). The framework fosters trust and transparency by shifting away from punitive models toward psychologically safe, behavior-aware oversight (UNESCO, 2021). It also supports digital inclusion, offering scalable governance that does not overburden smaller organizations

Ultimately, BYOAI reflects decentralized digital agency—not deviance. Employees using GenAI tools out of curiosity or need represent bottom-up innovation that warrants guidance, not suppression. The framework embraces co-responsibility and resilience, urging enterprises to integrate AI responsibly and inclusively into everyday work (Raju, 2024; van der Meulen & Wixom, 2024). Emerging literature strengthens this need: Legal risks in Shadow AI remain high in regulated sectors (Balogun et al., 2025); psychological harm, such as work alienation, is a concern in the absence of safeguards (Hai, Long, Honora, Japutra, & Guo, 2025); and ethics boards often lack teeth without systemic embedding (Schuett, Reuel, & Carlier, 2023). Newer governance trends now emphasize co-creation, skill-building, and agility over rigid control—principles echoed in the framework (Makarius, Mukherjee, Fox, & Fox, 2020; Mendy, Jain, & Thomas, 2024; Anthuvan, 2024).

6. Future Research and Limitations

While this study offers an empirically grounded foundation for understanding BYOAI behaviors and governance responses, several limitations merit consideration. The survey sample was predominantly India-centric, which, despite no statistically significant differences in cross-country risk perceptions ($p = 0.2833$), may limit generalizability to contexts with stricter regulatory regimes or lower GenAI adoption rates. The self-reported and exploratory nature of the data also constrains causal inferences, particularly regarding user motivations and behavioral shifts. Moreover, although the BYOAI-Gov framework was developed through rigorous synthesis of literature, survey insights, and expert feedback, it has not yet been field-tested in live organizational settings. Future research should employ longitudinal and experimental methodologies to assess behavioral evolution, intervention efficacy, and the psychological impact of governance strategies—such as red-zone enforcement protocols or task-based training modules. Sector-specific pilot implementations and cross-organizational comparisons are also essential for refining the framework's contextual adaptability and operational scalability. Such studies can

inform governance configurations tailored to industry maturity, task sensitivity, and employee readiness, thereby strengthening the empirical and practical utility of the BYOAI-Gov framework.

7. Conclusion

The rise of Bring Your Own AI (BYOAI) reflects a shift from centralized control to decentralized innovation in enterprise settings. Employees are informally adopting generative AI tools to enhance efficiency and relevance, often without formal guidance—creating both opportunity and risk. This study responds to that gap through a dual-method approach, offering a behavior-informed governance framework grounded in empirical insights and socio-technical theory. The proposed BYOAI-Gov framework moves beyond compliance-oriented models by incorporating behavioral archetypes, task sensitivity, and organizational maturity. It enables structured enablement rather than blanket restriction—positioning employees not as rule-breakers but as co-creators of responsible AI integration. By aligning governance with real-world usage patterns and promoting psychological safety, the framework helps organizations balance innovation with accountability. As generative AI technologies continue to evolve, enterprise governance must do the same—adopting adaptive, inclusive, and trust-based approaches. Institutions that embrace this ethos will be better prepared to harness AI's benefits while safeguarding ethical and operational integrity.

Glossary

- **BYOAI (Bring Your Own AI):** The informal, employee-led use of generative AI tools (e.g., ChatGPT, Midjourney, Bard) within the workplace, typically without official approval or integration into enterprise governance systems.
- **BYOAI-Gov™ framework:** A modular, behavior-sensitive governance framework developed in this study. It guides responsible AI use based on user archetypes, task sensitivity, and organizational maturity levels.
- **Generative AI:** A category of artificial intelligence systems capable of producing human-like outputs—such as text, images, audio, or code—through learned patterns, commonly used for automation and content generation.
- **Shadow AI:** The unauthorized use of AI technologies by individuals or teams without IT or policy oversight, akin to Shadow IT practices but specific to AI.
- **Psychological Safety:** A workplace condition where individuals feel safe to take interpersonal or creative risks (e.g., using new tools or suggesting improvements) without fear of negative consequences.
- **Behavioral Archetypes:** Distinct user personas identified in this study based on patterns of GenAI adoption, such as "Quiet Enablers," "Avoiders," or "Power Users," used to tailor governance interventions.
- **Maturity Model:** A staged framework to assess and guide an organization's readiness for AI governance—from early awareness through structured, embedded oversight.
- **Risk Zones:** A tiered classification system used in the BYOAI-Gov framework to map AI tasks by potential risk: Green (low risk), Amber (moderate), and Red (high risk), each with aligned governance actions.
- **Task-Aware Governance:** A strategy that evaluates and regulates AI use based on the specific task being performed and its contextual risk—rather than issuing blanket tool-level policies.

- **70:20:10 Rule:** A governance segmentation model proposed in this study: 70% of AI use falls in a low-risk "Enable" zone, 20% requires "Regulate" oversight, and 10% demands "Restrict" controls.

Supplementary Material

The supplementary file accompanying this article includes the complete survey instrument, detailed behavioral archetype profiles, extracted interview themes, and a glossary of key terms used within the BYOAI-Gov Framework.

Acknowledgments:

The authors gratefully acknowledge Dr. Baishaki Das and Mr. Govind Joshi for expert validation of the survey instrument used in this study.

Statements and Declarations

Funding

This research received no external funding.

Ethics approval

Not applicable. The study used an anonymous, voluntary survey of adult professionals and collected no personal identifiers.

Informed consent

Not applicable. Participation was voluntary, and no personal data were collected.

Competing interests

The authors declare no competing interests, financial or non-financial, relevant to the content of this article.

Data availability

De-identified data and materials are available from the corresponding author upon reasonable request.

References

Advance CTE. (2024). Understanding the national career clusters framework: Modernization. Retrieved from https://careertech.org/wp-content/uploads/2024/06/Frequently-Asked-Questions_-Understanding-the-National-Career-Clusters-Framework-Modernization-June-2024.pdf

Anthuvan, T. (2024). Pharma marketing 2030: Transforming with innovation and skills. *Indian Journal of Technical Education*, 47(Special Issue No. 1), 49–53. https://doi.org/10.5281/zenodo.14627657 Retrieved from http://www.isteonline.in/Viewtopics.aspx?MenuId=IJTE_Special_Issue_1416

Anthuvan, T., & Maheshwari, K. (2025). AI-C2C (conscious to conscience): A governance framework for ethical AI integration. AI and Ethics, Advance online publication, 1–18. https://doi.org/10.1007/s43681-025-00736-2

Anthuvan, T., Prabhuram, S., Wankhade, S. U., & Maheshwari, K. (2025). *Bring Your Own AI (BYOAI) in Indian B-Schools: A PLS-SEM-validated diagnostic and governance framework for readiness and responsible integration. Available at SSRN 5394898.* https://doi.org/10.2139/ssrn.5394898

Arnaout, A. (2025). Are you leading an artificial intelligence-capable healthcare organization? *Healthcare Management Forum*. Advance online publication. https://doi.org/10.1177/08404704251375388

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The ethical and legal implications of Shadow AI in sensitive industries: A focus on healthcare, finance and education. Journal of Engineering Research and Reports, 27(3), 1–22. https://doi.org/10.9734/jerr/2025/v27i31414

Bankins, S., Ocampo, A. C., Marrone, M., Restubog, S. L. D., & Woo, S. E. (2023). A multilevel review of artificial intelligence in organizations: Implications for organizational behavior research and practice. Journal of Organizational Behavior. Advance online publication. https://doi.org/10.1002/job.2735
Brynjolfsson, E., Li, D., & Raymond, L. (2023). Generative AI at work (Working Paper No. 31161). Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w31161
Cao, G., Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2021). Understanding managers' attitudes and behavioral intentions towards using artificial intelligence for organizational decision-making. Technological Forecasting and Social Change, 173, 120421. https://doi.org/10.1016/j.technovation.2021.102312
Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': The US, EU, and UK approach. Science and Engineering Ethics, 24(2), 505–528. https://doi.org/10.1007/s11948-017-9901-7
Chin, T., Li, Q., Mirone, F., & Papa, A. (2025). Conflicting impacts of shadow AI usage on knowledge leakage in metaverse-based business models: A Yin–Yang paradox framing. Technology in Society, 81, 102793. https://doi.org/10.1016/j.techsoc.2024.102793
Chowdhury, S., Budhwar, P., Jeyaraman, K., Pereira, V., & Tarba, S. (2022). AI–employee collaboration and business performance: Integrating knowledge-based view, socio-technical systems and organisational socialisation framework. Journal of Business Research, 144, 31–46. https://doi.org/10.1016/j.jbusres.2022.01.069
Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. Psychological Inquiry, 11(4), 227–268. https://doi.org/10.1207/S15327965PLI1104_01
Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Janssen, M., … (2019). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 47, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002
Edmondson, A. C., & Lei, Z. (2014). Psychological safety: The history, renaissance, and future of an interpersonal construct. Annual Review of Organizational Psychology and Organizational Behavior, 1(1), 23–43. https://doi.org/10.1146/annurev-orgpsych-031413-091305
ESOMAR. (2023). Demographics – Best practice recommendation on age. Retrieved from https://esomar.org/uploads/attachments/cl5v19rsk1f9rew3vhglmzn55-esomar-demographics-best-practice-recommendation-on-age-for-consultation.pdf
European Commission. (2021). Proposal for a regulation on a European approach for artificial intelligence. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., & Schafer, B. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
Ghosh, A., Saini, A., & Barad, H. (2025). Artificial intelligence in governance: Recent trends, risks, challenges, innovative frameworks, and future directions. AI & Society. Advance online publication. https://doi.org/10.1007/s00146-025-02312-y
Gregor, S. (2006). The nature of theory in information systems. MIS Quarterly, 30(3), 611–642. https://doi.org/10.2307/25148742

Hai, S., Long, T., Honora, A., Japutra, A., & Guo, T. (2025). The dark side of employee–generative AI collaboration in the workplace: An investigation on work alienation and employee expediency. International Journal of Information Management, 83, 102905. https://doi.org/10.1016/j.ijinfomgt.2025.102905
Jain, S., Garg, R., & Khera, S. (2022). Adoption of AI-enabled tools in social development organizations in India: An extension of UTAUT model. Frontiers in Psychology, 13, 893691. https://doi.org/10.3389/fpsyg.2022.893691
Jaiswal, A., Arun, C. J., & Varma, A. (2021). Rebooting employees: Upskilling for artificial intelligence in multinational corporations. The International Journal of Human Resource Management, 32, 1179–1208. https://doi.org/10.1080/09585192.2021.1891114
Jia, H. (2020). Yi Zeng: Promoting good governance of artificial intelligence. National Science Review, 7(12), 1954–1956. https://doi.org/10.1093/nsr/nwaa255
Korzyński, P., Costa e Silva, S., Górska, A. M., & Mazurek, G. (2024). Trust in AI and top management support in generative-AI adoption. Journal of Computer Information Systems. Advance online publication. https://doi.org/10.1080/08874417.2024.2401986
Makarius, E. E., Mukherjee, D., Fox, J., & Fox, A. K. (2020). Rising with the machines: A framework for augmenting human intelligence in organizations. Journal of Business Research, 120, 241–251. https://doi.org/10.1016/j.jbusres.2020.07.045
Mendy, J., Jain, A., & Thomas, A. (2024). Artificial intelligence in the workplace – challenges, opportunities and HRM framework: A critical review and research agenda for change. Journal of Managerial Psychology. Advance online publication. https://doi.org/10.1108/JMP-05-2024-0388
Morandini, F., Fraboni, F., De Angelis, M., Puzzo, G., Giusino, D., & Pietrantoni, L. (2023). The impact of artificial intelligence on workers' skills: Upskilling and reskilling in organisations. Informing Science: The International Journal of an Emerging Transdiscipline, 26, 39–68. https://doi.org/10.28945/5078
Morley, J., Kinsey, L., Elhalal, A., Garcia, F., Ziosi, M., & Floridi, L. (2023). Operationalising AI ethics: Barriers, enablers and next steps. AI & Society, 38, 411–423. https://doi.org/10.1007/s00146-021-01308-8
Newman, A., Round, H., Bhattacharya, S., & Roy, A. (2017). Ethical climates in organizations: A review and research agenda. Human Resource Management Review, 27(2), 265–284. https://doi.org/10.1016/j.hrmr.2017.01.001
Noblit, G. W., & Hare, R. D. (1988). Meta-ethnography: Synthesizing qualitative studies. Newbury Park, CA: Sage Publications.
Organisation for Economic Co-operation and Development. (2019). OECD principles on artificial intelligence. Paris, France: OECD Publishing. Retrieved from https://www.oecd.org/going-digital/ai/principles/
Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. Organization Science, 11(4), 404–428. https://doi.org/10.1287/orsc.11.4.404.14600
Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71
Park, J. S., & Park, H. J. (2024). Enablers and inhibitors of generative AI usage intentions in work environments. Journal of Korean Society for Quality Management, 52(3), 509–527. https://doi.org/10.7469/JKSQM.2024.52.3.509
Pavlou, P. A., & El Sawy, O. A. (2010). The "third hand": IT-enabled competitive advantage in turbulence through improvisational capabilities. Information Systems Research, 21(3), 443–471. https://doi.org/10.1287/isre.1100.0280

Puthal, D., Mishra, A. K., Mohanty, S. P., Longo, A., & Yeun, C. Y. (2025). Shadow AI: Cyber security implications, opportunities and challenges in the unseen frontier. SN Computer Science, 6, 405. https://doi.org/10.1007/s42979-025-03962-x
Raju, G. (2024, April 18). The BYOAI phenomenon. LinkedIn. Retrieved from https://www.linkedin.com/pulse/byoai-phenomenon-ganesh-raju-8ekcc/
Re Cecconi, F., Khodabakhshian, A., & Rampini, L. (2025). *Building tomorrow: Unleashing the potential of artificial intelligence in construction.* Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-031-77197-2
Roberts, T., & Oosterom, M. (2024). Digital authoritarianism: A systematic literature review. Information Technology for Development, 1–25. https://doi.org/10.1080/02681102.2024.2425352
Rowe, F., Suire, R., Raymond, M., & Jacob, F. (2024, December). *Beliefs, controversies, and innovation diffusion: The case of generative AI in a large technological firm.* In *Proceedings of the Twenty-Ninth DIGIT Workshop (Diffusion Interest Group in Information Technology), Bangkok, Thailand.* Association for Information Systems Electronic Library (AISeL). https://aisel.aisnet.org/digit2024/
Schuett, J., Reuel, A., & Carlier, A. (2023). How to design an AI ethics board. AI and Ethics, 5, 863–881. https://doi.org/10.1007/s43681-023-00409-y
Scott, W. R. (2013). Institutions and organizations: Ideas, interests, and identities (4th ed.). Thousand Oaks, CA: Sage Publications.
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
Tang, P. M., Yam, K. C., & Koopman, J. (2020). Feeling proud but guilty? Unpacking the paradoxical nature of unethical pro-organizational behavior. Organizational Behavior and Human Decision Processes, 157, 47–61. https://doi.org/10.1016/j.obhdp.2020.03.004
Tarafdar, M., Cooper, C. L., & Stich, J.-F. (2019). The technostress trifecta—Techno eustress, techno distress and design: Theoretical directions and an agenda for research. Information Systems Journal, 29(1), 6–42. https://doi.org/10.1111/isj.12169
UNESCO. (2021). Recommendation on the ethics of artificial intelligence. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000381137
United Nations, Department of Economic and Social Affairs. (2024). Manual on the classification of business functions. Retrieved from https://unstats.un.org/unsd/classifications/Econ/Download/Manual_on_the_Classification_of_Business_Functions_WEB_2024-08-19.pdf
van der Meulen, N., & Wixom, B. H. (2024, February 12). Bring your own AI: How to balance risks and innovation. MIT Sloan Management Review. Retrieved from https://sloanreview.mit.edu/article/bring-your-own-ai-how-to-balance-risks-and-innovation/
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540
Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. Communications of the Association for Information Systems, 37, 205–224. https://doi.org/10.17705/1CAIS.03709
Wang, B. Y., Boell, S. K., Riemer, K., & Peter, S. (2023). Human agency in AI configurations supporting organizational decision-making. ACIS 2023 Proceedings (Paper 53). Retrieved from https://aisel.aisnet.org/acis2023/53

Weritz, P., Wache, H., & Honigsberg, S. (2024). How digital readiness relates to the intention to use generative AI in workplace service systems. AMCIS 2024 Proceedings. Retrieved from https://aisel.aisnet.org/amcis2024/incl_sustain/incl_sustain/5

Whittlestone, J., Nyrup, R., Alexandrova, A., & Cave, S. (2019, January). The role and limits of principles in AI ethics: Towards a focus on tensions. In Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society (pp. 195–200). https://doi.org/10.1145/3306618.3314236

Winfield, A. F., & Jirotka, M. (2018). Ethical governance is essential to building trust in robotics and artificial intelligence systems. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133), 20180085. https://doi.org/10.1098/rsta.2018.0085

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. Regulation & Governance, 12(4), 505–523. https://doi.org/10.1111/rego.12158

Yusuf, S. O., Abubakar, J. E., Durodola, R. L., Ocran, G., Paul-Adeleye, A. H., & Yusuf, P. O. (2024). Impact of AI on continuous learning and skill development in the workplace: A comparative study with traditional methods. World Journal of Advanced Research and Reviews, 23(2), 1129–1140. https://doi.org/10.30574/wjarr.2024.23.2.2439

Zhao, Y., Dai, R., & Jun, N. (2025). Generative AI: The transformative impact of ChatGPT on systemic financial risk in Chinese banks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5162554

Zirar, A., Ali, S. I., & Islam, N. (2023). Worker and workplace artificial intelligence (AI) coexistence: Emerging themes and research agenda. Technovation, 122747. https://doi.org/10.1016/j.technovation.2023.102747