Yönetim Bilişim Sistemleri Alanında Yenilikçi Çözümler ve Güncel Yaklaşımlar – IV

Editör: Doç. Dr. Vahid SİNAP

ÖZGÜR YAYINLARI

Yönetim Bilişim Sistemleri Alanında Yenilikçi Çözümler ve Güncel Yaklaşımlar – IV

Editör:
Doç. Dr. Vahid SİNAP

ÖZGÜR YAYINLARI

Published by
Özgür Yayın-Dağıtım Co. Ltd.
Certificate Number: 45503

15 Temmuz Mah. 148136. Sk. No: 9 Şehitkamil/Gaziantep
+90.850 260 09 97
+90.532 289 82 15
www.ozguryayınlari.com
info@ozguryayinlari.com

Yönetim Bilişim Sistemleri Alanında Yenilikçi Çözümler ve Güncel Yaklaşımlar – IV

Editör: Doç. Dr. Vahid SİNAP

Language: Turkish-English
Publication Date: 2026
Cover design by Mehmet Çakır
Cover design and image licensed under CC BY-NC 4.0
Print and digital versions typeset by Çizgi Medya Co. Ltd.

ISBN (PDF): 978-625-8813-24-1

DOI: https://doi.org/10.58830/ozgur.pub1366

Suggested citation:
Sinap, V. (ed) (2026). *Yönetim Bilişim Sistemleri Alanında Yenilikçi Çözümler ve Güncel Yaklaşımlar – IV.* Özgür Publications. DOI: https://doi.org/10.58830/ozgur.pub1366. License: CC-BY-NC 4.0

The full text of this book has been peer-reviewed to ensure high academic standards. For full review policies, see https://www.ozguryayinlari.com/

ÖZGÜR YAYINLARI

Ön Söz

Dijital dönüşüm, işletmelerin teknolojiyle kurduğu ilişkiyi her geçen gün daha stratejik bir zemine taşımaktadır. Yönetim Bilişim Sistemleri alanı bu dönüşüm içinde iş süreçlerinin yeniden tasarlanması, karar mekanizmalarının güçlendirilmesi, kurumsal verinin korunması ve yönetişim kapasitesinin geliştirilmesi açısından merkezi bir konuma sahiptir. Bu eser, güncel teknolojik gelişmeleri işletmelerin yönetim pratikleriyle birlikte ele almakta ve dijital çağın ortaya çıkardığı yeni fırsatları, riskleri ve sorumluluk alanlarını bütüncül bir bakışla değerlendirmektedir.

Kitapta yer alan bölümler, düşük kodlu ve kodsuz platformların iş süreçleri üzerindeki dönüştürücü etkisini, insan kaynaklarında yapay zekâ kullanımının seçim ve değerlendirme süreçlerine getirdiği yeni tartışmaları ve Shadow AI uygulamalarının kurumsal bilgi güvenliği açısından doğurduğu riskleri incelemektedir. Bu yönüyle eser, işletmelerin dijital araçları daha etkin, güvenli ve sorumlu biçimde kullanabilmeleri için kavramsal ve uygulamaya dönük bir çerçeve sunmaktadır. Teknolojik yeniliklerin hız kazandığı bu dönemde yönetişim, etik duyarlılık, veri güvenliği ve kurumsal farkındalık konuları eserin temel eksenini oluşturmaktadır.

Bu dördüncü cildin, Yönetim Bilişim Sistemleri alanındaki güncel tartışmalara katkı sağlamasını ve araştırmacılar, öğrenciler ile uygulayıcılar için yol gösterici bir kaynak olmasını temenni ederim. Eserin hazırlanmasına katkı sunan tüm bölüm yazarlarına teşekkür eder, kitabın akademik literatüre ve uygulama dünyasına değer katmasını dilerim.

Doç. Dr. Vahid SİNAP

Editör

İçindekiler

Chapter 1

Who Selects the Best? Artificial Intelligence Era in Human Resources

Agah Başdeğirmen[1]

Şahin Özgür Çeri[2]

Tuğba Erhan[3]

Abstract

This chapter aims to discuss and introduce the role of artificial intelligence (AI) in the recruitment process from both conceptual and practical perspectives, with examples from different applications. Every segment of the organization seeks to adopt and use the technology that AI can provide. Human resource management (HRM) is one of the departments of the organization that has been affected by the constant digital transformation. HRM uses the implementation of AI during the recruitment process. Most of the organizations are open to change and adopt AI-driven recruitment systems. Along with multiple stages of the hiring process, the organizations require major applications, including intelligent candidate sourcing, automated resume screening, algorithmic matching, and AI-conducted first interviews using chatbots, providing a comprehensive explanation of the operational mechanisms of these technologies and their integration into contemporary recruitment workflows. Recruitment carried out by AI, in terms of its efficiency, consistency, and data support, is assessed in comparison to significant limitations and risks, among them transparency and data privacy problems. Emphasis is given to candidate experience, fairness in AI-based evaluation, and the reliability of AI-based interviews in the early stages of the recruitment process. The role, competencies, and accountability in decision-making in organizations, related to AI adoption, are addressed in the chapter. Moreover, the present chapter also attempts to sketch an outline

1 Assistant Professor, Isparta University of Applied Sciences, agahbasdegirmen@isparta.edu.tr, 0000-0001-7471-7977

2 PhD Student, Suleyman Demirel University, d2240253520@ogr.sdu.edu.tr, 0000-0002-0046-9736

3 Associate Professor, Suleyman Demirel University, tugbaerhan@sdu.edu.tr, 0000-0002-5697-490X

https://doi.org/10.58830/ozgur.pub1366.c5527

of various issues to be considered in terms of the practical implementation of AI-conducted interviews. Thus, by discussing the present practices and trends, this chapter attempts to provide a balanced framework for understanding AI-supported recruitment, along with providing necessary guidance to various organizations for the effective implementation of AI in the recruitment process.

1. Introduction

Some of the initial conflicts and concerns between humans and machines have significantly contributed to the debate on the place of technology in the workplace, especially concerning trust, control, and the possibility of replacing human judgment in decision-making within organizations (Küçükeşmen et al. 2023; Işıldak & Tunca, 2018). AI is increasingly used for recruitment purposes, although there is limited research of its effect on hiring speed and candidate selection (Aka et al., 2025). In the field of HRM, AI-driven tools have become one of the key transformative factors, significantly changing the manner in which organizations attract, evaluate, or select their workforce. Organizations increasingly utilize AI-based technology to activate their recruitment process, including sourcing applicants, resume screening, scheduling interviews, and initial evaluation, to improve efficiency while facilitating the decision-making processes, which have been the most labor-intensive and time-consuming stages for the organizations (Dadaboyev et al., 2025).

Studies on the integration of AI tools in talent recruitment processes have proven to be beneficial to organizations, such as faster processing of candidate data, cost-effectiveness, candidate experience, and elimination of human bias. AI tools apply machine learning algorithms, natural language processing, and predictive analytics to identify patterns in candidate qualifications and behaviors that may not be apparent to recruiters, thus enhancing the quality and consistency of talent acquisition processes (Swain and Malik, 2025). Organizations can realize the advantages of AI by considering its facilitating role in different capacities (Vijayasree, 2025). This chapter seeks to conduct an extensive research of the transformative role of AI in modern recruitment processes.

Despite these promising advantages, the employment of AI systems in recruitment has also been related to a range of critical ethical, legal, and practical concerns. For example, concerns over algorithmic bias, data privacy, and transparency of AI decision-making processes are still receiving attention from both scholars and practitioners. Algorithmic systems may learn from existing hiring practices and thus perpetuate existing inequalities in society. Such systems may thus discriminate against different demographic groups in society (Dadaboyev et al., 2025). Additionally, candidates' experiences in

AI-mediated recruitment tools may differ from one candidate to another. Such experiences can affect perceptions of fairness and legitimacy in organizational practices (Horodyski, 2023). In light of these developments and debates, this chapter is designed to examine AI in recruitment practices by analyzing its applications, advantages, and associated challenges. Additionally, the chapter explores how digital transformation is impacting recruitment practices and organizational decision-making in human resource management. In doing so, the chapter critically examines how AI influences recruitment practices in terms of efficiency, quality of candidate selection, and perceptions of fairness in organizational practices.

2. Digital Transformation in Human Resource Management

Digital transformation in HRM can be defined as the integration of digital technology into every aspect of the HRM department, which has a fundamental impact on how organizations acquire, develop, and retain their human resources. Digital transformation is not simply a matter of digitalizing documents or processes, but rather the integration of digital technologies into all aspects of organizational functions, which changes the essence of how work is carried out (Vial, 2021).

In the context of HRM, digital transformation has become a strategic necessity, facilitated by technological advancements such as AI, big data, human resource HR information systems, and cloud-based technology, which can aid decision-making and improve operational efficiencies. Digital transformation in HRM is defined as follows: "the use of digital technology to improve the way HRM operations are performed, making them more agile, responsive, and able to adapt to the changing business environment" (Asike et al., 2025).

One of the key aspects of this change is the transition from labor-intensive conventional HR practices to digital-based practices that not only speed up the process but also provide real-time access to data, thereby improving the overall employee experience. For instance, it has been identified that not only can the adoption of digital technology speed up the hiring process, but also improve the overall talent management, engagement, performance, and learning (Milhem et al., 2024). Research suggests that the adoption of digital technology in the HR function can improve organizational effectiveness, agility, and competitive advantage as the HR function evolves toward an analytical role (Asike et al., 2025). Moreover, digital transformation repositions HRM as a key facilitator of organizational strategic changes. This is achieved through ensuring that investments in HR technology are aligned with overall business strategies. Such strategies include leveraging AI and analytics to enable objective decision-making and a deeper understanding of workforce dynamics.

2.1. Conceptual Foundations of AI in Recruitment

The conceptual bases of AI in the field of recruitment are rooted in the inter-disciplinary amalgamation of the disciplines of management strategy, behavioral science, socio-technical theory, and ethics (Singh et al., 2025). These conceptual bases not only account for the adoption of AI for the purpose of increasing efficiency but also account for the cognitive, organizational, and societal interfaces of AI. The integration of AI in the field of recruitment has resulted in an impactful influence on the process of attracting, selecting, and recruiting individuals. Besides, AI-based tools have become integral components of the different stages of the recruitment process. This part of the current chapter utilizes highly cited and foundational research to discuss the major applications, theoretical underpinnings, and debates surrounding AI in recruitment. AI in HRM has been expounded through numerous theoretical lenses that seek to clarify its strategic, social, and ethical aspects. The key conceptual frameworks for AI in recruitment are as follows:

- **The Resource-Based View (RBV):** The resource-based view (RBV), which views human capital as an important driver of competitive advantage (Barney, 1991). AI-based HR systems support this view by facilitating the identification, development, and utilization of talent. In relation to AI-based recruitment, this framework argues that for an organization to thrive, its resources should align to adopt AI-based recruitment technologies (Willie, 2025).
- **Socio-Technical Systems Perspective**: From a socio-technical perspective, AI interacts with organizational structures and cultures, and with human actors in an organization. The success of AI in HRM would depend upon how well technology has been integrated with social processes like communication, trust, and employee participation (Sandeep et al.,2025).
- **Algorithmic Decision-Making:** Algorithmic decision-making has emerged as a key concept in AI-based HR practices. The algorithms process data to aid decisions in employee selection, promotion, and appraisal. Although it ensures objective and consistent decisions, it may perpetuate existing biases in the data used to develop algorithms, thereby undermining the concept of fairness and meritocracy in HRM (Rodgers et al., 2023).
- **Ethical and Governance Frameworks**: One of the foundational components of AI in HRM is ethical considerations. Concerns over data privacy, consent, and transparency require proper governance to guide the application of AI in managing people (Kumar, 2025). The

principles of responsible AI highlight the importance of explainability, fairness, and human oversight in ethical HRM practices.

2.2. Advantages & Disadvantages of AI in Recruitment

In the usual way of hiring people, time and location are often important issues. Hiring someone can be a long and complicated process. It can include lots of job advertisements, several interviews, and difficult decisions that are often made in a particular place. Using AI tools can help organizations get around geographical limitations and access a global talent pool, no matter where in the world they are. After looking at how people feel about using AI to recruit, there are a few important points that stand out. One major advantage is that AI enables faster and more precise outcomes compared to traditional methods. By leveraging AI, the selection process becomes both more efficient and reliable (Horodyski, 2023).

AI tools are becoming common in recruitment, from screening resumes to assessments, due to their efficiency and ability to automate various aspects of hiring. They can swiftly process large amounts of data to identify patterns, reducing bias by executing tasks objectively. This makes AI appealing for recruitment efficiency, cost reduction, and quality of hire. But the deployment of AI in recruitment has challenges. Lack of human intuition and potential ethical concerns raise questions about the ability of AI to make hiring decisions (Yanamala, 2021).

The use of AI recruitment tools raises significant concerns that demand careful attention and proactive solutions through both technical and managerial measures (Raub, 2018). While growing evidence suggests that AI systems may be more impartial than often assumed, algorithms can still produce biased outcomes, leading to unfair employment opportunities and discrimination without accountability. To fully harness the benefits of AI in recruitment, organizations must carefully evaluate the tools they adopt, ensure the implementation of transparent and accountable algorithms, and actively promote racial and gender diversity within the technology sector (Chen, 2023).

It is evident that organizations may encounter challenges in identifying and recruiting a diverse range of candidates due to the inherent bias of AI-based recruitment engines. These biases can be influenced by factors such as region, gender, and ethnicity, potentially leading to a gradual homogenization of team composition. This phenomenon can result in the diminution of the benefits that diversity can offer, including the enhancement of creativity, innovation, and inclusivity (Kodiyan, 2019). Hiring is one of the most significant decisions for HR professionals, employers, or entrepreneurs, as

these potential decisions have short and long-term outcomes that directly affect the organization's income, sustainability, and overall performance and productivity. These decisions also have inevitable impacts on employers. Thus, HR professionals and employers are expected to find the best people for the job quickly and efficiently when they don't have enough time and money to do it (Raghavan et al., 2020).

3. AI-Based Assessment Tools

3.1. Strategies of AI in Recruitment

In the modern business environment, it has been observed that organizations are extending their scope of recruitment to the global market, seeking individuals with both experience and growth potential. In today's business environment, it has been observed that organizations are using AI tools to find the most appropriate candidate for a vacant position. Therefore, it can be said that conventional methods of recruitment are not found appropriate by organizations, and AI tools are used extensively. Indeed, on algorithmic recruitment platforms, it has been found that the organization involved in placing a job advertisement has the authority to determine the target audience pool during the production of a job advertisement, depending on certain criteria (Langer & König, 2023).

Davenport and Ronanki (2018) posit that AI provides capabilities that support three areas of business operations. Firstly, the potential of AI to enhance business process automation is evident in its provision of cognitive capabilities within software. For instance, organizations employ AI to facilitate tasks requiring automated decision-making, such as credit processing and supply chain management, and to furnish cognitive insights into customer purchasing behavior. Besides, in order to support HRM, the National Aeronautics and Space Administration (NASA) found that AI-enhanced HR processes enabled 86% of HR tasks to be completed without human intervention (Davenport & Ronanki, 2018).

The utilization of AI technology, such as machine learning algorithms, natural language processing, and predictive analysis, has the potential to be of significant benefit within the domain of recruitment systems. Industries always remain in constant need of recruiting competent and efficient individuals in order to fulfill their requirements and attain corporate objectives. The utilization of AI technology has the potential of minimizing human interventions while increasing processing speeds. The process of categorizing job postings on dedicated recruitment websites has the potential of allowing new job applicants access to such job postings with ease and efficiency. The

utilization of AI technology is an ongoing process, which has the potential of allowing recruitment operations to be conducted at any time and any location (Johnson et al., 2021).

Machine learning algorithms are created with the sole intention of scanning the resume and selecting the best candidate according to specific parameters. Machine learning algorithms can be used to train a large dataset consisting of resumes and make predictions regarding the suitability of a candidate for a specific role. Machine learning algorithms are also being used to eliminate potential biases in the hiring process (Roy et al., 2020). When compared to traditional hiring strategies, such as resume screening or employee referrals, AI and machine learning algorithms have the potential to identify patterns that are normally overlooked. This approach is used to select the best candidate for a specific role in a company with greater ease and effectiveness (Faugoo, 2024).

In order to mitigate the risk of algorithmic bias, the algorithm must be designed and trained using unbiased data and criteria. Nevertheless, the efficacy of AI-based hiring strategies is contingent on numerous factors. For instance, the effectiveness of predictive analytics may be contingent on the quality of the data utilized to train the algorithms. Predictive analytics is the process of utilizing algorithms for the analysis of data to predict outcomes. Within the context of the hiring process, the utilization of predictive analytics has been shown to facilitate the identification of candidates who demonstrate a high probability of demonstrating effective performance within a particular role (Bakal et al. 2026). The quality of the data utilized in training algorithms is of paramount importance for the efficacy of predictive analytics. In the event of substandard data quality, the employment of algorithms may result in the generation of erroneous predictions, which can consequently precipitate unfavorable hiring decisions. Conversely, the efficacy of data training can be enhanced by the elimination of biased language and criteria from job descriptions and the utilization of data sets that reflect diverse experiences. Moreover, human supervision is essential to maintain fairness and impartiality in decision-making processes. Experts need to periodically monitor and assess the algorithm's performance to detect and mitigate potential biases (Albassam, 2023). Several strategies have been formulated concerning the methods employed in AI-supported recruitment processes (Albassam, 2023). The strategies have been identified as follows:

A. Resume Scanning

Resume screening constitutes a pivotal component within the broader hiring process, encompassing the meticulous evaluation of resumes to discern prospective candidates who are deemed to possess the requisite qualifications

and proficiencies for a specific position. However, this process can be both time-consuming and challenging, particularly for large organizations that receive a high volume of applications for a single position (Derous & Ryan, 2018). In order to address this challenge, a significant number of companies are adopting AI-powered resume screening tools to automate the process and reduce time expenditure (Vedapradha et al., 2019). The employment of AI algorithms for the purpose of resume screening is predicated on the analysis of resumes in accordance with a predetermined set of criteria, including, but not limited to, job requirements, qualifications and skills (Hunkenschroer & Luetge, 2022). These algorithms have been shown to facilitate the rapid and accurate identification of candidates who meet the required criteria (Smith, 2023). This, in turn, enables hiring specialists to focus on the most suitable candidates for the role, thereby reducing the time and effort required for manual screening.

In this domain, keyword scanning is one of the most frequently used techniques. The keywords used in job postings are matched with phrases in the resumes with the objective of evaluating the suitability of applicants to jobs. To exemplify this assertion, let us take a situation in which a job posting indicates that proficiency in Java is necessary for applicants. In such a case, it would be expeditiously possible for the system to identify applicants with knowledge in Java. However, in modern advanced systems, it has been observed that the application of job posting phrases is not limited to the presence of keywords alone. Moreover, it has been noted that the application of keywords depends upon the context in which it has been used in job postings, professional growth trajectory, and correlation between knowledge and experience (Chen, 2023).

B. Candidate Matching

Candidate matching is defined as the analysis of extensive data sets employing machine learning algorithms to ascertain the most appropriate candidates for a position based on their qualifications, skills, and experience (Cardoso et al., 2021). The objective of this approach is to optimize the hiring process and enhance the precision of the selection process by minimizing the time and effort expended on identifying suitable candidates. A plenty of candidate matching algorithms exhibit distinct strengths and weaknesses. For instance, while certain algorithms employ natural language processing techniques to extract pertinent information from CVs or job descriptions, others utilize predictive analytics to identify high-potential candidates based on past performance or other relevant data points (Soni et al., 2020).

C. Video Interviewing

Video interview analysis is an AI-based recruitment technique that has gained increasing attention in recent years. This method involves the analysis

of job candidates' video interviews using natural language processing and facial recognition algorithms to assess their suitability for the position (Dunlop et al., 2022). Video interview analysis offers several advantages over traditional interview methods. It provides valuable insights into candidates' communication skills, personality, and cultural fit, which are difficult to assess in other formats. For instance, facial recognition algorithms have been shown to detect a candidate's emotional expressions, eye contact, and body language, thereby providing non-verbal cues that can assist hiring managers in evaluating the candidate's communication skills (Hemamou et al., 2019). In a similar manner, natural language processing algorithms have the capacity to evaluate the candidate's verbal responses, thereby providing information regarding language proficiency, grammar, and vocabulary usage (Kadyan et al., 2021).

D. Chatbots

AI-based chatbots are extensively utilized in the recruitment process to automate various stages of hiring. The utilization of chatbots in the context of recruitment can facilitate the provision of real-time responses to candidates' queries, the dissemination of information pertaining to job postings, and the facilitation of a streamlined application process. The integration of chatbots with a variety of communication channels, including messaging applications, electronic mail, and social media platforms, facilitate enhanced interaction between candidates and recruitment specialists (Suen & Hung, 2023). AI-powered dialogue systems are being utilized with increasing frequency, particularly in the context of HRM, in the initial communication processes established with candidates. These systems employ natural language processing and machine learning techniques to interact with candidates in the early stages of the recruitment cycle. These chatbots function as virtual assistants within the recruitment process, contributing substantially to both candidate sourcing and selection by answering candidates' queries, gathering essential preliminary information, and providing guidance. These technologies have been shown to accelerate the process, enhance candidate experience, and reduce the workload for HR professionals (Nawaz & Gomes, 2019). Furthermore, the utilization of chatbots has the potential to facilitate the preliminary screening of candidates. By posing predetermined questions, chatbots can identify the most suitable candidates for a position and rank them accordingly. This approach has the potential to significantly reduce the time and effort required for hiring specialists in the initial stages of the recruitment process (Swapna & Arpana, 2021).

E. Gamification

Gamification, a prevalent AI-based recruitment strategy, employs game elements to enhance the hiring process. As demonstrated in the research

undertaken by Tansley et al. (2016), gamification has been shown to be a potent instrument for enhancing candidate engagement and offering insight into the skills and abilities of the candidates. The utilization of points, badges, and leaderboards within the recruitment process has been demonstrated to engender a sense of competition among candidates, thereby motivating them to enhance their performance. Furthermore, gamification can assist organizations in attracting and retaining the most talented candidates. It has the capacity to increase user engagement and motivation, thereby providing a more positive user experience. In the context of recruitment, this can assist organizations in cultivating a favorable brand image and attracting a greater number of candidates (Ergle & Ludviga, 2018).

F. Virtual Reality Assessments

Virtual reality (VR) assessments have emerged as a new tool in AI-based recruitment strategies, offering recruitment specialists an innovative and immersive way to evaluate job candidates' technical and practical skills. The utilization of simulated environments in VR assessments facilitates the evaluation of candidates' performance in various job-related tasks, thereby enabling hiring professionals to assess candidates' abilities and aptitudes in real-world scenarios. Guichet et al. (2022) posit that a significant proportion of the surveyed companies have indicated their interest in exploring the potential of VR assessments for the enhancement of their hiring processes. A notable benefit of VR assessments is their capacity to curtail the time and financial outlay typically devoted to conventional face-to-face evaluations. To illustrate this point, it is notable that VR assessments have the potential to obviate the necessity for costly equipment, travel expenses, and on-site testing facilities. Furthermore, VR assessments can be accessed remotely, enabling hiring professionals to more easily evaluate candidates in different locations.

G. Social Media Screening

The process of social media screening entails the systematic analysis of candidates' online presence, with the objective of ascertaining their interests, personality traits, and values. The utilization of social media screening has been demonstrated to yield valuable insights into candidates' suitability for a position and their cultural congruence with the organizational ethos (Jeske & Shultz, 2015). AI-powered recruitment systems conduct a comprehensive data collection process at this stage by scanning candidate profiles via social media and online career platforms. The data obtained is then analyzed using natural language processing techniques, with a focus on the digital posts, language use, and content of the candidates. Furthermore, a process of semantic matching is undertaken between job descriptions and candidate profiles, with the objective

of determining the degree of suitability for the position. The collected data is then analyzed, and the most suitable candidates are evaluated using automated scoring algorithms. This process guides the recruitment process.

H. Predictive Analytics

Predictive analytics constitutes an AI-based recruitment technique that is especially well-suited to large organizations with substantial recruitment data. The analysis of past recruitment data by recruitment specialists enables the identification of sources that have historically provided the most qualified candidates, the prediction of future recruitment needs, and the planning of recruitment activities accordingly. This technique is particularly useful for organizations in rapidly growing sectors such as technology or healthcare (Albassam, 2023).

3.2. Risks and Ethical Considerations

AI-based recruitment strategies offer significant advantages, but they also have various limitations. Among these limitations is the inability of AI to comprehensively evaluate all factors that affect a candidate's job performance. Qualities such as cultural fit, teamwork aptitude, communication skills, and situational flexibility can be decisive for job success. However, because these types of characteristics are difficult to measure and quantify, they may not be adequately represented in algorithmic evaluation processes (Albassam, 2023).

Another significant issue is the risk that AI systems may reproduce existing biases present in the data on which they are trained. In the event that the system has been trained on data that has historically contained discriminatory or imbalanced patterns, this has the potential to result in the perpetuation of such inequalities within the hiring process. Consequently, reliance on AI-based hiring tools alone may result in the exclusion of candidates who, despite not fully meeting predefined criteria, may in fact possess significant potential (Yarger et al. 2019). For instance, if the algorithm is trained on biased data or criteria, it may erroneously exclude qualified candidates from the selection pool. One of the most significant sources of bias in machine learning algorithms is the labels used as "real data" during the training process. When such labels are found to be biased, it is reasonable to expect that the underlying algorithms will reproduce these biases. The presence of bias in labels can be attributed to a variety of factors. This is particularly pertinent if the labels are based on past human decisions, in which case the bias can be directly transferred from the decision-makers to the system. To illustrate this point, consider the context of credit assessment. If an algorithm is trained exclusively on past approval decisions rather than on the outcomes of past credit assessments, the system

may learn and reproduce biases inherent in these decision-making processes (Fu et al., 2020). Although AI-based hiring strategies offer many advantages, organizations should be aware of the ethical issues surrounding their use. Taking proactive steps to ensure privacy and fairness can help organizations minimize potential risks and ethical concerns while leveraging AI technology to improve their hiring processes (Hunkenschrieder & Luetge, 2022).

3.3. Automated Resume Evaluation

To provide a thorough understanding of automation in contemporary recruitment, this section examines several essential technological integrations by evaluating AI-driven recruitment and job-search infrastructure, automated application protocols, and the shifting dynamics of preliminary interviews by contrasting AI-conducted sessions using realistic visual synthesis with human-led processes supported by AI. Through a comprehensive review of these domains, the following section elucidates the transformative impact of AI on each stage of the recruitment continuum.

3.3.1. AI-Driven Recruitment Process with Human-Led First Interview

This recruitment model represents a hybrid human–AI decision-making framework in which AI is used to optimize early-stage processes, while critical qualitative evaluations remain under human control (Kayalvizhiroja & Krishnan, 2025). The process begins with the definition of job requirements, where organizational needs, required competencies, and role-specific expectations are formally specified. Based on these inputs, an AI-generated job description is produced. This step ensures linguistic clarity, consistency, and alignment with market standards while reducing manual drafting effort. Once the job description is finalized, the system publishes the listing across multiple recruitment channels, including websites, mobile applications, and third-party platforms. As a result, candidate applications are collected through a centralized system. AI then performs candidate scoring, analyzing uploaded CVs in terms of skills, professional experience, educational background, and overall role fit. Using these metrics, the system identifies high-potential candidates who demonstrate the strongest alignment with the job requirements. For shortlisted candidates, the system initiates automated interview scheduling. Candidates receive email invitations that direct them to a self-service interface, allowing them to select an available interview time slot. This automation minimizes administrative overhead and improves candidate experience. The first interview is conducted by a human recruiter, who evaluates candidates through structured or semi-structured interviews and records qualitative notes.

These notes, together with candidate CVs and original job requirements, are subsequently analyzed through AI-based crossmatching. Based on this combined evaluation, a final shortlist of suitable candidates is generated. Candidates who do not progress further in the process receive automated feedback, ensuring transparency and timely communication (See in Figure 1).

Within contemporary recruitment landscapes, organizations are increasingly adopting AI-driven tools that align closely with this hybrid model. For example, platforms such as AgentHR use machine learning and intelligent automation to screen resumes, prioritize candidate pipelines, and reduce manual screening workload, allowing recruiters to focus on high-value interactions. In practice, organizations are adopting AI-driven recruitment tools that reflect this hybrid Human-AI model. Instead of replacing recruiters, these systems are aiming to automate early-stage tasks to reduce human decision-makers' workload (https://agenthr.ai/). Moreover, AgentHR applies machine learning and intelligent automation to CV screening and candidate prioritization. By reducing the time for these activities, recruiters are able to focus more on candidate interaction, evaluation, and strategic hiring decisions. Similarly, LinkedIn's Hiring Assistant shows how AI agents are being integrated into a large-scale recruitment environment. The system uses a global talent database, recommending qualified profiles, etc. to support recruiters. This allows for improving shortlist quality, final decisions, and hiring decisions remain under control.

Industry analysts also show that AI-powered candidate sources and engagement are transforming HR operations globally. Tools now integrate natural language processing (NLP) and predictive analytics to identify candidates who might be overlooked by traditional search methods, recommend the best channels to advertise roles, and maintain candidate communication with automated chatbots to keep applicants informed and engaged. HR operations worldwide are being reshaped by AI-powered sourcing and engagement technologies. NLP and predictive analytics help organizations to identify/find suitable candidates who may be overlooked by traditional keyword-based searches, optimize job advertising channels, and maintain consistent communication with automated messaging by chatbots. Across a wide range of sectors, from tech companies to larger enterprises, AI is now regularly used for the early stages, such as CV parsing, shortlist generation, and automated candidate engagement, etc. As a summary, the real-world applications show that hybrid recruitment models are not only feasible but also scalable and sustainable in modern talent acquisition practices (https://business.linkedin.com/in/en/hire/resources/hr-glossary/ai-in-hr-hiring)

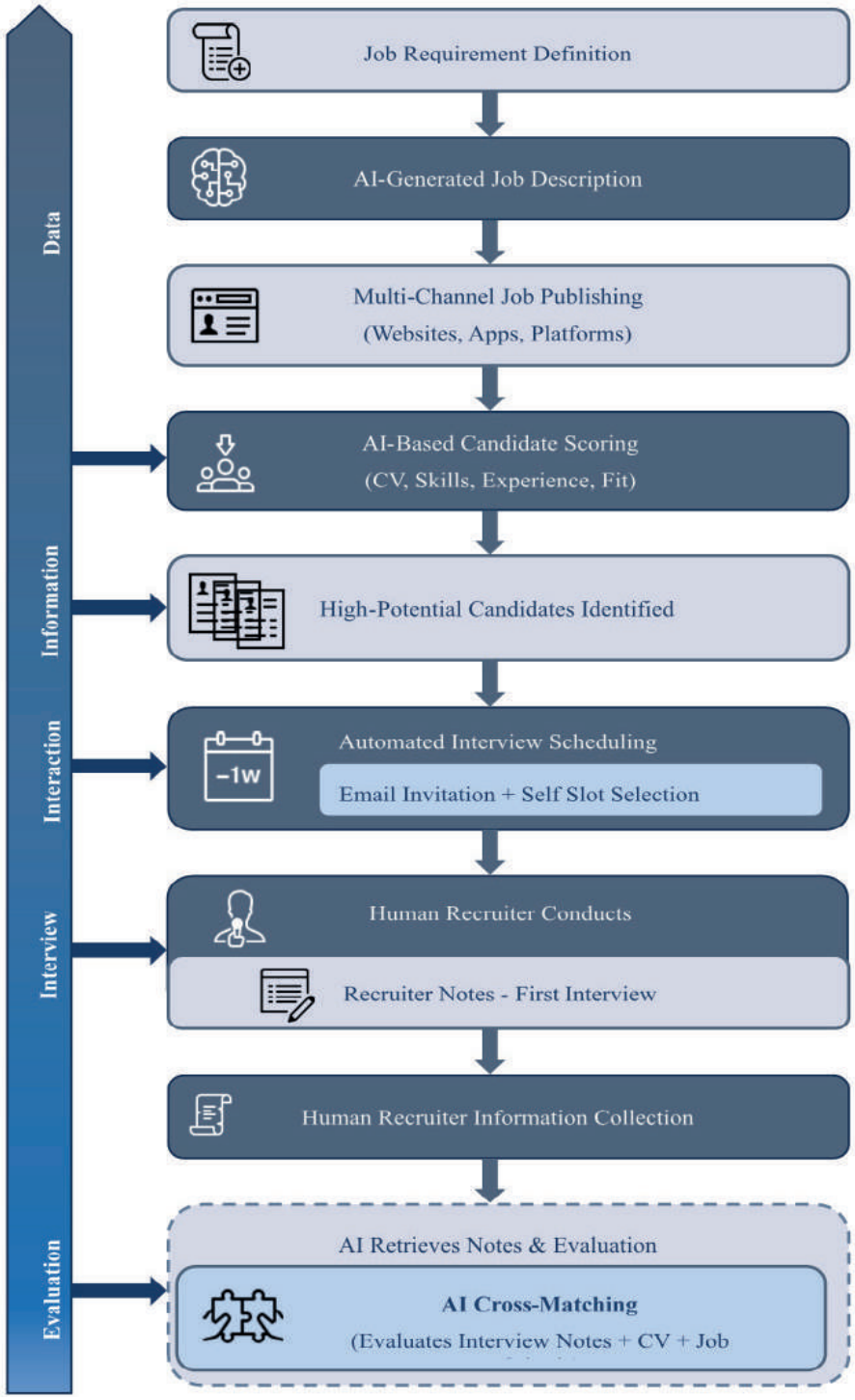


Figure 1- AI-Driven Recruitment Process with Human-Led First Interview

3.3.2. AI-Conducted First Interview Using Realistic Visual AI

This recruitment model represents a fully AI-driven early interview process, designed for scalability, standardization, and objective evaluation. Similar to the hybrid model, the process begins with job requirement definition, followed by the generation of a detailed AI-generated job description. The listing is then published across multiple platforms, and candidate applications are collected.

AI conducts candidate scoring by evaluating CV content against job-specific criteria. High-potential candidates are automatically identified and invited to participate in the next stage. The system manages automated interview scheduling, allowing candidates to select interview times via a self-service interface. Unlike traditional models, the first interview is conducted by a realistic visual AI interviewer. This AI system can conduct multiple interviews simultaneously, enabling significant scalability without proportional increases in cost or HRM. During interviews, the AI collects structured outputs, including competency-based scores, behavioral indicators, and interview transcripts. These outputs are systematically evaluated and cross-matched with job requirements on a criterion-by-criterion basis. Based on this evaluation, the system generates a new AI-driven shortlist. Candidates who do not meet the defined thresholds receive automated feedback, ensuring consistent communication and reducing bias introduced by human subjectivity (See in Figure 2).

In recent years, AI-conducted interviewing has progressed from a conceptual research topic to practical usage in real-world business environments. As a part of AI, conversational agents and virtual interview systems are now used to run structured interviews, generate transcripts/minutes, and produce evaluation metrics that support hiring decisions. (https://www.shortlistd.io/blog/ai-voice-interviews-outperform-human-recruiters-2025-research-analysis).

AI interview simulation shows how large language models can create personalized yet standardized interview experiences. By dynamically adapting interview questions to candidate responses over the job requirements, these systems balance realism and scalability, offering organizations a consistent and repeatable approach to early-stage candidate assessment (Nguyen et al., 2025).

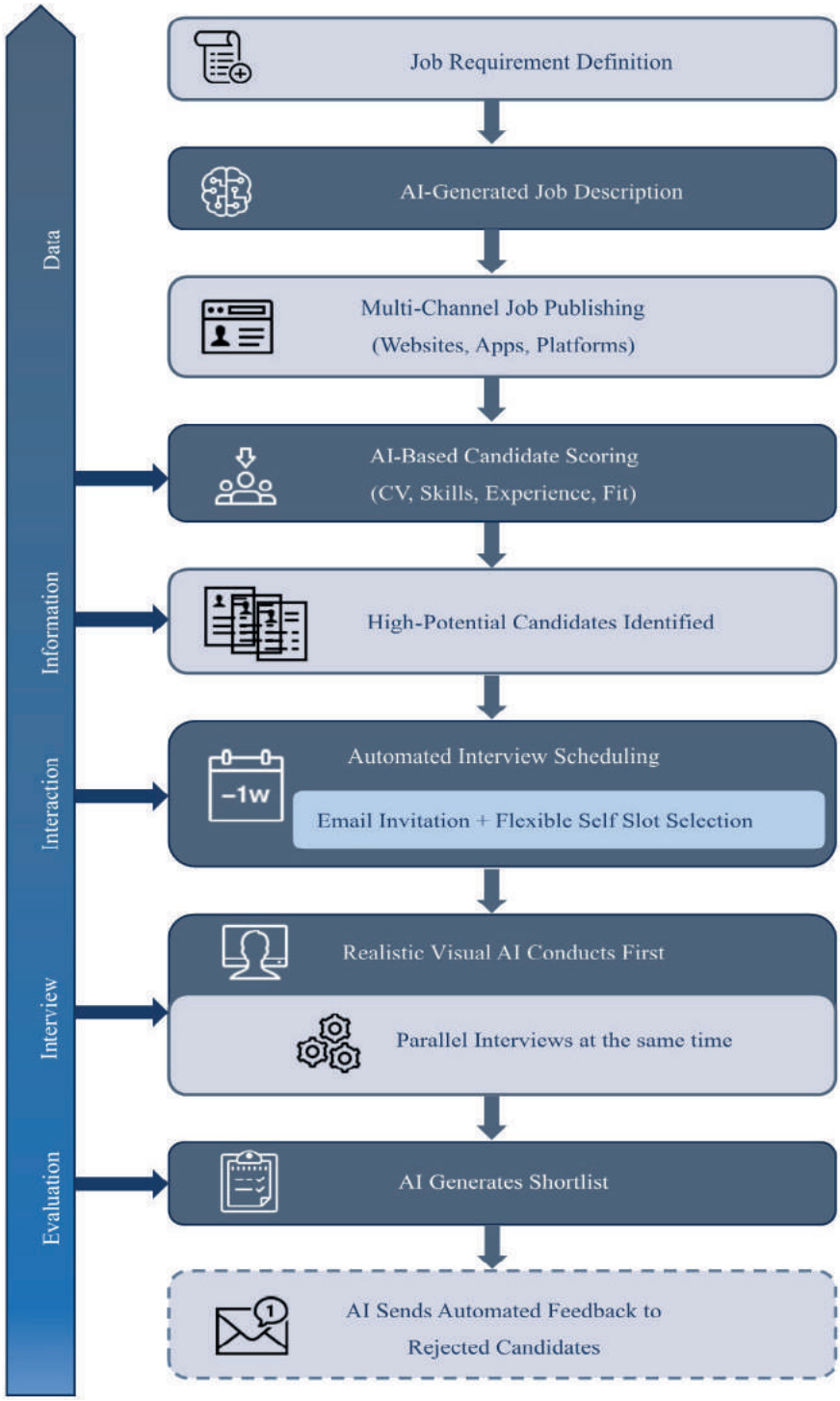


Figure 2- AI-Conducted First Interview Using Realistic Visual AI

3.3.3. AI-Supported Job Search and Automated Application System

This system focuses on supporting job seekers through an AI-assisted job search and application optimization process. The process begins when a user registers for the AI-powered job search platform. Upon registration, the user uploads their CV, which is then analyzed by AI. The AI identifies key skills, experience patterns, and role-relevant competencies. Following this analysis, the system scores the user's strengths and performs CV optimization, improving structure, clarity, and alignment with labor market expectations.

The AI then searches across multiple job listing platforms to identify positions for which the user has the highest probability of success. For each identified job listing, the system performs job-specific CV customization, tailoring content to match the required skills and qualifications.

After optimization, the AI automatically applies to the most suitable job listings on behalf of the user. Throughout this process, the system continuously collects application-level data. Finally, the platform generates and shares statistical insights with the user. These insights may include the number of applications submitted, match scores, response rates, and comparative performance metrics, enabling users to make informed career decisions (See in Figure 3).

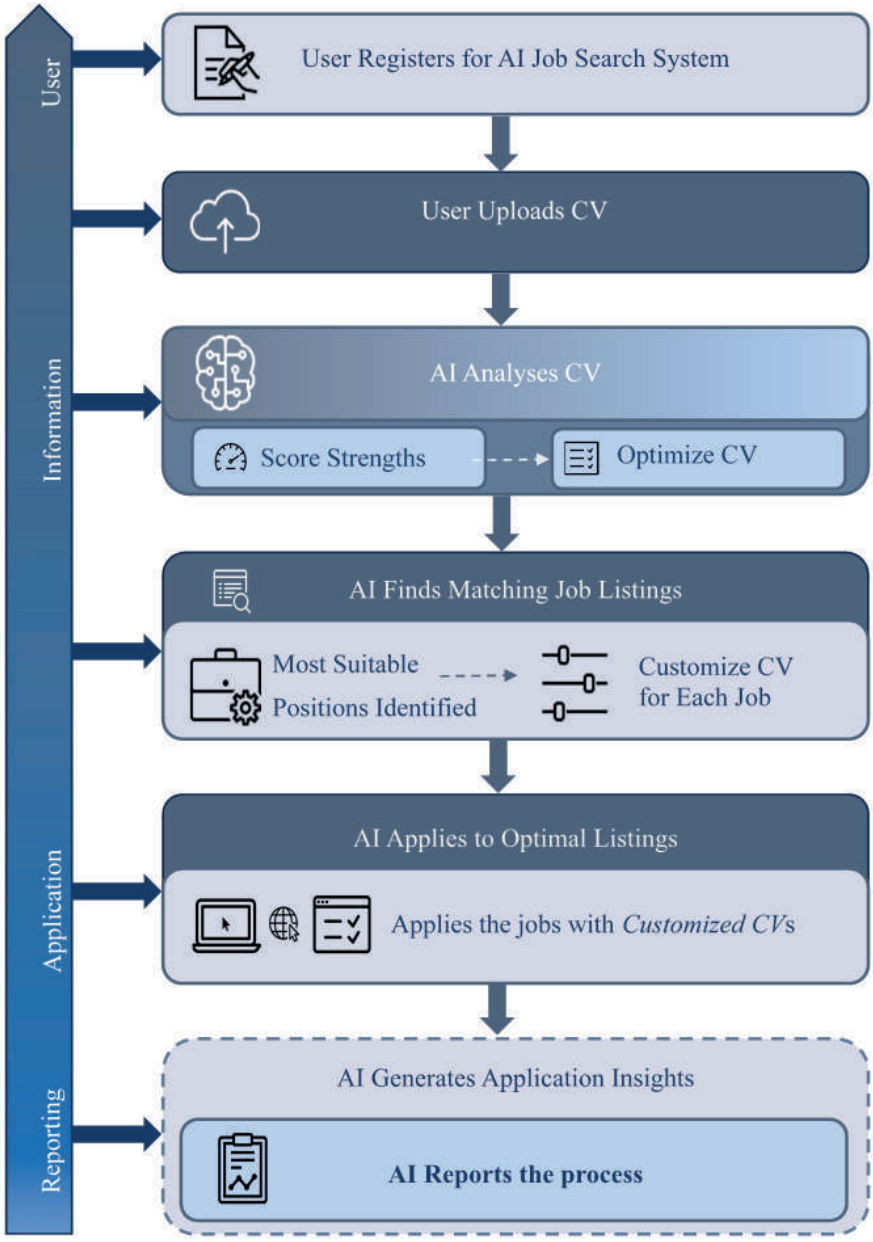


Figure 3 -AI-Supported Job Search and Automated Application System

With the rapid evolution of algorithmic processing, a growing number of AI-powered job search and matching platforms have emerged that align closely with the described system, using automated CV analysis to identify key competencies and improve job-market fit. For example, services like AIJobMatch (https://aijobmatch.io/) analyze uploaded resumes to extract skills and experience, then generate ranked job matches tailored to the candidate's profile, demonstrating the practical application of AI-driven profile interpretation and job recommendation.

Similarly, AI-based CV optimization tools such as MatchMe AI (https://www.matchme-ai.com/) provide automated suggestions for strengthening resume content and improving match scores against specific job requirements, helping job seekers present themselves more effectively to potential employers.

Platforms and tools in the broader ecosystem, such as AI-enhanced search features on LinkedIn that allow NLP job queries and more relevant job discovery, show how AI can complement traditional job boards by aligning candidate inputs with appropriate opportunities (Weatherbed, 2025). This has been driven by the rapid proliferation of algorithmic solutions in the job market, and consequently, a considerable array of AI-powered recruitment and matching platforms has been developed, which have been in close alignment with the proposed framework using CV analysis to optimize candidate-market matching.

4. Conclusion

The rapid development of technology in recent years has profoundly changed how HRM management operates. The accelerating pace of technological advancement in recent times has resulted in the increased accessibility of AI-based solutions and their concomitant strategic importance in the realm of HRM. The transition from conventional recruitment methodologies to data-driven and AI-supported approaches signifies a transformative shift that not only redefines the process design paradigm but also the decision-making logic, the distribution of responsibility, and the candidate experience. This transformation extends beyond mere operational gains, such as reduced costs and efficient time management, to enable recruitment decisions to be produced in a more consistent, traceable, and justifiable manner.

The primary objective of this chapter is to examine processes towards AI-supported implementations as a substitute for conventional recruitment interviews. Therefore, it is aimed to seek how elucidate the potential ramifications of AI-assisted processes on the employee selection landscape. In this section, the parties have used step by step diagram to show how

the AI-supported interview methodology works. This process is considered instrumental in ensuring a comprehensive understanding of the potential advantages and disadvantages.

The utilization of AI-based recruitment algorithms enables human resources professionals to allocate their time and efforts towards more strategic and value-added activities, as these algorithms assume responsibility for routine and repetitive tasks. In businesses experiencing high application volumes, the implementation of such systems has been shown to facilitate more efficient and accurate management of laborious processes, such as the screening and pre-screening of CVs. A more accurate assessment of candidates' qualifications and competencies facilitates the placement of the right people in suitable positions, thus minimizing errors stemming from subjective evaluations. This approach is conducive to businesses making more robust investments in talent management and gaining a competitive advantage. It is anticipated that, in the long term, the integration of AI will result in a reduction in employee turnover rates and a reduction in the time required for recruitment (Aguinis et al., 2024). Consequently, the utilization of AI-supported applications within the domain of HRM has emerged as a pivotal element, contributing not only to the enhancement of operational efficiency but also to the fortification of the strategic sustainability of organizations.

Overall, AI in recruitment has many benefits, but cannot replicate the understanding, empathy, and contextual awareness brought to the process by human recruiters. Human intuition is crucially important in assessing factors that are difficult to quantify, such as a candidate's cultural fit, motivation, and potential for growth within the organization. Therefore, further studies are suggested to evaluate perceptions and attitudes towards AI-conducted interviews.

References

Adil. (2025). *Game-changing research: AI interviews beat human recruiters*. Shortlistd. https://www.shortlistd.io/blog/ai-voice-interviews-outperform-human-recruiters-2025-research-analysis

AgentHR. (n.d.). *AI agents for HR operations, onboarding, and recruitment*. https://agenthr.ai/

Aguinis, H., Beltran, J. R., & Cope, A. (2024). How to use generative AI as a human resource management assistant. *Organizational Dynamics, 53*(1), Article 101029. https://doi.org/10.1016/j.orgdyn.2024.101029

AIJobmatch.io. (n.d.). *AI-powered job search and resume matching platform*. https://aijobmatch.io/

Aka, A., Palikot, E., Ansari, A., & Yazdani, N. (2025). Better together: Quantifying the benefits of AI-assisted recruitment. *arXiv*. https://doi.org/10.48550/arXiv.2507.08029

Albassam, W. A. (2023). The power of artificial intelligence in recruitment: An analytical review of current AI-based recruitment strategies. *International Journal of Professional Business Review, 8*(6), Article e02089. https://doi.org/10.26668/businessreview/2023.v8i6.2089

Asike, A., Dinsar, A., & Muslimin, U. (2025). Human resource management transformation in the digital era: Literature review. *Jurnal Ekonomi Ichsan Sidenreng Rappang, 4*(2), 508–518. https://doi.org/10.61912/jeinsa.v4i2.327

Bakal, C., Ayden, C., Kişman, Z. A., & Eşidir, O. V. (2026). İşe alım süreçlerinde yapay zeka kullanımının avantajları ve dezavantajları [Advantages and disadvantages of using artificial intelligence in recruitment processes]. *Iğdır Üniversitesi Sosyal Bilimler Dergisi*, (41), 211–231.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1016/S0742-3322(00)17018-4

Cardoso, A., Mourão, F., & Rocha, L. (2021). The matching scarcity problem: When recommenders do not connect the edges in recruitment services. *Expert Systems with Applications, 175*, Article 114764. https://doi.org/10.1016/j.eswa.2021.114764

Chen, Z. (2023a). Collaboration among recruiters and artificial intelligence: Removing human prejudices in employment. *Cognition, Technology & Work, 25*(1), 135–149. https://doi.org/10.1007/s10111-022-00716-0

Chen, Z. (2023b). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications, 10*, Article 567. https://doi.org/10.1057/s41599-023-02079-x

Dadaboyev, S. M. U., Abdullayeva, J., Abbosova, N., Suleymenova, A., & Mamadjanova, K. (2025). Role of artificial intelligence in employee recruitment: Systematic review and future research directions. *Discover Global Society, 3*(1), 1–16. https://doi.org/10.1007/s44282-025-00246-w

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review, 96*(1), 108–116.

Derous, E., & Ryan, A. M. (2018). When your resume is (not) turning you down: Modelling ethnic bias in resume screening. *Human Resource Management Journal, 29*(2), 113–130. https://doi.org/10.1111/1748-8583.12217

Dunlop, P. D., Holtrop, D., & Wee, S. (2022). How asynchronous video interviews are used in practice: A study of an Australian-based AVI vendor. *International Journal of Selection and Assessment, 30*(3), 339–350. https://doi.org/10.1111/ijsa.12372

Ergle, D., & Ludviga, I. (2018). Use of gamification in human resource management: Impact on engagement and satisfaction. In *Proceedings of the 10th International Scientific Conference Business and Management*. https://doi.org/10.3846/bm.2018.45

Faugoo, D. (2024). AI-driven recruitment and selection: Enhanced HR decision-making with accrued benefits of organizational success. *International Journal of Business and Technology Management, 6*(3), 529–536. https://doi.org/10.55057/ijbtm.2024.6.3.47

Fu, R., Huang, Y., & Singh, P. V. (2020). Artificial intelligence and algorithmic bias: Source, detection, mitigation, and implications. In *Pushing the boundaries: Frontiers in impactful OR/OM research* (pp. 39–63). INFORMS. https://doi.org/10.1287/educ.2020.0215

Guichet, P. L., Huang, J., Zhan, C., Millet, A., Kulkarni, K., Chhor, C., Mercado, C., & Fefferman, N. (2022). Incorporation of a social virtual reality platform into the residency recruitment season. *Academic Radiology, 29*(6), 935–942. https://doi.org/10.1016/j.acra.2021.05.024

Hemamou, L., Felhi, G., Martin, J.-C., & Clavel, C. (2019). Slices of attention in asynchronous video job interviews. In *Proceedings of the 2019 8th International Conference on Affective Computing and Intelligent Interaction (ACII)* (pp. 1–7). IEEE. https://doi.org/10.1109/acii.2019.8925439

Horodyski, P. (2023a). Applicants' perception of artificial intelligence in the recruitment process. *Computers in Human Behavior Reports, 11*, Article 100303. https://doi.org/10.1016/j.chbr.2023.100303

Horodyski, P. (2023b). Recruiter's perception of artificial intelligence (AI)-based tools in recruitment. *Computers in Human Behavior Reports, 10*, Article 100298. https://doi.org/10.1016/j.chbr.2023.100298

Hunkenschroer, A. L., & Luetge, C. (2022). Ethics of AI-enabled recruiting and selection: A review and research agenda. *Journal of Business Ethics, 178*(4), 977–1007. https://doi.org/10.1007/s10551-022-05049-6

Işıldak, B., & Tunca, M. (2018). Havalimanı hizmetlerinde müşteri memnuniyetini etkileyen faktörler üzerine bir araştırma. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 23*(1), 241–255. https://izlik.org/JA87KL96FX

Jeske, D., & Shultz, K. S. (2016). Using social media content for screening in recruitment and selection: Pros and cons. *Work, Employment and Society, 30*(3), 535–546. https://doi.org/10.1177/0950017015613746

Johnson, R. D., Stone, D. L., & Lukaszewski, K. M. (2021). The benefits of eHRM and AI for talent acquisition. *Journal of Tourism Futures, 7*(1), 40–52. https://doi.org/10.1108/JTF-02-2020-0013

Kadyan, V., Singh, A., Mittal, M., & Abualigah, L. (2021). *Deep learning approaches for spoken and natural language processing*. Springer. https://doi.org/10.1007/978-3-030-79778-2

Kayalvizhiroja, T., & Krishnan, J. (2025). HR adoption and perception of AI-driven recruitment: A hybrid approach for the IT sector. *Leadership and Organizational Insights, 1*(2), 20–27. https://doi.org/10.64229/xx2pfe50

Kodiyan, A. A. (2019). *An overview of ethical issues in using AI systems in hiring with a case study of Amazon's AI-based hiring tool* [Unpublished manuscript]. ResearchGate. https://www.researchgate.net

Küçükesmen, E., Şimşek, A., & Türkoğlu, M. E. (2023). Dijital yerli(ler) yönetici adaylarının sosyal medya bağımlılık düzeyleri [Social media addiction levels of digital native manager candidates]. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 28*(2), 155–179.

Kumar, C. (2025). From automation to ethics: Responsible AI in human resource management across industries with insights from the power sector. *Research Review International Journal of Multidisciplinary, 10*(4), 63–81. https://doi.org/10.31305/rrijm.2025.v10.n4.009

Langer, M., & König, C. J. (2023). Introducing a multi-stakeholder perspective on opacity, transparency and strategies to reduce opacity in algorithm-based human resource management. *Human Resource Management Review, 33*(1), Article 100881. https://doi.org/10.1016/j.hrmr.2021.100881

MatchMe AI. (n.d.). *AI CV builder and recruitment matching platform*. https://www.matchme-ai.com/

Milhem, M., Ateeq, A., Al Astal, A., & Almeer, S. (2024). Digital transformation in HRM: Navigating the future of human resource management. In *Business sustainability with artificial intelligence (AI): Challenges and opportunities* (Vol. 2, pp. 23–33). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-71318-7_3

Nawaz, N., & Gomes, A. M. (2019). Artificial intelligence chatbots are new recruiters. *International Journal of Advanced Computer Science and Applications, 10*(9), 1–6. https://doi.org/10.2139/ssrn.3521915

Nguyen, T. T. H., Nguyen, T. D. Q., Cao, H. L., Tran, T. C. T., Truong, T. C. M., & Cao, H. (2025). SimInterview: Transforming business education through large language model-based simulated multilingual interview training system. *arXiv*. https://doi.org/10.48550/arXiv.2508.11873

Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020). Mitigating bias in algorithmic hiring: Evaluating claims and practices. In *Proceedings of the 2020 ACM Conference on Fairness, Accountability, and Transparency* (pp. 469–481). ACM. https://doi.org/10.1145/3351095.3372828

Raub, M. (2018). Bots, bias and big data: Artificial intelligence, algorithmic bias and disparate impact liability in hiring practices. *Arkansas Law Review, 71*(2), 529–570.

Rodgers, W., Murray, J. M., Stefanidis, A., Degbey, W. Y., & Tarba, S. Y. (2023). An artificial intelligence algorithmic approach to ethical decision-making in human resource management processes. *Human Resource Management Review, 33*(1), Article 100925. https://doi.org/10.1016/j.hrmr.2022.100925

Roy, P. K., Chowdhary, S. S., & Bhatia, R. (2020). A machine learning approach for automation of resume recommendation system. *Procedia Computer Science, 167*, 2318–2327. https://doi.org/10.1016/j.procs.2020.03.284

Sandeep, M. M., Lavanya, V., & Balakrishnan, J. (2025). Leveraging AI in recruitment: Enhancing intellectual capital through resource-based view and dynamic capability framework. *Journal of Intellectual Capital, 26*(2), 404–425. https://doi.org/10.1108/JIC-05-2024-0155

Singh, R., Joshi, A., Dissanayake, H., Nainanayake, D., & Kumar, V. (2025). Harnessing artificial intelligence and human resource management for circular economy and sustainability: A conceptual integration. *Sustainability, 17*(15), 1–19. https://doi.org/10.3390/su17157054

Sandeep, M. M., Lavanya, V., & Balakrishnan, J. (2025). Leveraging AI in recruitment: Enhancing intellectual capital through resource-based view and dynamic capability framework. *Journal of Intellectual Capital, 26*(2), 404–425. https://doi.org/10.1108/JIC-05-2024-0155

Soni, M., Gomathi, S., & Adhyaru, Y. B. K. (2020). Natural language processing for the job portal enhancement. In *Proceedings of the 2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1–4). IEEE. https://doi.org/10.1109/ICSSS49621.2020.9201922

Suen, H.-Y., & Hung, K.-E. (2023). Building trust in automatic video interviews using various AI interfaces: Tangibility, immediacy, and transparency. *Computers in Human Behavior, 143*, Article 107713. https://doi.org/10.1016/j.chb.2023.107713

Swain, P., & Malik, A. (2025). The role of AI in recruitment: A systematic literature review. *GRS Journal of Multidisciplinary Research and Studies, 2*(6), 21–30. https://doi.org/10.5281/zenodo.15572327

Swapna, H. R., & Arpana, D. (2021). Chatbots as a game changer in e-recruitment: An analysis of adaptation of chatbots. In *Lecture Notes in Networks and Systems* (Vol. 201, pp. 61–69). Springer. https://doi.org/10.1007/978-981-16-0666-3_7

Tansley, C., Hafermalz, E., & Dery, K. (2016). Talent development gamification in talent selection assessment centres. *European Journal of Training and Development, 40*(7), 490–512. https://doi.org/10.1108/ejtd-03-2016-0017

Vial, G. (2021). Understanding digital transformation: A review and a research agenda. In *Managing digital transformation* (pp. 13–66). Routledge.

Vijayasree, D. (n.d.). Artificial intelligence: Conceptual foundations and emerging trends in human resource management. In *Handbook of modern practices in commerce and management* (Vol. 9). https://doi.org/10.59646/541

Weatherbed, J. (2025, March). LinkedIn's new AI search tool lets you describe your ideal job. *The Verge*. https://www.theverge.com/news/662490/linkedin-ai-job-search-tool-availability

Willie, M. (2025). Leveraging digital resources: A resource-based view perspective. *Golden Ratio of Human Resource Management, 5*(1), 1–14. https://doi.org/10.52970/grhrm.v5i1.415

Yanamala, K. K. R. (2021). Integration of AI with traditional recruitment methods. *Journal of Advanced Computing Systems, 1*(1), 1–7. https://doi.org/10.69987/JACS.2021.10101

Yarger, L., Cobb Payton, F., & Neupane, B. (2020). Algorithmic equity in the hiring of underrepresented IT job candidates. *Online Information Review, 44*(2), 383–395. https://doi.org/10.1108/OIR-10-2018-0334

Chapter 2

Shadow AI and Organizational Information Security: Risks, Challenges, and Governance Strategies

Vahid Sinap[1]

Abstract

The rapid diffusion of generative and agentic artificial intelligence has enabled employees to use powerful AI tools outside formal organizational oversight. This phenomenon, known as shadow AI, can improve productivity, creativity, and problem-solving while creating significant risks for information security, privacy, intellectual property, regulatory compliance, and decision quality. This chapter examines the conceptual foundations, organizational drivers, and security implications of shadow AI from a management information systems perspective. It explains how technological accessibility, task–technology misfit, work pressure, inadequate organizational tools, and unclear policies encourage unauthorized AI use. The chapter also discusses risks related to data leakage, unreliable outputs, prompt injection, excessive agency, undocumented integrations, and weak accountability. A risk-based governance approach is proposed, combining clear policies, approved AI tools, technical controls, employee training, human oversight, monitoring, and adaptive authorization mechanisms. The chapter concludes that effective shadow AI management depends on visibility, proportionality, accountability, and employee enablement.

1. Introduction

Artificial intelligence (AI) has rapidly evolved from a specialized technological capability into an accessible component of everyday organizational work. Generative AI systems can produce text, images, software code, analyses, and other forms of digital content in response to natural-language instructions, substantially expanding the range of tasks that can be supported by AI (Feuerriegel et al., 2024). Employees now use AI-powered chatbots, coding

1 Assoc. Prof. Dr., Ufuk University, vahidsinap@gmail.com, https://orcid.org/0000-0002-8734-9509

https://doi.org/10.58830/ozgur.pub1366.c5528

assistants, analytical platforms, browser extensions, and productivity applications to prepare reports, summarize documents, analyze data, communicate with customers, and support decision-making. Experimental evidence indicates that generative AI can reduce the time required to complete professional writing tasks while improving output quality (Noy & Zhang, 2023). Similarly, a large-scale study of customer-support employees found that access to a generative AI assistant increased worker productivity, although the magnitude of this improvement differed across employees (Brynjolfsson et al., 2025). These capabilities make AI tools attractive not only to organizations pursuing formal digital transformation initiatives but also to individual employees seeking faster and more effective ways to perform their work.

The accessibility of these technologies has gradually shifted part of organizational AI adoption away from centrally coordinated information technology processes. Employees can begin using publicly available AI applications, personal subscriptions, external application programming interfaces, and AI functions embedded in third-party software without requiring substantial technical expertise or organizational infrastructure. As a result, the AI tools formally approved by an organization may differ considerably from those actually used in its daily operations. The use of AI tools, models, or applications without the knowledge, authorization, or oversight of relevant organizational units is commonly described as shadow AI (Puthal et al., 2025). These units may include information technology, cybersecurity, legal, data governance, procurement, and regulatory compliance departments.

Shadow AI is conceptually rooted in the broader phenomenon of shadow information technology. Shadow IT refers to technological systems, applications, or services that employees use or develop outside formally authorized organizational IT arrangements (Haag & Eckhardt, 2017). However, shadow AI extends this phenomenon by introducing systems that do more than store, transfer, or present information. AI applications can process organizational data, identify patterns, generate new content, recommend actions, and influence human decisions. Consequently, the risks associated with shadow AI may continue to affect an organization even after the initial interaction with an unauthorized tool has ended. Data submitted to an external AI service may be retained or processed beyond the organization's direct control, while AI-generated outputs may subsequently be incorporated into reports, software, communications, or decision processes without a clear record of their origin.

The emergence of shadow AI should not be explained exclusively through employee negligence or deliberate noncompliance. Research on shadow IT shows that employees frequently adopt unauthorized technologies because formally provided systems do not adequately meet their operational needs (Haag & Eckhardt, 2024). Employees may also encounter lengthy approval procedures, limited access to organizational AI systems, insufficient technical support, or tools that do not offer the functionality required for a particular task. At the same time, demands for higher productivity, faster task completion, experimentation, and innovation may encourage employees to adopt immediately available AI applications. Unauthorized technology use can therefore reflect an attempt to resolve a task–technology mismatch rather than an intention to harm the organization. Haag and Eckhardt (2024) consequently argue that shadow technology should be managed by addressing both cybersecurity requirements and legitimate user needs instead of relying solely on restrictive controls.

This perspective reveals a fundamental tension surrounding shadow AI. On the one hand, employee-driven AI adoption may facilitate experimentation, creativity, learning, and rapid problem-solving. It can also reveal unmet technological needs that formal organizational systems have failed to address. On the other hand, the absence of organizational oversight may expose sensitive information, intellectual property, personal data, internal communications, source code, customer records, and strategic documents to external providers. Puthal et al. (2025) associate shadow AI with data leakage, security breaches, regulatory noncompliance, model vulnerabilities, and an expanded organizational attack surface. The risks are not limited to the confidentiality of data. Generative AI systems may also produce inaccurate, biased, fabricated, or misleading outputs, creating threats to information integrity and the reliability of organizational decisions. The Generative Artificial Intelligence Profile published by the National Institute of Standards and Technology identifies risks concerning data privacy, information security, confabulation, intellectual property, harmful bias, and human overreliance as important considerations in the organizational use of generative AI (National Institute of Standards and Technology [NIST], 2024).

Limited visibility makes these risks particularly difficult to manage. When an AI application is adopted outside formal organizational processes, managers may be unable to determine which tools are being used, what information is entered into them, where the information is processed, how long it is retained, or whether generated outputs are verified before use. Unauthorized applications may also bypass existing controls for vendor assessment, access authorization, data classification, procurement, incident reporting, and

regulatory compliance. Traditional information security arrangements generally protect known systems, recognized users, and observable data flows. Shadow AI creates an oversight gap because the organization cannot effectively assess or control AI uses whose existence it has not identified. This gap becomes increasingly important as AI tools are integrated into routine workflows and begin to affect organizational knowledge, business processes, and managerial decisions.

Shadow AI should therefore be viewed as more than an isolated cybersecurity problem. From a management information systems perspective, it constitutes a sociotechnical challenge involving the interaction of employees, organizational structures, work requirements, data, digital technologies, and governance mechanisms. Managing this challenge requires technical controls, but technical restrictions alone are unlikely to eliminate informal AI use. Organizations must also understand why employees adopt unauthorized tools, distinguish low-risk experimentation from high-risk practices, provide secure alternatives, establish clear responsibilities, and create accessible procedures for approving new AI applications. The NIST AI Risk Management Framework emphasizes that effective AI risk management should be integrated into organizational policies and processes through the interconnected functions of governing, mapping, measuring, and managing AI risks (NIST, 2023). Its generative AI profile further stresses that risk-management practices must be adapted to the context, objectives, legal obligations, and risk tolerance of each organization (NIST, 2024).

Against this background, this chapter examines shadow AI as an emerging organizational information security phenomenon. It first clarifies the concept and explains the organizational conditions that encourage employees to use unauthorized AI tools. It then evaluates the implications of shadow AI for information confidentiality, privacy, intellectual property, regulatory compliance, cybersecurity, and decision integrity. Finally, it discusses governance strategies through which organizations can increase the visibility and accountability of AI use without unnecessarily suppressing employee initiative and digital innovation. Rather than assuming that all informal AI use is inherently harmful, the chapter adopts a balanced perspective that recognizes both the operational value and the security consequences of employee-driven AI adoption. In doing so, it positions shadow AI at the intersection of information systems management, employee technology behavior, organizational innovation, cybersecurity, and AI governance.

2. Conceptual Foundations and Organizational Drivers of Shadow AI

2.1. Conceptual Boundaries and Manifestations of Shadow AI

Shadow AI can be understood as a contemporary extension of shadow information technology, but the two concepts should not be treated as completely interchangeable. Shadow IT broadly refers to software, hardware, or digital services that organizational members acquire, develop, or use without alignment with the formal IT function (Klotz et al., 2019). Shadow AI represents a more specific form of this phenomenon in which the unauthorized or undisclosed technological resource possesses AI-based capabilities such as content generation, prediction, classification, recommendation, decision support, or autonomous task execution (Puthal et al., 2025). The defining characteristic is therefore not simply the presence of AI but the absence of appropriate organizational visibility, authorization, or governance.

This distinction is important because the use of an externally developed or employee-selected AI application does not automatically constitute shadow AI. An employee may identify an AI tool independently and subsequently disclose it to the relevant organizational units, obtain approval, and use it under agreed security and data-management conditions. Such an arrangement is more appropriately regarded as employee-initiated or business-managed AI rather than shadow AI. Klotz et al. (2019) similarly distinguish covert shadow IT from business-managed IT, in which business units assume responsibility for technological resources while remaining aligned with the formal IT organization. Applying this distinction to AI suggests that organizational alignment, rather than the original source of the technology, determines whether an application remains in the shadows.

Conversely, an officially available AI system can generate shadow AI practices when it is used beyond its approved purpose or under conditions that evade organizational controls. An employee may, for example, use an approved generative AI assistant but enter a category of data that organizational policy prohibits, connect the system to an unauthorized external source, or rely on its output for a decision for which human review is mandatory. Shadow AI may therefore involve both the adoption of an unapproved technology and the unapproved use of an otherwise authorized technology. This broader interpretation is consistent with shadow IT taxonomies that include not only unofficial systems but also the misuse or unintended use of official technological resources (Klotz et al., 2019).

The boundary of shadow AI can be clarified through four interrelated criteria. The first is authorization, referring to whether the application, model, or use case has received formal approval. The second is visibility, which concerns whether IT, cybersecurity, data-governance, or managerial units know that the AI system is being used. The third is governance alignment, referring to whether the use is subject to organizational requirements concerning data handling, vendor assessment, access control, accountability, and human oversight. The fourth is purpose alignment, which indicates whether the AI system is being used for an approved organizational task and within its authorized scope. A practice may therefore become shadow AI when one or more of these conditions are absent, even when the employee does not deliberately intend to conceal the technology.

Shadow AI may appear in multiple forms, ranging from occasional interactions with public chatbots to AI-enabled workflows embedded in routine business processes. Some uses are direct and visible to the employee, such as entering a document into a public generative AI service. Others are less apparent because AI capabilities are integrated into browser extensions, office applications, analytical platforms, customer-management systems, or software-development tools. The growing modularity of AI also allows employees to connect external models to organizational data through application programming interfaces, no-code platforms, custom assistants, and automated agents. Puthal et al. (2025) emphasize that shadow AI can include unauthorized models, tools, and systems operating beyond the supervision of centralized IT and cybersecurity functions.

Table 1 Common Manifestations of Shadow AI in Organizations

Manifestation	**Illustrative employee practice**	**Why the practice constitutes shadow AI**
Public generative AI services	Using a personal account to summarize internal reports, generate correspondence, or analyze organizational documents	The service and its data-processing conditions have not been evaluated or approved by the organization
AI-enabled browser extensions and add-ons	Installing an extension that reads webpages, emails, documents, or meeting content to generate summaries or responses	The AI capability may access organizational information without appearing as a separate organizational system
External coding and analytical tools	Uploading source code, datasets, or technical logs to an external AI assistant for debugging or analysis	The tool operates outside approved development, data-analysis, and vendor-management environments

Employee-built assistants and models	Creating a custom chatbot, fine-tuned model, or retrieval-based assistant using organizational documents	The resulting system may process or reproduce organizational knowledge without registration, testing, or formal ownership
AI-supported no-code automations	Connecting an external model to email, cloud storage, customer records, or business applications through a no-code platform	The integration creates an unapproved data flow and may automate actions outside existing controls
Autonomous or semi-autonomous AI agents	Configuring an agent to retrieve information, communicate with third parties, modify records, or perform multistep tasks	The agent may exercise delegated authority without formal approval, monitoring, or clearly assigned accountability

Note. Developed by the author based on Klotz et al. (2019), Puthal et al. (2025), and Waters-Lynch et al. (2025). The categories are not mutually exclusive, as a single shadow AI practice may combine several tools and forms of automation.

Shadow AI may also differ in its scale, duration, and degree of autonomy. It can be limited to a single employee completing a one-time task or become a shared practice adopted by an entire team. Similarly, some practices remain temporary experiments, whereas others become embedded in recurring workflows and gradually assume operational importance. The latter situation is particularly significant because an AI tool may begin as an informal productivity aid but eventually become an undocumented dependency for a business process. At that point, discontinuing or controlling the tool may become difficult because employees, information flows, and operational routines have already adapted to its presence.

The concept of shadow user innovation further illustrates that informal AI use may extend beyond simple technology adoption. Waters-Lynch et al. (2025) define shadow user innovation as covert, employee-initiated value creation enabled by digital tools that can be used and concealed relatively easily. From this perspective, employees do not merely select an unauthorized application; they may design new workflows, combine models with organizational knowledge, and develop task-specific AI solutions. Such activities can reveal valuable opportunities for organizational learning and innovation. Nevertheless, their covert character prevents the organization from evaluating, documenting, scaling, or governing the resulting practices. Shadow AI should consequently be understood as a continuum that ranges from informal individual assistance to the concealed redesign of organizational processes.

2.2. Organizational and Behavioral Drivers of Shadow AI

The emergence of shadow AI cannot be adequately explained by a single motive. A useful starting point is the framework developed by Klotz et al. (2019), which categorizes the causes of shadow IT into enablers, motivators, and missing barriers. Enablers make unauthorized technology adoption technically or practically possible; motivators create reasons for employees to adopt it; and missing barriers reduce the likelihood that the behavior will be prevented or redirected. This framework is particularly suitable for shadow AI because its growth reflects a combination of technological accessibility, work-related benefits, and gaps in organizational governance.

The primary technological enabler is the increasing accessibility of powerful AI capabilities. Generative AI applications can be accessed through ordinary web browsers, mobile applications, personal accounts, browser extensions, and embedded software features. Natural-language interfaces further reduce the expertise needed to use these systems. Employees no longer need to develop a model or request extensive technical support to perform activities such as summarization, translation, coding, content generation, or data interpretation. As Klotz et al. (2019) observe in the broader shadow IT context, declining technological complexity and the expansion of easily accessible digital services enable business users to deploy technological solutions independently. AI intensifies this trend by transforming natural language into an interface for technological development and automation.

The concealability of generative AI constitutes another important enabler. Unlike a conventional unauthorized information system, which may require software installation, dedicated infrastructure, or a visible organizational project, many AI tools can be used through a personal browser session or an existing software platform. Waters-Lynch et al. (2025) argue that generative AI enables covert employee innovation partly because these tools are readily accessible and relatively easy to conceal. Furthermore, AI functions may be embedded within applications already used by the organization, making it difficult for employees and managers to recognize when an ordinary digital tool has begun processing organizational information through an external AI model.

Although accessibility makes shadow AI possible, employees generally require a work-related motivation to use it. Performance expectancy is particularly important. Employees may believe that an AI application will allow them to complete tasks more rapidly, improve the quality of their outputs, overcome skill limitations, or manage an excessive workload. Nguyen (2024) found that performance expectancy and effort expectancy significantly

influenced employees' intentions to use shadow IT. These findings are highly relevant to shadow AI because generative AI combines potentially high performance benefits with relatively low usage effort. The perceived balance between substantial task-related value and minimal adoption cost can make informal AI use especially attractive.

A mismatch between employee needs and formally available technologies may strengthen this motivation. Official systems may lack the required functionality, be difficult to use, or respond too slowly to emerging task requirements. Approval and procurement procedures may also be incompatible with the speed at which employees are expected to deliver results. Haag and Eckhardt (2024) show that shadow IT frequently arises when employees attempt to overcome work-related challenges that authorized technologies do not adequately address. Accordingly, the continued use of shadow AI may signal not only a security problem but also weaknesses in the organization's technological support, user experience, or responsiveness to business needs.

Innovation-related motives also deserve attention. Employees may use AI to test ideas, create prototypes, explore alternative solutions, or develop new methods without waiting for formal authorization. In such cases, shadow AI enables local experimentation and may help employees respond to opportunities that centralized IT structures have not yet recognized. Waters-Lynch et al. (2025) conceptualize this behavior as a form of user innovation capable of contributing to organizational capability renewal. However, the same employees may choose to conceal their experiments because they expect managerial resistance, fear that the activity will be prohibited, or believe that formal disclosure will introduce delays. Innovation-oriented use and policy avoidance can therefore occur simultaneously.

Social influences may further normalize shadow AI. When colleagues regularly use generative AI tools, employees may interpret this behavior as acceptable even when no formal policy permits it. Nguyen (2024) found that subjective norms significantly affected shadow IT usage intention, suggesting that employee behavior is influenced by perceptions of what relevant others expect or consider normal. Informal encouragement from supervisors may have a similar effect. A manager who prioritizes rapid results while remaining silent about how those results are achieved may unintentionally communicate that unauthorized AI use is tolerable. The absence of visible negative outcomes can reinforce this perception and reduce the employee's sense that formal approval is necessary.

Employees may also view their behavior as reasonable because they do not intend to damage the organization. Barlette et al. (2025) describe shadow

IT as the voluntary adoption of unapproved tools for greater efficiency, even though such adoption may violate organizational security policies. Their findings indicate that users can perceive shadow technology as both beneficial and threatening and may attempt to reduce some risks while preserving the efficiency advantages they obtain. This suggests that employees are not always indifferent to information security. Instead, they may rely on their own informal risk assessments, such as removing obvious identifiers from a document or avoiding certain categories of information. The problem is that these individual precautions may not reflect the actual technical, contractual, or regulatory conditions under which the AI provider processes data.

Missing organizational barriers form the third group of drivers. Shadow AI is more likely to emerge when organizations have no clear AI-use policy, when employees do not understand existing rules, or when responsibilities are fragmented among IT, cybersecurity, legal, procurement, and data-governance units. A general instruction to "use AI responsibly" may be insufficient because it does not explain which tools are authorized, what data may be entered, which outputs require verification, or how employees can request approval for a new use case. Weak monitoring and limited inventories of AI applications also allow unauthorized practices to continue without detection.

Paradoxically, highly restrictive policies may not eliminate shadow AI when they are unaccompanied by usable alternatives. Haag and Eckhardt (2024) conclude that shadow IT cannot be addressed through a universal control strategy and recommend balancing cybersecurity requirements with employee needs. When employees perceive that compliance prevents them from completing legitimate tasks, restrictions may encourage concealment rather than secure behavior. Effective governance must therefore reduce the organizational conditions that make shadow AI necessary or attractive. This requires accessible approved tools, proportionate approval procedures, clear data-use boundaries, responsive technical support, and opportunities for employees to disclose useful AI experiments without automatically facing sanctions.

Taken together, these drivers show that shadow AI is produced by the interaction of technological opportunity, individual expectations, social norms, work pressures, and organizational limitations. It should not be reduced to either employee misconduct or technological inevitability. Shadow AI becomes more likely when highly accessible AI tools offer immediate task-related value while formal organizational arrangements remain slow, unclear, or poorly aligned with users' needs. Understanding this combination is essential

because governance strategies that target only employee behavior will leave the underlying technological and organizational causes unchanged.

3. Organizational Information Security Risks

Shadow AI changes the nature of organizational information security risk because it creates data flows, technological dependencies, and AI-supported decisions that remain partly or entirely outside formal oversight. Conventional cybersecurity practices are generally designed around identifiable assets, registered users, approved vendors, and documented information flows. In shadow AI environments, however, the organization may not know which applications are being used, what information is being transferred, what external services are processing that information, or how AI-generated outputs are entering organizational processes. The central problem is therefore not only that an AI system may be technically vulnerable. It is also that the organization cannot effectively assess, monitor, or respond to a system whose use has not been formally identified.

These risks affect the three conventional objectives of information security: confidentiality, integrity, and availability. Shadow AI may compromise confidentiality when employees disclose organizational or personal data to unauthorized services. It may weaken integrity when inaccurate, manipulated, or unverified AI outputs are incorporated into organizational records and decisions. It may also affect availability and operational continuity when business processes become dependent on external AI applications that the organization does not control. In addition, generative AI introduces risks relating to privacy, intellectual property, human oversight, regulatory accountability, and autonomous action that extend beyond traditional cybersecurity boundaries (National Institute of Standards and Technology [NIST], 2024; Puthal et al., 2025).

3.1. Confidentiality, Privacy, and Intellectual Property Exposure

The most immediate risk associated with shadow AI arises when employees submit organizational information to an unauthorized external service. Prompts may contain customer records, employee information, meeting transcripts, financial figures, contractual documents, software code, product designs, internal policies, strategic plans, or research findings. Even when the employee uses the information only to request a summary, translation, analysis, or rewritten text, the interaction constitutes a transfer of information to a third-party technological environment. Because the tool has not been formally assessed, the organization may lack reliable information about where the data are processed, how long they are retained, whether they are used for service

improvement or model training, and which subcontractors or jurisdictions are involved.

This uncertainty distinguishes shadow AI from approved enterprise AI services. Formal procurement and security-assessment processes can evaluate contractual terms, retention periods, access controls, encryption, incident-notification procedures, and restrictions on secondary data use. Shadow AI bypasses these processes. As a result, the organization may be unable to determine whether an external provider's practices are consistent with its data-classification policies, contractual commitments, or legal obligations. The European Data Protection Board's technical report on large language models emphasizes that privacy risks must be assessed by examining data flows across the entire system lifecycle and identifying the parties that process, store, or receive the information (Barberá, 2025). Such an assessment becomes difficult when employees introduce AI services without disclosure.

Personal data deserve particular attention. Under the General Data Protection Regulation, personal data must be processed lawfully, fairly, and transparently and must be collected for specified purposes while remaining adequate, relevant, and limited to what is necessary (European Parliament & Council of the European Union, 2016). When employees enter personal information into an unauthorized AI system, the organization may be unable to establish the lawful basis for this additional processing or determine whether the use is compatible with the original purpose for which the data were collected. It may also be unable to provide accurate information to affected individuals, respond to data-subject requests, establish appropriate processing agreements, or verify international data-transfer conditions.

The problem is not limited to obviously identifiable records. Employees may assume that removing a person's name is sufficient to make a document safe for external AI processing. However, contextual details, job titles, transaction histories, locations, unusual events, and combinations of indirect identifiers may permit reidentification. AI systems can also generate inferences about individuals from seemingly ordinary information. Barberá (2025) therefore treats excessive data collection, insufficient anonymization, unauthorized access, lack of transparency, and the exposure of sensitive attributes as distinct but interconnected privacy risks. Informal employee judgments about whether information is "anonymous enough" may not provide adequate protection.

Confidentiality risks can also emerge after data have entered an AI system. Large language models may reproduce or reveal information contained in their training or adaptation data under particular conditions. Carlini et al. (2021) demonstrated that individual training examples, including personally

identifiable information and source code, could be extracted from a language model through carefully designed queries. This finding does not mean that every prompt submitted to every commercial AI service will later be disclosed. It does demonstrate, however, that model memorization and data extraction constitute technically plausible risks and that organizations should not assume that data become irretrievable merely because they have been processed by a model.

Sensitive information may also be exposed through AI-generated outputs. The OWASP Foundation (2024) identifies sensitive information disclosure as a major vulnerability of applications based on large language models. Such disclosure may involve personal data, financial information, health records, legal documents, security credentials, proprietary algorithms, or confidential business information. In a shadow AI context, the risk is intensified because the organization may not have configured output restrictions, access controls, data filters, or logging mechanisms. An employee-built assistant connected to a shared document repository, for example, may return information to users who would not have been authorized to access the original files.

Intellectual property risks overlap with confidentiality risks but are not identical to them. Employees may upload copyrighted materials, unpublished manuscripts, product specifications, proprietary datasets, software code, formulas, designs, or trade secrets to generate new content or obtain technical assistance. NIST (2024) notes that generative AI may create intellectual property risks through the use of protected material in system inputs, training processes, and generated outputs. An organization may therefore face uncertainty about whether it has the right to submit particular material to the service, whether generated content reproduces protected material, and who owns or may reuse the resulting output.

The exposure of trade secrets is especially significant because the economic value of such information depends on its continued secrecy and controlled use. An employee may believe that submitting a limited excerpt of code or a partial commercial strategy presents little risk. Yet repeated interactions by multiple employees can collectively reveal substantial elements of an organization's knowledge base. The absence of centralized visibility prevents the organization from understanding this cumulative exposure. Shadow AI may consequently produce a gradual form of information leakage in which no single prompt appears catastrophic, but the aggregated flow of prompts, uploaded documents, custom instructions, and model integrations reveals valuable organizational knowledge.

Confidential communications may also be affected. Employees in human resources, legal, finance, healthcare, education, or management positions may use public AI systems to summarize disputes, draft responses, evaluate cases, or prepare recommendations. These interactions may disclose information protected by professional, contractual, or sector-specific confidentiality requirements. Moreover, the organization may be unable to preserve an appropriate audit trail showing what information was disclosed and how it was processed. The informational value of an AI interaction should therefore be assessed not only by examining the individual prompt but also by considering its context, the identity of the affected parties, and the sensitivity of the organizational process in which it occurs.

3.2. Information Integrity, Decision Reliability, and Regulatory Accountability

Shadow AI creates a second category of risk by allowing AI-generated content to enter organizational workflows without systematic verification or provenance records. Generative AI systems produce outputs by estimating statistically plausible continuations rather than by independently confirming the truth of every statement. As a result, they may generate inaccurate facts, fabricated references, incorrect calculations, false explanations, or internally inconsistent recommendations. NIST (2024) uses the term confabulation to describe confidently presented but erroneous or false generative AI content. Farquhar et al. (2024) similarly demonstrate that large language models can generate plausible but arbitrary and incorrect answers, particularly when reliable information is unavailable.

The organizational consequence depends on how the output is used. An inaccurate sentence in an informal brainstorming exercise may have limited impact, whereas an inaccurate output incorporated into a financial report, legal document, customer communication, software application, employee assessment, or strategic recommendation may produce significant harm. Shadow AI makes this distinction difficult to manage because the same public tool can be used for both low-impact and high-impact tasks without a formal change in authorization. Employees may initially adopt the tool for editing text and later begin relying on it for interpretation, analysis, or recommendations.

The fluent and confident presentation of AI-generated content may also encourage automation bias. Users may interpret detailed, well-structured, and professionally worded responses as evidence of accuracy even when the system provides no verifiable basis for its claims. NIST (2024) observes that users may over-rely on generative AI and perceive its outputs as being of

higher quality than they actually are. This tendency is especially important when employees operate under time pressure or lack the domain expertise required to identify subtle errors. Shadow AI may therefore substitute apparent efficiency for careful verification.

Errors may also become difficult to trace after AI-generated material has been edited or integrated into other documents. An employee may copy part of an AI response into a report, revise the wording, and remove any indication that AI was involved. The resulting document appears to be an ordinary organizational output even though some of its claims originated in an external probabilistic system. When an error is later discovered, managers may be unable to reconstruct the prompt, the model version, the data sources, or the reasoning that produced it. This loss of provenance undermines accountability and prevents the organization from learning systematically from AI-related incidents.

The integrity problem is not limited to factual errors. AI-generated outputs can contain biased assumptions, inappropriate generalizations, insecure code, or recommendations that are unsuitable for the organizational context. A model may generate a technically plausible policy that conflicts with internal procedures, summarize a contract while omitting a critical exception, or produce software code containing exploitable weaknesses. Because the tool is unauthorized, these outputs may not be subjected to the testing, validation, and human oversight requirements that would apply to an approved organizational system.

Information integrity may also be deliberately attacked. External content used by an AI application may contain hidden or manipulative instructions designed to alter the system's behavior. An employee may ask an AI assistant to summarize a webpage, document, email, or shared file without realizing that the content includes instructions intended for the model rather than the human reader. Greshake et al. (2023) show that this blurring of the boundary between data and instructions creates indirect prompt-injection vulnerabilities in applications integrated with large language models. A malicious document can therefore influence the AI-generated summary, redirect the system's behavior, or cause it to disclose information from connected sources.

Regulatory accountability becomes more difficult when the organization cannot document how AI is being used. The EU AI Act adopts a risk-based approach and assigns different responsibilities according to the nature of the AI system and the role of the organization using it (European Parliament & Council of the European Union, 2024). Shadow AI can prevent an organization from determining whether a particular use falls within a regulated

category or whether obligations concerning documentation, human oversight, transparency, monitoring, or risk management apply. Even when the AI Act does not classify the use as high-risk, other legal frameworks may continue to govern personal data, employment practices, consumer protection, intellectual property, professional responsibility, and sectoral confidentiality.

The governance gap is particularly important when AI outputs influence decisions about individuals. Employees may informally use AI to screen applications, summarize performance records, evaluate customer complaints, interpret medical or educational information, or recommend personnel actions. The final decision may still be made by a human, but the AI system may shape which information is emphasized and which alternatives are considered. If this use remains undisclosed, the organization may be unable to evaluate fairness, accuracy, explainability, or the adequacy of human oversight. It may also be difficult to respond when an affected individual asks how the decision was reached.

Shadow AI may thus create a form of accountability fragmentation. The employee selects the tool, an external provider operates the model, organizational data supply the context, and a manager may rely on the result. Yet no party within the organization has formally accepted responsibility for evaluating the entire process. When harm occurs, uncertainty may arise concerning whether responsibility belongs to the employee, the manager, the IT department, the data owner, the organization, or the AI provider. This fragmentation is not simply a legal issue; it is an information systems problem because effective accountability requires clearly defined ownership of data, systems, outputs, and decisions.

3.3. Expanded Attack Surface and Operational Exposure

Shadow AI also expands the organizational attack surface by creating connections between external AI systems and internal information resources. A simple chatbot interaction may involve only text entered manually by an employee. More advanced shadow AI practices may connect a model to email, cloud storage, source-code repositories, customer databases, calendars, web browsers, or enterprise applications. Each integration creates additional pathways through which data can be accessed, instructions can be manipulated, and actions can be executed. Because these integrations are not formally registered, security teams may not include them in asset inventories, threat models, penetration tests, access reviews, or incident-response plans.

Prompt injection is one of the most prominent risks in this environment. A direct prompt injection occurs when a user deliberately supplies instructions

intended to override the model's expected behavior. An indirect prompt injection occurs when the malicious instruction is embedded in external content later retrieved by the model (OWASP Foundation, 2024). The latter is particularly relevant to employee-built assistants and no-code automations because the employee may trust the AI system to read websites, emails, or documents from multiple sources. A successful injection can manipulate outputs, disclose sensitive information, access unauthorized functions, influence decisions, or initiate commands in connected systems.

Retrieval-augmented generation does not eliminate this problem. Although connecting an AI system to an internal knowledge base can improve the relevance of its responses, it also creates a pathway through which malicious or improperly classified content can affect the generated output. If access controls are poorly implemented, the assistant may retrieve information beyond the requesting employee's authorization. If documents within the knowledge base contain hidden instructions, the model may interpret them as commands. Greshake et al. (2023) demonstrate that application-integrated language models can be remotely manipulated through content that the model retrieves and processes.

The growing use of autonomous and semi-autonomous AI agents further increases operational risk. An AI agent may be permitted to call external tools, send messages, access records, create files, modify databases, or complete multistep tasks. The OWASP Foundation (2024) describes excessive agency as a vulnerability arising when an AI system has more functionality, permissions, or autonomy than is necessary. When an unauthorized agent operates through an employee account, the organization may not know that decision authority has effectively been delegated to an external model. A hallucinated instruction, manipulated input, or compromised plugin can then produce actions rather than merely inaccurate text.

The consequences of excessive agency extend across confidentiality, integrity, and availability. An agent with broad permissions may read confidential documents, modify records, send unauthorized communications, approve transactions, or delete files. The risk is particularly severe when the agent uses a shared or privileged identity rather than acting within the authorization scope of the individual employee. Human confirmation may also be absent if the employee has configured the workflow to maximize speed. A shadow AI assistant can therefore evolve from a personal productivity tool into an unmonitored actor within the organization's digital environment.

Supply-chain vulnerabilities constitute another source of exposure. AI applications frequently depend on external models, plugins, browser extensions,

open-source libraries, datasets, vector databases, and application programming interfaces. The employee may evaluate the visible functionality of the tool without understanding these underlying dependencies. A compromised extension, insecure software component, manipulated model, or change in the provider's service may affect organizational data and workflows. The organization may have no contractual right to receive notice of such changes because the service was adopted through a personal or free account.

Data and model poisoning can similarly undermine integrity. An attacker may manipulate training, fine-tuning, retrieval, or embedding data to introduce biased behavior, hidden triggers, or misleading outputs. NIST (2024) identifies data poisoning as a threat capable of altering a generative AI system's operation, while the OWASP Foundation (2024) includes data and model poisoning among the principal security risks for large language model applications. Shadow AI increases this risk because employees may construct custom assistants using datasets whose quality, provenance, and security have not been examined.

Improper handling of AI-generated outputs can create downstream vulnerabilities even when the model itself has not been directly compromised. Generated code may be executed without security testing; model-produced queries may be passed to databases; generated HTML may be displayed in an application; and AI-generated instructions may be sent to other automated systems. When outputs are treated as trusted rather than untrusted content, they can enable code execution, unauthorized requests, or data corruption. This risk becomes greater in no-code and low-code environments where employees can connect multiple services without understanding the security implications of each connection.

Availability and business continuity also require consideration. Employees may gradually embed unauthorized AI tools into essential workflows, making task completion dependent on services that the organization does not manage. The provider may change prices, functionality, usage limits, model behavior, or access conditions without organizational planning. Accounts may be suspended, services may become unavailable, or employees who created the workflow may leave the organization without documenting it. The organization may then discover that an important process depends on a personal subscription, undocumented prompt library, or external automation for which no alternative exists.

Shadow AI incidents may also be difficult to detect and investigate. Traditional monitoring systems may record that an employee visited an AI website but may not reveal the meaning or sensitivity of the information

entered into a prompt. Personal accounts and devices further reduce visibility. When an incident occurs, security teams may lack logs showing which data were disclosed, which model processed them, what outputs were generated, and whether those outputs were shared or acted upon. This weakens containment, notification, evidence preservation, and post-incident analysis.

Table 2 Principal Organizational Information Security Risks Associated with Shadow AI

Risk domain	**Shadow AI mechanism**	**Organizational assets affected**	**Potential consequences**
Confidential data disclosure	Employees enter internal documents, records, code, or strategic information into unauthorized AI services	Commercially sensitive information, customer data, source code, internal communications	Data leakage, loss of confidentiality, contractual breaches, reputational damage
Privacy and personal data misuse	Personal data are processed without an established purpose, lawful basis, transparency process, or approved provider relationship	Customer, employee, patient, student, or applicant information	Privacy violations, inability to fulfil data-subject rights, regulatory exposure
Intellectual property exposure	Protected content, trade secrets, designs, datasets, or unpublished materials are submitted to external systems or reproduced in outputs	Copyrighted works, patents, trade secrets, proprietary knowledge	Loss of control over intellectual assets, infringement claims, weakening of competitive advantage
Information integrity failure	Confabulated, biased, incomplete, or contextually inappropriate outputs enter reports and decisions	Organizational records, analyses, policies, software, managerial decisions	Incorrect decisions, operational errors, unreliable records, stakeholder harm
Loss of provenance and accountability	AI involvement, prompts, data sources, model versions, and human review are undocumented	Audit trails, decision records, governance responsibilities	Inability to explain or reproduce decisions, fragmented responsibility, weak incident learning
Prompt injection and manipulation	Malicious instructions are entered directly or embedded in websites, emails, and documents retrieved by the AI system	Connected data sources, model behavior, downstream applications	Unauthorized disclosure, manipulated output, control bypass, command execution

Excessive agency	Unauthorized agents receive broad permissions to access systems or execute actions	Email, databases, cloud storage, business applications, user accounts	Unauthorized transactions, data modification or deletion, operational disruption
AI supply-chain exposure	Employees rely on unassessed models, plugins, extensions, APIs, libraries, or datasets	AI workflows, credentials, internal systems, processed data	Compromise through third parties, malicious updates, hidden dependencies
Data and model poisoning	Manipulated training, retrieval, fine-tuning, or embedding data alter model behavior	Knowledge bases, custom assistants, analytical outputs	Persistent misinformation, biased results, hidden backdoors, loss of model reliability
Availability and continuity risk	Critical work becomes dependent on personal accounts or uncontrolled external services	Business processes, employee knowledge, organizational productivity	Service interruption, vendor lock-in, undocumented dependencies, loss of operational capability
Incident-response blind spots	AI use and prompt content are not visible in formal logs or asset inventories	Security monitoring, evidence, incident records	Delayed detection, incomplete containment, inaccurate breach assessment

Note. Developed by the author based on Barberá (2025), Greshake et al. (2023), NIST (2024), OWASP Foundation (2024), and Puthal et al. (2025).

The risks summarized in Table 2 are interdependent rather than isolated. A single shadow AI practice can simultaneously expose confidential data, violate privacy requirements, introduce inaccurate information, and create a new attack pathway. For example, an employee-built agent connected to a customer database may disclose personal information through an external model, generate an incorrect response, and perform an unauthorized action after receiving a manipulated instruction. The severity of shadow AI therefore depends not only on the selected tool but also on the sensitivity of the data, the employee's permissions, the degree of system integration, the autonomy granted to the AI, and the importance of the organizational process in which it is used.

4. Shadow AI Governance and Mitigation Strategies

Effective shadow AI governance requires a structured approach that connects organizational policies, employee needs, cybersecurity controls, legal requirements, and ongoing oversight. A complete prohibition on workplace

AI use may appear to provide a simple solution, yet it does not address the productivity, accessibility, and task-related motivations that encourage employees to adopt unauthorized tools. Weak or ambiguous governance creates a different problem by leaving employees to make individual decisions about data sensitivity, acceptable use, and output reliability. Organizations need governance arrangements that make AI use visible, distinguish different levels of risk, provide secure alternatives, and assign responsibility for decisions throughout the AI lifecycle.

Organizational AI governance refers to the rules, practices, processes, and capabilities through which an organization directs and controls its use of AI in accordance with its strategies, values, ethical principles, and legal obligations (Mäntymäki et al., 2022). This definition is relevant to shadow AI because unauthorized use frequently develops in the spaces between formal rules, technological access, and actual working practices. Governance must therefore cover AI systems formally acquired by the organization, employee-selected applications, embedded AI features, custom assistants, external models, and autonomous agents. The scope must also include approved tools that employees use for unapproved data, purposes, or decisions.

4.1. Governance Architecture and Risk-Based Oversight

A clear governance architecture provides the organizational foundation for managing shadow AI. Senior management should establish the organization's objectives, risk tolerance, and general principles for AI use. Operational responsibilities can then be distributed among information technology, cybersecurity, data governance, legal affairs, compliance, procurement, human resources, internal audit, and relevant business units. This distribution requires explicit decision rights because fragmented responsibility can allow risky AI practices to remain unaddressed. Mäntymäki et al. (2022) describe organizational AI governance as a system that aligns AI-related decisions with organizational strategy, values, and legal requirements. Shadow AI governance applies this logic to technologies and use cases that may initially remain outside formal decision structures.

A cross-functional AI governance committee can coordinate these responsibilities and prevent governance from becoming the exclusive concern of the IT department. The committee may define acceptable-use rules, evaluate proposed tools, approve higher-risk use cases, review incidents, and monitor changes in legal and technological conditions. Business-unit participation is essential because operational managers understand why employees adopt particular tools and which formal systems fail to meet their needs. Cybersecurity

and legal specialists can evaluate risks that employees or line managers may overlook. Internal audit can assess whether declared policies are reflected in actual practice.

A formal AI policy should define the organizational boundaries of acceptable use. The policy needs to specify which AI services are approved, which data categories may be processed, which activities require prior authorization, and which uses are prohibited. Rules should distinguish public consumer applications from enterprise services that provide contractual protections, administrative controls, and organizational logging. The policy should also cover personal accounts, browser extensions, application programming interfaces, custom assistants, retrieval systems, AI-generated code, and autonomous agents. A policy limited to well-known chatbot websites may become ineffective as AI capabilities are increasingly embedded in ordinary workplace software.

Purpose and context should guide authorization decisions. The same AI service may create a limited risk when used to generate generic brainstorming ideas and a substantial risk when used to process customer records or recommend personnel decisions. The European Union's AI Act similarly adopts a risk-based regulatory approach in which obligations depend on the characteristics, context, and potential effects of an AI system (European Parliament & Council of the European Union, 2024). An organizational framework can adapt this principle by classifying use cases according to data sensitivity, decision impact, system integration, user permissions, affected stakeholders, and degree of autonomy.

A practical classification may separate AI use into low-risk, controlled, high-risk, and prohibited categories. Low-risk uses may include generating generic ideas or editing nonsensitive text. Controlled uses may include working with internal information inside an approved enterprise environment under specified conditions. High-risk uses may involve personal data, confidential information, automated recommendations, external communication, software deployment, or decisions affecting individuals. Prohibited uses may include entering restricted data into public systems, allowing unsupervised AI agents to execute sensitive actions, or using AI for decisions that violate legal or organizational requirements. The purpose of such classification is to match the intensity of governance with the potential severity of harm.

An organizational AI inventory is necessary for applying this classification consistently. The inventory should record approved applications, providers, models, business owners, intended purposes, data categories, integrations, user groups, contractual conditions, and review dates. The NIST AI Risk

Management Framework places governance and contextual mapping at the center of risk management because organizations need to understand where AI is used, who is affected, and which risks arise from each context (National Institute of Standards and Technology [NIST], 2023). An inventory designed for shadow AI should also accept reports of previously unknown tools and uses. Its function is to improve visibility rather than to document only systems that have already completed formal procurement.

A simple and responsive approval process can increase the accuracy of the inventory. Employees are less likely to disclose an AI tool when approval requires lengthy paperwork, unclear communication, or several weeks of waiting. A tiered process can allow rapid approval for low-risk uses while directing sensitive or integrated applications to a more detailed assessment. The assessment should examine the provider, terms of service, privacy conditions, information retention, model-training practices, security controls, technical dependencies, accessibility of logs, and procedures for deleting organizational data. ISO/IEC 42001:2023 supports a management-system approach in which organizations establish, implement, maintain, and continually improve policies and processes for the responsible development, provision, and use of AI systems (International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2023).

AI impact assessments provide a useful mechanism for high-risk use cases. An assessment can document the intended objective, expected benefits, relevant stakeholders, potential harms, data sources, human oversight, limitations, and proposed controls. The assessment should also evaluate whether the use is necessary and whether a less risky method can achieve the same objective. High-impact applications require clear criteria for testing, approval, monitoring, suspension, and retirement. Shadow AI practices that have already become embedded in a business process may require a retrospective assessment before they can be converted into formally governed systems.

Legal and regulatory mapping forms part of the assessment. The organization must determine whether the use involves personal data, protected intellectual property, employment decisions, consumer interactions, financial records, health information, or sector-specific obligations. The AI Act creates responsibilities for providers and deployers according to the role they perform and the risk characteristics of the AI system (European Parliament & Council of the European Union, 2024). Existing data-protection, cybersecurity, contractual, and professional obligations continue to apply when AI is introduced into a process. Organizational approval does not remove these obligations; it provides a mechanism through which they can be identified and addressed.

Risk ownership must remain identifiable after a tool has been approved. Each AI use case should have a business owner responsible for its purpose and outcomes, a technical owner responsible for configuration and integration, and a data owner responsible for the information processed. Higher-risk systems may require independent review from cybersecurity, privacy, legal, or internal-audit functions. Approval decisions should record any accepted residual risks, usage restrictions, review dates, and conditions that would trigger reassessment. Model updates, new integrations, broader user access, and increased autonomy can materially change the original risk profile.

4.2. Technical and Operational Controls

Technical controls translate governance decisions into enforceable conditions. Their purpose is to reduce unauthorized data movement, limit excessive permissions, detect unapproved services, preserve records, and prevent AI-generated outputs from producing uncontrolled actions. The NIST Cybersecurity Framework 2.0 organizes cybersecurity outcomes around the functions of Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024b). These functions can be adapted to shadow AI by connecting AI governance with existing cybersecurity and incident-management processes.

Approved enterprise AI services provide the first layer of protection. Organizations should offer tools that satisfy common employee needs while providing stronger contractual, administrative, and technical safeguards than personal consumer accounts. Relevant capabilities may include single sign-on, centralized account management, configurable retention, restrictions on model training, organizational logging, access control, and support for data-residency requirements. An approved tool will reduce shadow AI only when it is accessible, functional, and sufficiently responsive to employees' tasks. Haag and Eckhardt (2024) emphasize that effective responses to shadow IT must address cybersecurity requirements and user needs within the same management approach.

Identity and access management should apply the principle of least privilege to AI systems and their integrations. Employees should access only the models, data sources, plugins, and external functions required for their roles. Custom assistants connected to organizational repositories should preserve the access permissions of the underlying documents. Shared accounts should be avoided because they obscure responsibility and make it difficult to revoke access selectively. Privileged AI functions, such as connecting external tools or creating autonomous agents, may require additional approval and stronger authentication.

Data-classification rules should be translated into clear AI-processing rules. Employees need practical guidance showing which data may be entered into public, enterprise, or internally hosted AI systems. Labels such as public, internal, confidential, personal, restricted, and trade secret can be linked to specific processing conditions. Data-loss prevention systems, secure web gateways, endpoint controls, and cloud-access monitoring can help identify or restrict the transfer of sensitive information to unauthorized services. Technical restrictions should be proportionate because overly broad blocking may disrupt legitimate work and encourage employees to seek less visible alternatives.

Prompt and input controls can reduce accidental disclosure within approved systems. Automated checks may detect personal data, credentials, confidential terms, source code, or restricted document labels before information is submitted to a model. Redaction and pseudonymization can reduce exposure when the full identity of a person or organization is unnecessary for the task. These measures do not eliminate the need for employee judgment because automated detection may miss contextual sensitivity. Data minimization should remain the default principle: the model should receive only the information needed to complete the approved task.

Vendor assessment should examine the full AI supply chain rather than focusing exclusively on the visible application. AI services may depend on external model providers, hosting environments, plugins, datasets, libraries, and subcontractors. The assessment should review data retention, secondary use, breach notification, deletion, encryption, access management, change notification, audit rights, service continuity, and dependency management. ISO/IEC 42001:2023 requires organizations to manage AI-related risks and opportunities through a systematic and continually improving management structure (ISO & IEC, 2023). Vendor oversight fits within this structure because external providers can alter the organization's risk exposure throughout the service relationship.

Logging and monitoring should provide evidence about how approved AI systems are used. Relevant records may include user identities, timestamps, selected models, connected data sources, administrative changes, tool calls, generated outputs, and human approvals. The sensitivity of prompts and outputs requires careful decisions about log access and retention. Excessive logging can create a new repository of confidential information, while insufficient logging can prevent incident investigation and accountability. Monitoring should therefore collect information that supports security and audit requirements under clearly defined access controls.

Discovery mechanisms can identify potential shadow AI use without assuming that every detected interaction represents misconduct. Network records, endpoint inventories, browser-extension lists, software-as-a-service discovery tools, procurement data, and expense records may reveal unapproved services. Surveying employees and inviting voluntary disclosure can identify practices that technical monitoring cannot observe. Discovery findings should be evaluated in context because visiting an AI website differs from uploading restricted information or connecting an external agent to an internal database.

Output governance is required because secure input handling does not guarantee reliable results. High-impact outputs should undergo qualified human review before they are used in decisions, external communications, software deployment, or official records. Reviewers need access to relevant source materials and should be able to reject the output without pressure to defer to the model. NIST's Generative Artificial Intelligence Profile identifies confabulation, harmful bias, data privacy, information security, intellectual property, and human overreliance as interconnected areas of generative AI risk (NIST, 2024a). Review procedures should be designed according to the type of harm that could arise from an error.

Provenance records can support review and accountability. Documents, analyses, code, or recommendations produced with substantial AI assistance may need records showing the tool used, date, relevant data sources, reviewer, and level of human modification. The required detail should correspond to the significance of the output. Informal brainstorming does not require the same documentation as a regulatory filing, employment recommendation, or deployed software component. Provenance requirements should preserve traceability without creating administrative burdens that drive AI use back into secrecy.

Agentic AI requires stricter operational boundaries because the system may perform actions across connected environments. Agent permissions should be limited to predefined tools, data sources, and actions. Sensitive operations can require explicit human confirmation, while financial transactions, record deletion, external publication, and privilege changes may remain outside the agent's authority. Sandboxed execution, tool allowlists, rate limits, transaction limits, session timeouts, and emergency termination mechanisms can reduce the consequences of model error or manipulation. OWASP Foundation (2024) identifies excessive agency as a major risk when an AI-enabled application receives functionality, permissions, or autonomy beyond what its task requires.

Security testing should address AI-specific vulnerabilities before deployment. Testing may examine prompt injection, sensitive information disclosure,

insecure output handling, supply-chain weaknesses, model or data poisoning, and excessive agency (OWASP Foundation, 2024). Custom assistants should be tested with adversarial documents and manipulated inputs when they retrieve information from external sources. Generated code should pass ordinary secure-development reviews and automated testing before implementation. AI security must remain connected to established application security because model-related safeguards cannot compensate for weak authentication, insecure interfaces, or excessive user privileges.

Incident-response plans should explicitly include unauthorized AI use. Employees need a clear process for reporting accidental data disclosure, suspicious model behavior, manipulated outputs, compromised plugins, or agent actions. Response procedures should identify who can suspend access, preserve evidence, contact providers, assess affected data, notify stakeholders, and determine legal reporting obligations. NIST's Generative Artificial Intelligence Profile recommends integrating generative AI use cases into incident-response and recovery planning (NIST, 2024a). Existing response teams may require additional expertise to interpret prompts, model configurations, retrieval sources, and AI-generated actions.

Table 3 presents an integrated governance cycle that connects organizational decisions with operational evidence. The cycle begins with discovering actual AI use and continues through classification, authorization, control, monitoring, and organizational learning.

Table 3 *Integrated Governance Cycle for Managing Shadow AI*

Governance function	**Core practices**	**Expected evidence**	**Principal risks addressed**
Discover	Identify AI tools, embedded features, personal accounts, browser extensions, integrations, custom assistants, and agents used for organizational work	AI inventory, employee disclosures, software discovery records, network and procurement findings	Invisible data flows, undocumented dependencies, unknown vendors
Classify	Evaluate data sensitivity, decision impact, affected stakeholders, integration level, user permissions, and system autonomy	Risk classification, data-flow map, preliminary impact assessment	Inconsistent controls, underestimation of high-impact uses, regulatory uncertainty

Authorize	Approve, restrict, reject, or redesign the use case; assign business, technical, and data ownership	Approval record, usage conditions, named owners, review date, accepted residual risks	Fragmented accountability, unauthorized processing, unclear decision rights
Enable and protect	Provide approved tools, restrict permissions, apply data controls, test integrations, and establish human-review requirements	Access configuration, vendor assessment, data-processing rules, test results, review procedures	Data leakage, excessive agency, insecure integrations, unreliable outputs
Monitor and assure	Review logs, usage patterns, model changes, incidents, output quality, compliance, and control effectiveness	Monitoring reports, audit records, performance indicators, reassessment decisions	Undetected misuse, model drift, policy avoidance, declining control effectiveness
Respond and learn	Contain incidents, support affected users, revise controls, improve approved tools, and incorporate useful employee innovations	Incident records, corrective actions, updated policies, formalized use cases, lessons-learned reports	Repeated incidents, persistent shadow use, loss of employee-generated innovation

Note. Developed by the author through a synthesis of Haag and Eckhardt (2024), NIST (2023, 2024a, 2024b), ISO and IEC (2023), OWASP Foundation (2024), and Waters-Lynch et al. (2025).

4.3. Employee Enablement and Adaptive Governance

Employee behavior determines whether formal controls will produce secure AI use or drive it further from organizational visibility. Shadow AI often reflects a difference between the technologies employees need and the services the organization provides. Governance should therefore treat employees as participants in risk management and sources of information about emerging use cases. A punitive approach may increase concealment when employees believe that disclosure will result in automatic prohibition or disciplinary action.

Approved alternatives should address the tasks that motivate unauthorized adoption. Employees who need summarization, translation, coding support, document analysis, or brainstorming should have access to suitable enterprise tools and clear guidance on their permitted use. Slow or functionally limited

alternatives may satisfy formal compliance requirements while failing to change actual behavior. Haag and Eckhardt (2024) argue that the management of shadow technology should combine cybersecurity protection with attention to user needs. This balance is central to shadow AI because public generative AI tools often provide immediate functionality with little effort.

AI literacy programs should explain the practical consequences of using different tools and data types. General warnings that AI may be risky are unlikely to guide employees during specific tasks. Training should use realistic scenarios involving customer information, source code, internal reports, meeting transcripts, personnel records, and AI-generated recommendations. Employees need to understand data retention, model limitations, hallucination, prompt injection, intellectual property, personal accounts, and human-review responsibilities. The EU AI Act recognizes AI literacy as part of responsible organizational AI use, placing attention on the knowledge and competence of people who operate AI systems (European Parliament & Council of the European Union, 2024).

Role-specific training is more useful than a uniform course for the entire organization. Software developers need guidance on generated code, external repositories, licensing, and secure testing. Human resources personnel need guidance on personal data, fairness, and decisions affecting employees or applicants. Legal and research staff need guidance on confidentiality, citations, intellectual property, and fabricated sources. Managers need guidance on accountability, appropriate delegation, and the risks of pressuring employees to use AI without formal support.

An accessible disclosure mechanism can surface useful AI practices before they become deeply embedded dependencies. Employees should be able to report a tool, propose a use case, or describe an existing workflow without navigating a complex procurement process. A limited safe-harbor approach may encourage voluntary disclosure when the employee acted to improve a legitimate task and reports the practice before an incident occurs. Deliberate misuse, concealment of known harm, and repeated violation of explicit restrictions can remain subject to ordinary disciplinary procedures. The distinction between good-faith experimentation and reckless behavior strengthens the credibility of governance.

Employee experimentation can be moved into controlled environments. Sandboxes may permit teams to test models with synthetic, anonymized, or low-sensitivity data while the organization evaluates value and risk. Successful experiments can then proceed through formal assessment, integration, and ownership. Waters-Lynch et al. (2025) describe covert generative AI use as

a form of shadow user innovation that may create organizational value while avoiding formal oversight. Governance can capture this value by creating a path through which employee-developed practices become visible, evaluated, and scalable.

Leadership behavior shapes the practical meaning of AI policy. Managers who demand faster AI-enabled results while ignoring approval requirements create conflicting expectations. Senior executives who use personal AI accounts or bypass controls weaken the legitimacy of restrictions applied to other employees. Governance therefore requires consistent conduct across hierarchical levels. Managers should discuss acceptable AI use during project planning and workload allocation rather than treating compliance as a separate technical concern.

Performance measures should evaluate governance quality rather than focusing only on the number of blocked tools or policy violations. Useful measures may include the proportion of AI use cases registered, average approval time, employee access to approved alternatives, frequency of voluntary disclosures, number of high-risk uses remediated, completion of role-specific training, AI-related incidents, and recurrence of previously identified problems. A declining number of detected tools may indicate improved compliance, reduced detection capacity, or deeper concealment. Measures should therefore be interpreted alongside employee feedback and technical evidence.

Continuous review is necessary because AI services, organizational uses, legal obligations, and threat techniques change rapidly. An approved tool may introduce new features, connect to additional data sources, change its retention terms, or add autonomous functions. A low-risk use case may become high-risk when it expands to new users or begins influencing consequential decisions. ISO/IEC 42001:2023 places continual improvement within the structure of an AI management system (ISO & IEC, 2023). Shadow AI governance should adopt the same orientation through scheduled reassessment, incident learning, and policy revision.

Adaptive governance creates a controlled path from discovery to legitimate organizational use. Low-value and high-risk shadow practices can be discontinued. Useful practices can be redesigned, secured, and formally supported. Uncertain practices can remain within limited experimentation environments until adequate evidence is available. This approach treats shadow AI as a source of security exposure and organizational learning. Its effectiveness depends on maintaining visibility, proportionality, accountability, and a credible response to employee needs.

5. Future Research Directions

Shadow AI has recently emerged as a distinct research subject at the intersection of management information systems, cybersecurity, organizational behavior, knowledge management, and AI governance. Existing studies have clarified its basic characteristics, identified several cybersecurity risks, and emphasized the tension between employee-driven innovation and organizational control (Puthal et al., 2025; Waters-Lynch et al., 2025). Research has also begun to examine governance responses and the relationship between shadow AI use and organizational knowledge leakage (Chin et al., 2025; Dolci & Aguiar, 2025). The available evidence remains limited in comparison with the speed and diversity of organizational AI adoption. Many current arguments are based on conceptual analysis, practitioner observations, or insights transferred from the established shadow IT literature. A stronger evidence base requires clear conceptual boundaries, validated measurement instruments, longitudinal research designs, multilevel analysis, and direct evaluations of governance interventions.

Future research should preserve the dual character of shadow AI. A narrow focus on security violations may overlook productivity gains, employee learning, local experimentation, and the discovery of unmet technological needs. A purely innovation-oriented perspective may underestimate data leakage, unreliable outputs, accountability gaps, and the expansion of organizational attack surfaces. Chin et al. (2025) found an inverted U-shaped relationship between shadow AI use and organizational knowledge leakage within metaverse-related businesses, indicating that its consequences may change according to the intensity and context of use. Waters-Lynch et al. (2025) similarly frame covert generative AI use as a form of employee-driven innovation whose organizational value depends on whether firms can identify and integrate useful practices. These findings support a research agenda that investigates conditions, thresholds, and trade-offs rather than assuming uniformly beneficial or harmful outcomes.

5.1. Conceptualization, Measurement, and Multilevel Explanation

Conceptual clarity represents the first research priority. Studies need to distinguish shadow AI from approved enterprise AI, employee-initiated AI, business-managed AI, accidental policy violations, malicious AI misuse, and the unauthorized use of approved systems. A technology may be selected by an employee and remain aligned with organizational governance after disclosure and approval. An approved application may enter the shadow domain when employees use restricted data, activate unapproved integrations, or apply its

outputs to unauthorized decisions. Future definitions should therefore address the status of the tool, the visibility of the practice, the data involved, the purpose of use, the degree of system integration, and the level of autonomy granted to the AI.

The unit of analysis also requires clarification. Shadow AI can refer to an individual act, a recurring employee behavior, a team-level routine, an unofficial technological system, or an organizational condition characterized by limited AI visibility. These levels should not be combined without explanation. An employee who occasionally uses a public chatbot for nonsensitive editing presents a different theoretical and practical case from a department that connects an external model to customer records through an undocumented application programming interface. Research designs should identify whether they examine shadow AI adoption, usage frequency, concealment, risk intensity, organizational prevalence, or dependence on unauthorized AI-supported processes.

Validated measurement instruments are needed to support cumulative empirical research. A binary measure asking whether an employee has used an unapproved AI tool cannot represent the range of relevant behaviors. A multidimensional scale could assess undisclosed tool adoption, unauthorized data processing, policy-inconsistent use of approved systems, hidden AI integration, reliance on unverified outputs, and delegation of actions to unauthorized agents. Frequency, duration, organizational importance, data sensitivity, and system autonomy could be measured separately because they influence the severity of a practice. Scale development should begin with qualitative interviews, critical-incident reports, expert review, and employee diaries before proceeding to exploratory and confirmatory validation across independent samples.

Measurement research must address social desirability and concealment. Employees may underreport shadow AI use when they fear sanctions, reputational damage, or managerial disapproval. Managers may also underestimate its prevalence because they interpret the absence of reported incidents as evidence of compliance. Anonymous surveys can reduce this problem but may remain vulnerable to self-presentation and recall errors. Randomized-response techniques, list experiments, indirect questioning, and scenario-based measures may produce more accurate estimates of sensitive behavior. Digital trace data from network records, browser extensions, software inventories, and AI service logs could be combined with employee surveys when legal, ethical, and privacy conditions permit.

Behavioral studies should examine why employees choose shadow AI when approved alternatives exist. Performance expectancy, effort expectancy, task–technology misfit, workload, time pressure, AI self-efficacy, perceived policy legitimacy, and dissatisfaction with official systems may shape this decision. Social influences may arise when colleagues and supervisors normalize AI use without discussing authorization or data protection. Employees may also rely on neutralization strategies that allow them to interpret policy violations as harmless, necessary, or beneficial to the organization. Statements such as "everyone uses it," "the data were not truly confidential," or "the organization did not provide a suitable tool" may reduce perceived personal responsibility.

Several theoretical perspectives can explain different parts of this behavior. Task–technology fit can explain how deficiencies in approved systems encourage employees to seek external tools. Technology acceptance perspectives can clarify the influence of perceived usefulness and ease of use. Deterrence theory can examine the effects of sanction certainty and severity, while protection motivation theory can address threat perceptions and coping responses. Neutralization theory can explain how employees justify policy-inconsistent behavior. Affordance theory can show how accessibility, concealability, generativity, and automation create opportunities for unauthorized use. A sociotechnical systems perspective can connect individual behavior with work design, organizational structures, security controls, and technological capabilities.

The coexistence of these perspectives does not require placing many theories within a single model. Research should select the theoretical lens that matches the focal question and level of analysis. A study examining initial adoption may focus on task–technology fit and performance expectancy. A study examining concealment may use neutralization, perceived policy legitimacy, or psychological safety. A governance study may examine deterrence, organizational justice, and trust. A multilevel study may connect leadership signals and security climate with individual decisions. Theoretical precision will provide greater explanatory value than models containing numerous weakly connected constructs.

Outcome research should extend beyond data leakage. Potential employee-level outcomes include productivity, learning, creativity, job autonomy, stress, role ambiguity, and perceived surveillance. Team-level outcomes may include knowledge sharing, workflow adaptation, coordination, and the development of undocumented dependencies. Organizational outcomes may include information security incidents, innovation speed, decision quality, compliance costs, intellectual property exposure, resilience, and AI capability

development. Chin et al. (2025) demonstrate that shadow AI may have nonlinear relationships with knowledge-related outcomes. Future studies should test curvilinear, threshold, and configurational effects across a broader range of organizational settings.

Temporal dynamics deserve greater attention. Shadow AI practices may begin as occasional experiments and gradually become established routines. The perceived usefulness of a tool may increase employee reliance, while repeated use may lead to the transfer of more sensitive information or broader integration with internal systems. Organizational responses may also change behavior over time. An initial prohibition may reduce visible use but increase concealment, whereas access to a suitable enterprise alternative may gradually redirect employees toward approved services. Longitudinal surveys, diary studies, repeated digital-trace observations, and process studies can capture these transitions more effectively than cross-sectional designs.

Multilevel research can explain how organizational conditions shape individual behavior. Policy clarity, ethical climate, information security culture, AI literacy programs, leadership conduct, availability of approved tools, and the responsiveness of IT departments may influence employees' risk assessments. Team-level norms may create variation within the same organization because some managers actively discuss acceptable AI use while others focus exclusively on performance outcomes. Cross-level models could examine whether organizational governance reduces shadow AI directly or changes the effects of task pressure, AI self-efficacy, and perceived usefulness on employee behavior.

Sectoral and institutional contexts should be incorporated into theory testing. Healthcare, finance, education, public administration, software development, consulting, and research organizations differ in data sensitivity, professional responsibility, regulatory exposure, and acceptable tolerance for experimentation. A shadow AI practice that creates limited consequences in generic content preparation may be unacceptable in clinical, legal, financial, or employment decisions. Comparative studies can identify whether the same drivers and governance responses operate consistently across sectors.

Cross-national research can examine how legal systems, cultural values, labor relations, and institutional trust affect shadow AI. Employees' willingness to disclose unauthorized use may vary according to power distance, perceptions of managerial fairness, job security, and confidence in organizational reporting procedures. Data-protection regimes and AI regulations may also affect policy design and managerial attention. Studies based on a single country should

avoid treating their findings as universal, particularly when organizational AI use is shaped by different regulatory and cultural environments.

5.2. Governance Effectiveness, Technical Detection, and Agentic AI

Governance research should move from descriptive recommendations toward comparative evaluation. Existing work proposes policies, inventories, employee training, approved alternatives, technical monitoring, and controlled experimentation environments as potential responses to shadow AI (Dolci & Aguiar, 2025; Puthal et al., 2025). The effectiveness of these measures remains an empirical question. Organizations may adopt similar policies while producing different outcomes because of implementation quality, employee trust, managerial consistency, and the usefulness of approved systems.

Future studies should compare restrictive, enabling, and adaptive governance models. A restrictive model emphasizes blocking, sanctions, and centralized approval. An enabling model focuses on approved tools, guidance, and rapid access to AI capabilities. An adaptive model combines risk-based controls with sandboxes, voluntary disclosure, continuous review, and pathways for formalizing useful employee innovations. Comparative case studies can reveal how these models operate in practice, while longitudinal designs can assess their effects on security incidents, employee behavior, innovation, and organizational trust.

Field experiments and natural experiments would strengthen causal evidence. Organizations may introduce training, approved AI platforms, revised policies, safe-harbor reporting procedures, or new monitoring technologies in phases. Researchers could compare business units before and after implementation or examine matched units receiving different interventions. Relevant outcomes may include the use of personal AI accounts, attempts to transfer sensitive data, voluntary disclosure rates, time required to obtain approval, employee satisfaction with authorized tools, and the number of useful shadow practices converted into governed applications.

Governance effectiveness should not be measured solely through reductions in detected unauthorized use. A decrease may indicate stronger compliance, reduced AI use, displacement to personal devices, or more successful concealment. Evaluation should combine security indicators with employee perceptions, technical records, incident data, and operational outcomes. Suitable indicators may include policy comprehension, perceived legitimacy, trust in the reporting process, use of approved alternatives, approval speed,

recurrence of violations, decision quality, productivity, and the rate at which employee innovations become formally supported.

The relationship between monitoring and employee privacy requires systematic investigation. Technical discovery mechanisms can identify visits to AI services, browser extensions, unapproved integrations, and potential transfers of sensitive data. Extensive monitoring may create concerns about workplace surveillance, autonomy, and the collection of employee prompts. Employees who perceive monitoring as disproportionate may avoid organizational systems or reduce voluntary disclosure. Research should examine which forms of monitoring employees consider legitimate, how transparency affects acceptance, and whether privacy-preserving discovery methods can provide sufficient security visibility.

Technical studies should evaluate the accuracy and limitations of shadow AI detection. Web traffic classification may identify known services while missing embedded AI features, locally hosted models, encrypted connections, personal devices, or newly created applications. Data-loss prevention systems may detect recognizable personal data or confidential labels but fail to understand contextual sensitivity. False positives can interrupt legitimate work and weaken trust in security systems. False negatives may create misplaced confidence. Benchmark datasets and standardized evaluation criteria are needed to compare detection approaches under realistic organizational conditions.

Privacy-preserving monitoring presents a promising research area. Organizations need information about risky AI use without creating repositories containing every employee prompt and output. Future systems could apply local classification, data minimization, pseudonymization, aggregate reporting, differential privacy, or risk-based escalation. Low-risk events might be recorded only as aggregated usage patterns, while high-risk transfers could trigger more detailed review under defined procedural safeguards. Studies should evaluate the security value, employee acceptability, and legal implications of these architectures.

Research should also investigate the conversion of shadow AI into governed organizational capability. Some employee-created workflows may offer substantial value once their data sources, permissions, ownership, and review requirements have been formalized. Waters-Lynch et al. (2025) argue that covert generative AI use may contribute to capability renewal when organizations can identify and integrate valuable employee innovations. Process research could examine how organizations discover these practices, decide which ones to support, transfer individual knowledge to formal teams, and prevent dependence on undocumented personal systems.

Agentic AI creates an urgent extension of the shadow AI research agenda. Employees can increasingly configure systems that retrieve information, call external tools, communicate with other services, and execute multistep tasks. Unauthorized agent use changes the risk profile because an error or manipulated instruction can produce an organizational action. Research should distinguish shadow AI tools that generate advice from shadow agents that exercise delegated authority.

Agentic AI studies should examine permission design, action limits, human confirmation, identity management, tool access, memory, and inter-agent communication. Low-code agent development may allow employees to create complex automations without fully understanding the permissions or dependencies involved. Emerging research on agentic explainability reports limited organizational visibility into agent configurations and interactions across agent networks (Elsayed & Jones, 2026). Shadow agent research should therefore consider observability at design time and runtime, including who created the agent, which resources it can access, what decisions it makes, and how its actions can be reconstructed.

Human oversight requires more precise operationalization in agentic environments. Requiring a person to click "approve" may provide weak protection when the user lacks time, expertise, or sufficient information to evaluate the proposed action. Future experiments should compare forms of oversight, including confirmation before every action, approval for specific risk categories, transaction limits, exception-based review, dual authorization, and retrospective auditing. Research should measure how these designs affect error detection, employee workload, automation benefits, and responsibility attribution.

Liability and accountability research will become increasingly important as shadow agents affect customers, employees, and external stakeholders. An employee may configure the agent, a third-party provider may operate the model, an organizational account may supply access, and a manager may benefit from its output. The distribution of control across these actors complicates responsibility. Legal, information systems, and organizational behavior researchers should jointly examine how organizations assign ownership and how employees understand their responsibility when AI systems perform actions on their behalf. Table 4 summarizes a research agenda that connects these gaps with suitable questions, levels of analysis, and methodological approaches.

Table 4 Research Agenda for Shadow AI

Research domain	**Illustrative research questions**	**Primary level of analysis**	**Suitable methods**
Conceptual boundaries	When does employee-initiated AI become shadow AI? How should unauthorized tools be distinguished from unauthorized uses of approved systems?	Practice, system, organization	Concept analysis, expert panels, Delphi studies, comparative case studies
Measurement	Which dimensions capture the frequency, concealment, sensitivity, integration, and autonomy of shadow AI use?	Individual and team	Interviews, scale development, validation studies, randomized-response techniques
Behavioral drivers	How do task–technology misfit, work pressure, AI self-efficacy, social norms, and policy legitimacy influence shadow AI?	Individual	Surveys, experiments, diary studies, multilevel modeling
Innovation and performance	Under which conditions does shadow AI improve productivity, learning, creativity, or capability development?	Individual, team, organization	Longitudinal surveys, field studies, process research, configurational analysis
Security and knowledge outcomes	How do usage intensity, data sensitivity, integration, and autonomy shape data leakage and decision risk?	Use case and organization	Incident analysis, digital traces, nonlinear modeling, simulations
Governance effectiveness	Which combinations of policies, approved alternatives, training, disclosure mechanisms, and sanctions produce sustainable compliance?	Team and organization	Field experiments, natural experiments, comparative cases, difference-in-differences analysis
Employee trust and surveillance	How does AI-use monitoring affect privacy concerns, trust, disclosure, and concealment?	Individual and organization	Vignette experiments, surveys, interviews, privacy impact assessments
Technical discovery	How accurately can organizations detect embedded, local, encrypted, and agent-based shadow AI while limiting false alarms?	System and network	Benchmarking, security testing, prototype evaluation, red-team exercises
Formalization of employee innovation	How can valuable shadow practices be transferred into secure and scalable organizational systems?	Team and organization	Longitudinal case studies, action research, process tracing

Shadow agents	How do autonomy, memory, permissions, and inter-agent communication alter security and accountability?	Agent, workflow, organization	Agent simulations, controlled experiments, runtime log analysis, threat modeling
Sectoral and cross-national variation	How do regulation, professional norms, culture, and data sensitivity change the causes and consequences of shadow AI?	Sector and country	Cross-country surveys, comparative institutional analysis, multigroup models

The research domains in Table 4 are interconnected. Measurement quality will influence the validity of studies examining behavioral drivers and organizational outcomes. Governance research requires reliable indicators of actual behavior, while technical detection research must consider employee trust and privacy. Agentic AI research will also require cooperation among cybersecurity, information systems, organizational behavior, law, and human–computer interaction scholars. Interdisciplinary designs should retain a clear focal question and define how each disciplinary perspective contributes to its explanation.

Future evidence should ultimately help organizations answer three practical questions: where shadow AI exists, why employees rely on it, and which response produces an acceptable balance among security, accountability, innovation, and employee needs. Research that addresses these questions through transparent measurement, longitudinal evidence, and field-based evaluation can move the literature from general risk awareness toward a mature body of organizational knowledge.

6. Conclusion

Shadow AI has emerged as a significant organizational challenge as employees gain direct access to powerful generative and agentic AI tools. These technologies can support productivity, creativity, learning, and rapid problem-solving, yet their use outside formal organizational oversight creates serious risks for information security, privacy, intellectual property, regulatory compliance, and decision quality. The defining problem is the gap between the AI systems organizations believe they manage and the tools, data flows, integrations, and automated processes that employees actually use.

The analysis presented in this chapter shows that shadow AI cannot be explained solely as employee misconduct or weak cybersecurity. Its emergence is shaped by technological accessibility, performance expectations, task–technology mismatches, time pressure, inadequate organizational tools,

ambiguous policies, and social norms surrounding AI use. Employees often adopt unauthorized AI applications because these tools provide immediate solutions to operational problems. Shadow AI therefore reflects weaknesses in organizational technology provision and governance as well as individual choices.

The risks associated with shadow AI extend across the confidentiality, integrity, and availability of organizational information. Employees may expose confidential data, personal information, source code, internal documents, and intellectual property to unapproved external services. AI-generated outputs may introduce factual errors, fabricated information, bias, insecure code, or misleading recommendations into organizational workflows. Undocumented integrations and autonomous agents may expand the organizational attack surface by connecting external models to internal data sources and business applications. These risks become more difficult to detect and manage when organizations lack visibility into how AI is actually being used (National Institute of Standards and Technology [NIST], 2024; Puthal et al., 2025).

Effective governance requires a balance between organizational control and employee enablement. Blanket prohibitions may reduce visible use while encouraging employees to move their AI activities to personal accounts, devices, and less observable environments. Weak governance leaves employees to make complex decisions about data sensitivity, legal requirements, and output reliability without sufficient guidance. A more effective approach combines clear policies, risk-based classification, approved enterprise tools, rapid authorization procedures, technical safeguards, human review, employee training, monitoring, and incident-response mechanisms. Haag and Eckhardt (2024) similarly argue that shadow technology should be managed through an approach that addresses cybersecurity requirements and legitimate user needs.

Organizational AI governance should treat visibility as a central objective. Organizations need to identify which AI tools are used, what data they process, how they are integrated into workflows, which decisions they influence, and who is responsible for their outcomes. AI inventories, impact assessments, ownership structures, access controls, data-classification rules, vendor evaluations, and provenance records can support this objective. Governance arrangements should remain adaptive because AI applications, provider conditions, threat techniques, and organizational use cases change rapidly. The governance of AI is therefore an ongoing organizational capability rather than a one-time compliance exercise (Mäntymäki et al., 2022; NIST, 2023).

Employee participation is essential for improving organizational visibility. Workers are often the first to recognize where AI can improve a process or

where existing systems fail to meet operational requirements. Reporting mechanisms, controlled experimentation environments, and pathways for formalizing useful employee-created solutions can help organizations convert valuable shadow practices into secure organizational capabilities. Waters-Lynch et al. (2025) emphasize that covert generative AI use may contribute to organizational renewal when employee innovations are identified, evaluated, and integrated into formal structures. Governance should therefore distinguish responsible experimentation from reckless or harmful use.

The growth of agentic AI will make this distinction increasingly important. AI systems are beginning to move beyond content generation toward task execution, tool use, data retrieval, and automated interaction with business systems. Unauthorized agents may act through employee accounts, access multiple data sources, and perform actions without adequate human review. Future governance models must therefore consider levels of autonomy, permission boundaries, identity management, tool access, action limits, and accountability for AI-generated decisions and actions.

Shadow AI ultimately represents a test of organizational adaptability. Organizations that respond through rigid control may suppress useful experimentation without eliminating hidden use. Organizations that ignore the issue may expose themselves to escalating security, legal, and operational risks. Sustainable governance requires proportionate controls, secure alternatives, credible accountability, and continuous dialogue between employees, managers, technical specialists, legal professionals, and security teams.

The central argument of this chapter is that shadow AI should be managed through visibility, proportionality, accountability, and enablement. Visibility allows organizations to understand actual AI use. Proportionality ensures that controls correspond to the sensitivity and impact of each use case. Accountability clarifies responsibility for data, systems, outputs, and decisions. Enablement provides employees with secure and practical alternatives to unauthorized tools. Organizations that develop these capabilities will be better positioned to benefit from AI while protecting their information assets and maintaining trust among employees, customers, regulators, and other stakeholders.

References

Barberá, I. (2025). *AI privacy risks & mitigations: Large language models (LLMs)*. European Data Protection Board.

Barlette, Y., Berthevas, J.-F., Richet, J.-L., & Georg Schaffner, L. (2025). Investigating the influence of emotions on shadow IT usage behaviours. *Systèmes d'Information & Management, 30*(2), 99–149. https://doi.org/10.54695/sim.252.0099

Brynjolfsson, E., Li, D., & Raymond, L. (2025). Generative AI at work. *The Quarterly Journal of Economics, 140*(2), 889–942. https://doi.org/10.1093/qje/qjae044

Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, Ú., Oprea, A., & Raffel, C. (2021). Extracting training data from large language models. In *Proceedings of the 30th USENIX Security Symposium* (pp. 2633–2650). USENIX Association. https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting

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*, Article 102793. https://doi.org/10.1016/j.techsoc.2024.102793

Dolci, P. C., & Aguiar, M. S. (2025). Governance and generative artificial intelligence: Challenges and risks of shadow AI in business environment. In *Proceedings of the 31st Americas Conference on Information Systems (AMCIS 2025)*. Association for Information Systems. https://aisel.aisnet.org/amcis2025/lacais/lacais/1/

Elsayed, Y., & Jones, C. (2026). Agentic explainability at scale: Between corporate fears and XAI needs [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2604.14984

European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union, L*, 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Farquhar, S., Kossen, J., Kuhn, L., & Gal, Y. (2024). Detecting hallucinations in large language models using semantic entropy. *Nature, 630*, 625–630. https://doi.org/10.1038/s41586-024-07421-0

Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. *Business & Information Systems Engineering, 66*, 111–126. https://doi.org/10.1007/s12599-023-00834-7

Greshake, K., Abdelnabi, S., Mishra, S., Endres, C., Holz, T., & Fritz, M. (2023). Not what you've signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection. In *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security* (pp. 79–90). Association for Computing Machinery. https://doi.org/10.1145/3605764.3623985

Haag, S., & Eckhardt, A. (2017). Shadow IT. *Business & Information Systems Engineering, 59*(6), 469–473. https://doi.org/10.1007/s12599-017-0497-x

Haag, S., & Eckhardt, A. (2024). Dealing effectively with shadow IT by managing both cybersecurity and user needs. *MIS Quarterly Executive, 23*(4), 399–412. https://doi.org/10.17705/2msqe.00104

International Organization for Standardization, & International Electrotechnical Commission. (2023). *Information technology—Artificial intelligence—Management system* (ISO/IEC Standard No. 42001:2023). International Organization for Standardization. https://www.iso.org/standard/81230.html

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. https://doi.org/10.12821/ijispm070102

Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics, 2*(4), 603–609. https://doi.org/10.1007/s43681-022-00143-x

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.600-1

National Institute of Standards and Technology. (2024b). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Nguyen, T. (2024). Understanding shadow IT usage intention: A view of the dual-factor model. *Online Information Review, 48*(3), 500–522. https://doi.org/10.1108/OIR-04-2022-0243

Noy, S., & Zhang, W. (2023). Experimental evidence on the productivity effects of generative artificial intelligence. *Science, 381*(6654), 187–192. https://doi.org/10.1126/science.adh2586

OWASP Foundation. (2024). *OWASP Top 10 for LLM applications 2025*. https://genai.owasp.org/llm-top-10/

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*, Article 405. https://doi.org/10.1007/s42979-025-03962-x

Waters-Lynch, J., Allen, D. W. E., Potts, J., & Berg, C. (2025). Shadow user innovation: Governing covert generative-AI use for dynamic-capability renewal. *Innovation: Organization & Management*, 1–17. https://doi.org/10.1080/14479338.2025.2519546

Bölüm 3

Düşük Kodlu/Kodsuz Platformlar ile İş Süreçleri Dönüşümü: Fırsatlar, Riskler ve Yönetişim Yaklaşımları[1]

Başak Gök[1]

Özet

Dijital dönüşüm, kuruluşların iş süreçlerini tasarlama, yönetme ve iyileştirme biçimlerini temelden değiştirmiştir. Kurumsal çeviklik, hızlı inovasyon ve operasyonel verimliliğe yönelik artan talepler, geleneksel yazılım geliştirme yaklaşımlarına alternatif olarak Düşük Kodlu/Kodsuz (Low-Code/No-Code - LCNC) platformların benimsenmesini hızlandırmıştır. Sınırlı programlama uzmanlığına sahip kullanıcıların uygulama geliştirmesine ve iş akışlarını otomatikleştirmesine olanak tanıyan LCNC platformları, dijital çözüm geliştirme süreçlerine katılımı genişletmiş ve vatandaş geliştirici (citizen developer) yaklaşımının ortaya çıkmasına katkı sağlamıştır. Bu platformlar, süreç inovasyonu ve kurumsal çeviklik açısından önemli fırsatlar sunarken; yönetişim, güvenlik, veri yönetimi ve kurumsal kontrol alanlarında çeşitli zorlukları da beraberinde getirmektedir.

Bu çalışmada, LCNC platformlarının iş süreçleri dönüşümündeki rolü; iş süreci yönetimi, vatandaş geliştirici yaklaşımı ve bilgi teknolojileri yönetişimi perspektiflerinden incelenmiştir. Bu kapsamda LCNC platformlarının kavramsal temelleri ele alınmış, süreç çevikliği, kullanıcı katılımı, süreç görünürlüğü ve iş birimleri ile bilgi teknolojileri departmanları arasındaki iş birliği üzerindeki etkileri tartışılmıştır. Ayrıca LCNC destekli süreç dönüşümünün güçlü yönlerini, zayıf yönlerini, fırsatlarını ve tehditlerini değerlendirmek amacıyla SWOT analizi gerçekleştirilmiştir. Elde edilen bulgular, LCNC platformlarının süreç geliştirme hızını, operasyonel esnekliği ve kullanıcı katılımını önemli ölçüde artırabildiğini; buna karşılık gölge BT, teknik borç, güvenlik açıkları ve yönetişim sorunları gibi riskleri de beraberinde getirebildiğini göstermektedir.

1 Dr. Öğretim Üyesi, Gazi Üniversitesi Uygulamalı Bilimler Fakültesi Yönetim Bilişim Sistemleri Bölümü, Ankara – Türkiye, basakgok@gazi.edu.tr, https://orcid.org/0000-0002-8687-5961

https://doi.org/10.58830/ozgur.pub1366.c5529

Bulgular doğrultusunda bölümde, stratejik yönetişim, süreç yönetişimi, veri yönetişimi, teknoloji yönetişimi ve güvenlik yönetişimi boyutlarından oluşan bütünleşik bir yönetişim modeli önerilmektedir. Önerilen çerçeve, örgütsel çeviklik ile kontrol mekanizmaları arasında denge kurmayı amaçlamakta ve vatandaş geliştirici girişimlerinin sürdürülebilir biçimde yönetilmesine yönelik rehberlik sunmaktadır. Yapay zekâ entegrasyonu, süreç madenciliği, hiperotomasyon ve vatandaş geliştiricilerin dijital dönüşüm girişimlerindeki değişen rolleri gelecekteki gelişim alanları olarak değerlendirilmiştir.

1. Giriş

Sanayi toplumundan bilgi toplumuna geçiş sürecinde teknoloji, bilgi ve insan sermayesi ekonomik ve örgütsel sistemlerin temel belirleyicileri haline gelmiştir. Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, kurumların rekabet avantajı elde etme biçimlerini önemli ölçüde değiştirmiş; örgütler yalnızca operasyonel süreçlerini değil, aynı zamanda yönetim anlayışlarını, örgütsel yapılarını ve insan kaynakları uygulamalarını da dijital temelde yeniden yapılandırmak zorunda kalmışlardır (Gök, 2026). Bu dönüşümün bir sonucu olarak dijital dönüşüm, günümüzde kurumların iş yapma biçimlerini, organizasyonel yapılarını ve süreç yönetimi anlayışlarını yeniden şekillendiren temel unsurlardan biri haline gelmiştir. Artan rekabet koşulları, müşteri beklentilerindeki hızlı değişim, veri hacmindeki büyüme ve teknolojik gelişmeler, kurumların süreçlerini daha çevik, esnek ve hızlı hale getirme gereksinimini artırmaktadır (Verhoef vd., 2021). Bu bağlamda organizasyonlar yalnızca mevcut faaliyetlerini dijital ortama taşımayı değil, aynı zamanda süreçlerini yeniden tasarlayarak daha etkin, verimli ve sürdürülebilir biçimde yönetmeyi amaçlamaktadır. İş süreçlerinin dijitalleşmesi; operasyonel verimliliğin artırılmasına, karar alma süreçlerinin hızlandırılmasına ve organizasyonların değişen çevresel koşullara daha hızlı uyum sağlayabilmesine katkı sunmaktadır (Bharadwaj vd., 2013). Bu nedenle günümüzde dijital dönüşümün başarısı, büyük ölçüde iş süreçlerinin ne ölçüde yeniden tasarlanabildiği, otomatikleştirilebildiği ve etkin biçimde yönetilebildiği ile ilişkilendirilmektedir.

İş süreçleri yönetimi (business process management), kurumların iş süreçlerini sistematik biçimde analiz etme, modelleme, uygulama, izleme ve sürekli iyileştirme faaliyetlerini kapsayan bütünleşik bir yönetim yaklaşımıdır (Dumas vd., 2018, Şahinarslan, 2023). Geleneksel iş süreçleri yönetimi yaklaşımlarında süreçlerin modellenmesi ve geliştirilmesi çoğunlukla bilgi teknolojileri (BT) birimleri tarafından yürütülmektedir. Ancak merkezi BT yaklaşımı; uzun geliştirme döngüleri, yüksek maliyetler, iş birimleri ile teknik ekipler arasında iletişim sorunları ve kullanıcı ihtiyaçlarına hızlı cevap verememe gibi çeşitli sınırlılıklar ortaya çıkarabilmektedir (Mendling vd., 2020). Özellikle

hızla değişen iş ortamlarında organizasyonların yalnızca süreçlerini tanımlaması yeterli olmamakta, süreçlerin dinamik biçimde yürütülebilir ve güncellenebilir olması önem kazanmaktadır.

Bu ihtiyaçlar doğrultusunda son yıllarda Düşük Kodlu/Kodsuz (Low-Code/No-Code – LCNC) platformlar kurumların dijital dönüşüm stratejilerinde önemli bir yere sahip olmaya başlamıştır. LCNC platformları, kullanıcıların sınırlı düzeyde programlama bilgisiyle veya herhangi bir yazılım geliştirme bilgisine ihtiyaç duymadan uygulama geliştirmelerine ve süreç otomasyonları oluşturmalarına olanak tanımaktadır (Sanchis vd., 2020). Görsel tasarım araçları, sürükle-bırak ara yüzleri, hazır bileşenler ve entegrasyon mekanizmaları sayesinde bu platformlar uygulama geliştirme süreçlerini hızlandırmakta ve iş birimlerinin süreç geliştirme faaliyetlerine daha aktif katılımını desteklemektedir.

LCNC platformlarının yaygınlaşmasıyla birlikte "vatandaş geliştirici" (citizen developer) kavramı da önem kazanmaya başlamıştır. Vatandaş geliştiriciler, profesyonel yazılım geliştiricisi olmamalarına rağmen kurumsal ihtiyaçlara yönelik uygulamalar ve iş akışları geliştirebilen kullanıcıları ifade etmektedir. Bu yaklaşım, süreç geliştirme faaliyetlerinin yalnızca BT departmanlarının sorumluluğunda olmadığı, iş birimlerinin de aktif olarak süreç tasarlayabildiği daha demokratik bir yapı ortaya çıkarmaktadır. Böylece süreç geliştirme faaliyetleri merkezi yapılardan dağıtık yapılara doğru evrilmekte ve organizasyonlar daha yüksek düzeyde çeviklik kazanabilmektedir.

Bununla birlikte süreç geliştirme faaliyetlerinin organizasyon genelinde yaygınlaşması yalnızca fırsatlar değil aynı zamanda çeşitli riskler de ortaya çıkarmaktadır. Kontrol mekanizmaları dışında geliştirilen uygulamalar ve süreçler, literatürde sıklıkla "Gölge BT" (Shadow IT) olarak ifade edilmektedir (Behrens, 2009). Kontrolsüz süreç geliştirme faaliyetleri veri bütünlüğü problemleri, güvenlik açıkları, standartlaşma sorunları, teknik borç (technical debt) ve yönetişim eksiklikleri gibi riskleri beraberinde getirebilmektedir (Lamanna, 2025). Özellikle vatandaş geliştiricilerin oluşturduğu uygulamaların kurumsal bilgi sistemleriyle entegrasyonu ve sürdürülebilir yönetimi önemli bir yönetişim konusu haline gelmektedir.

Bu bağlamda LCNC platformlar yalnızca yazılım geliştirme araçları olarak değerlendirilmemeli; süreç yönetimini, kullanıcı rollerini ve organizasyonel yapıların işleyişini dönüştüren sosyoteknik sistemler olarak ele alınmalıdır. Bu bölümün amacı, LCNC platformlarının iş süreçlerinin dönüşümündeki rolünü vatandaş geliştirici yaklaşımı ve yönetişim perspektifi çerçevesinde incelemek; bu teknolojilerin sağladığı fırsatları, organizasyonel etkileri ve ortaya çıkardığı yönetsel sorunları literatür temelinde değerlendirmektir.

2. LCNC Platformlar ve Kuramsal Temeller

2.1. İş Süreçleri Yönetimi ve Dijitalleşme

İş süreçleri, belirli bir kurumsal hedefin gerçekleştirilmesi amacıyla birbirleriyle ilişkili faaliyetlerin sistematik biçimde yürütülmesini ifade etmektedir. İş süreçleri yönetimi ise süreçlerin analiz edilmesi, modellenmesi, uygulanması, izlenmesi ve sürekli iyileştirilmesini kapsayan bütünleşik bir yönetim yaklaşımıdır (Dumas vd., 2018; Şahinarslan, 2023; Çelik, 2025). İş süreçleri yönetimi yaklaşımı yalnızca süreçlerin tanımlanmasına odaklanmamakta; aynı zamanda süreç performansının artırılması, maliyetlerin azaltılması ve organizasyonel çevikliğin geliştirilmesini amaçlamaktadır (Sebetci vd., 2018; Czvetkó vd., 2022). Bu yönüyle İş süreçleri yönetimi, kurumsal operasyonların stratejik hedeflerle uyumlu biçimde yönetilmesini sağlayan önemli bir yönetim aracı olarak değerlendirilmektedir.

Dijital dönüşümün hız kazanmasıyla birlikte iş süreçlerinin organizasyonel performans üzerindeki etkisi daha görünür hale gelmiştir. İş süreçleri artık yalnızca operasyonel faaliyetleri yöneten mekanizmalar değil; aynı zamanda kurumların rekabet avantajı oluşturmasında kritik rol oynayan dinamik yapılar olarak değerlendirilmektedir (Bharadwaj vd., 2013; Özan, 2021, Özveri & Kabak, 2016). Veri odaklı süreç yönetimi sayesinde organizasyonlar müşteri beklentilerine daha hızlı yanıt verebilmekte, inovasyon faaliyetlerini destekleyebilmekte ve değişen çevresel koşullara daha kolay uyum sağlayabilmektedir (Beerepoot vd., 2023).

Bununla birlikte geleneksel iş süreçleri yaklaşımlarında süreç modelleme ve geliştirme faaliyetlerinin büyük ölçüde merkezi BT ekipleri tarafından yürütülmesi çeşitli sınırlılıklar ortaya çıkarabilmektedir. Özellikle süreç değişikliklerinin uygulanmasındaki gecikmeler, iş birimleri ile teknik ekipler arasında oluşan iletişim sorunları ve kullanıcı beklentilerinin tam olarak karşılanamaması bu sınırlılıkların başında gelmektedir (Mendling vd., 2020). Bu durum daha çevik, kullanıcı odaklı ve esnek süreç geliştirme yaklaşımlarına olan ihtiyacı artırmıştır.

2.2. LCNC Platformlar ve Yazılım Geliştirmenin Demokratikleşmesi

LCNC platformlar, uygulama geliştirme faaliyetlerini hızlandırmak amacıyla görsel modelleme araçları, hazır bileşenler, sürükle-bırak ara yüzleri ve otomatik süreç mekanizmaları sunan platformlar olarak tanımlanmaktadır (Sanchis vd., 2020). Geleneksel yazılım geliştirme süreçlerinde uygulama geliştirme büyük ölçüde programlama becerilerine bağlıyken, LCNC platformları

teknik karmaşıklığı azaltarak daha geniş kullanıcı gruplarının süreç geliştirme faaliyetlerine katılımını mümkün hale getirmektedir (Waszkowski, 2019).

LCNC platformlarının yaygınlaşmasının temel nedenlerinden biri, kurumların artan dijitalleşme ve uygulama geliştirme taleplerine geleneksel yöntemlerle yeterince hızlı cevap verememesidir. Bu platformlar uygulama geliştirme sürelerini kısaltmakta, maliyetleri azaltmakta ve organizasyonel çevikliği artırmaktadır (Sahay vd., 2020; Serekov vd., 2025). Ayrıca API tabanlı entegrasyon mekanizmaları ve hazır iş akışı bileşenleri sayesinde iş birimleri ile BT ekipleri arasındaki etkileşimi güçlendirmekte ve süreç geliştirme faaliyetlerini daha erişilebilir hale getirmektedir (Kirchhof vd., 2023).

Bu gelişmeler yazılım geliştirmenin demokratikleşmesi olarak ifade edilen yeni bir yaklaşımın ortaya çıkmasına katkı sağlamıştır. Yazılım geliştirmenin demokratikleşmesi, uygulama geliştirme faaliyetlerinin yalnızca profesyonel yazılımcılar tarafından değil, teknik bilgisi sınırlı alan uzmanları tarafından da gerçekleştirilebilmesini ifade etmektedir (Sahay vd., 2020). Böylece çalışanlar teknolojinin yalnızca kullanıcıları değil, aynı zamanda kurumsal dijital dönüşümün aktif üreticileri haline gelmektedir. Bu yaklaşım özellikle yetişmiş yazılım geliştirici eksikliğinin yaşandığı ortamlarda kurumların dijitalleşme kapasitesini artırabilecek stratejik bir fırsat olarak değerlendirilmektedir.

Bununla birlikte LCNC platformları yalnızca uygulama geliştirme araçları olarak değerlendirilmemelidir. Son dönem çalışmalar, bu platformların organizasyonel süreçleri, karar alma mekanizmalarını ve iş yapma biçimlerini dönüştüren önemli bir dijitalleşme bileşeni olduğunu savunmaktadır (Ajimati vd., 2025).

2.3. Vatandaş Geliştirici Yaklaşımı ve BT Yönetişimi Perspektifi

LCNC platformlarının yaygınlaşmasıyla birlikte vatandaş geliştirici kavramı bilgi sistemleri literatüründe önemli bir yer edinmiştir. Vatandaş geliştiriciler, profesyonel yazılım geliştirme uzmanı olmamalarına rağmen iş süreçleri ihtiyaçlarına yönelik dijital çözümler geliştirebilen kullanıcılar olarak tanımlanmaktadır (Binzer & Winkler, 2024). Artan dijitalleşme gereksinimleri, yazılım geliştirici eksikliği ve organizasyonların çeviklik ihtiyacı bu yaklaşımın yaygınlaşmasında etkili olmuştur (France & Rumpe, 2007; Sahay vd., 2020).

Vatandaş geliştirici yaklaşımı, iş süreçlerine ilişkin bilgi ve deneyime sahip kullanıcıların süreç geliştirme faaliyetlerine doğrudan katılmasını sağlayarak gereksinimlerin daha doğru belirlenmesine ve uygulama geliştirme sürelerinin kısalmasına katkı sunmaktadır (Muhammad vd., 2024). Görsel modelleme araçları, sürükle-bırak tasarımlar ve üretken yapay zeka destekli geliştirme

ortamları, teknik bilgi gereksinimini azaltarak bu dönüşümü desteklemektedir (Çelik, 2025; Özdem & Bora, 2022).

Ancak süreç geliştirme faaliyetlerinin organizasyon genelinde yaygınlaşması bazı yönetsel ve teknik riskleri de beraberinde getirmektedir. Bu bağlamda BT yönetişimi yaklaşımı önem kazanmaktadır. BT yönetişimi, BT'nin organizasyonel hedeflerle uyumlu biçimde kullanılmasını sağlayan yapı, süreç ve kontrol mekanizmalarını ifade etmektedir (Weill & Ross, 2004). LCNC ortamlarında süreç geliştirme faaliyetlerinin merkezi BT yapılarından iş birimlerine doğru yayılması, veri yönetimi, güvenlik, standartlaşma ve denetlenebilirlik konularında yeni gereksinimler ortaya çıkarmaktadır (Binzer vd., 2024).

Bu kapsamda literatürde sıklıkla vurgulanan kavramlardan biri Gölge BT'dir. Gölge BT, çalışanlar veya iş birimleri tarafından merkezi BT departmanının bilgisi veya kontrolü dışında geliştirilen ve kullanılan uygulamaları ifade etmektedir (Behrens, 2009; Rokis & Kirikova, 2023). Kontrolsüz uygulama geliştirme faaliyetleri veri bütünlüğü problemlerine, güvenlik açıklarına, entegrasyon sorunlarına ve teknik borç oluşumuna neden olabilmektedir (Davenport, 2023; Acitelli vd., 2024; Lamanna, 2025).

Bu nedenle güncel literatür, LCNC platformlarının başarılı biçimde uygulanabilmesi için teknoloji yönetişiminin yanı sıra süreç yönetişimi, veri yönetişimi ve vatandaş geliştirici yönetiminin birlikte ele alınması gerektiğini vurgulamaktadır (Binzer vd., 2024; Viljoen vd., 2024). Bu çerçevede LCNC platformları yalnızca yazılım geliştirme araçları olarak değil, süreçleri, kullanıcı rollerini ve organizasyonel yapıları dönüştüren sosyoteknik sistemler olarak değerlendirilmelidir.

3. Düşük Kodlu/Kodsuz Platformlar ile İş Süreçlerinin Dönüşümü

Dijital dönüşümün hız kazanmasıyla birlikte organizasyonlar yalnızca süreçlerini dijital ortama aktarmaya değil, aynı zamanda süreçlerini yeniden tasarlamaya ve daha çevik yapılar oluşturmaya yönelmektedir. Geleneksel süreç yönetimi yaklaşımları uzun geliştirme döngüleri, yüksek teknik bağımlılık ve sınırlı kullanıcı katılımı nedeniyle günümüzün dinamik iş ortamlarında bazı yetersizlikler gösterebilmektedir (Mendling vd., 2020). Bu bağlamda LCNC platformlar, süreç geliştirme faaliyetlerinin hızlandırılmasına ve iş süreçlerinin daha esnek biçimde yönetilmesine olanak sağlayan önemli teknolojik araçlar olarak öne çıkmaktadır.

LCNC platformlarının iş süreçleri üzerindeki etkisi yalnızca uygulama geliştirme hızındaki artışla sınırlı değildir. Bu platformlar süreçlerin tasarlanma, uygulanma, izlenme ve iyileştirilme biçimlerini dönüştürerek organizasyonların

iş yapma anlayışında önemli değişikliklere yol açmaktadır. Özellikle süreç yönetiminin merkezi BT yapılarından daha katılımcı ve dağıtık yapılara doğru evrilmesinde LCNC teknolojilerinin önemli rol oynadığı görülmektedir (Binzer vd., 2024).

3.1. Geleneksel Süreç Yaklaşımından LCNC Tabanlı Süreç Yönetimine Geçiş

Geleneksel süreç geliştirme yaklaşımlarında iş süreçlerinin dijital ortama aktarılması genellikle iş analistleri, yazılım geliştiriciler ve sistem uzmanlarından oluşan ekipler tarafından yürütülmektedir. Süreç gereksinimlerinin belirlenmesi, teknik tasarımın hazırlanması, yazılım geliştirme faaliyetlerinin gerçekleştirilmesi ve uygulamanın devreye alınması çoğu zaman uzun zaman alan aşamalardan oluşmaktadır (Dumas vd., 2018).

Bu yaklaşım özellikle süreç gereksinimlerinin sık değiştiği organizasyonlarda çeşitli sorunlara neden olabilmektedir. İş birimlerinin ihtiyaçları ile geliştirilen çözümler arasında zaman içinde uyumsuzluklar oluşabilmekte, süreç güncellemeleri gecikebilmekte ve BT birimleri önemli bir talep yüküyle karşı karşıya kalabilmektedir (Mendling vd., 2020).

LCNC platformları bu bağlamda süreç geliştirme faaliyetlerini daha çevik hale getirmektedir. Görsel süreç modelleme araçları, sürükle-bırak tasarım bileşenleri ve hazır entegrasyon mekanizmaları sayesinde süreç tasarımları daha kısa sürede oluşturulabilmekte ve süreç değişiklikleri daha hızlı uygulanabilmektedir (Sanchis vd., 2020). Böylece süreç geliştirme faaliyetleri yalnızca teknik ekiplerin sorumluluğunda olmaktan çıkmakta ve iş birimlerinin aktif katılımıyla yürütülebilen bir yapıya dönüşmektedir.

Bu dönüşüm yalnızca teknolojik değil, aynı zamanda organizasyonel bir değişimi de ifade etmektedir. Süreç geliştirme faaliyetlerinin demokratikleşmesi, süreç sahiplerinin ve alan uzmanlarının süreç tasarımına daha aktif katılım göstermesine olanak tanımaktadır. Bu durum süreçlerin gerçek operasyonel ihtiyaçlarla daha uyumlu biçimde geliştirilmesine katkı sağlamaktadır (Muhammad vd., 2024).

3.2. İş Süreçleri Üzerindeki Organizasyonel Etkiler

LCNC platformlarının yaygınlaşmasıyla birlikte iş süreçlerinde çeşitli organizasyonel etkiler ortaya çıkmaktadır. Literatürde bu etkiler çoğunlukla süreç çevikliği, kullanıcı katılımı, süreç görünürlüğü ve organizasyonel iş birliği başlıkları altında değerlendirilmektedir.

3.2.1. Süreç Çevikliği

LCNC platformlarının en önemli katkılarından biri süreç çevikliğini artırmasıdır. Geleneksel geliştirme yaklaşımlarında haftalar veya aylar sürebilen süreç güncellemeleri, LCNC platformlarında daha kısa sürelerde gerçekleştirilebilmektedir. Bu durum organizasyonların değişen müşteri taleplerine ve çevresel koşullara daha hızlı uyum sağlamasına olanak tanımaktadır (Rokis & Kirikova, 2023).

Özellikle pandemi sonrası dönemde hızla değişen iş koşulları, organizasyonların süreçlerini sürekli güncellemesini gerekli kılmıştır. LCNC platformları bu değişimlerin daha düşük maliyet ve daha kısa sürelerle gerçekleştirilmesine katkı sağlamaktadır (Sahay vd., 2020).

3.2.2. Kullanıcı Katılımı ve Süreç Sahipliği

LCNC platformları süreç geliştirme faaliyetlerini yalnızca BT uzmanlarının yürüttüğü bir faaliyet olmaktan çıkararak iş birimlerinin de sürece aktif katılımını mümkün kılmaktadır. Bu durum kullanıcıların süreçlere ilişkin bilgi ve deneyimlerini doğrudan tasarım sürecine yansıtabilmelerine olanak tanımaktadır (Binzer & Winkler, 2024).

Vatandaş geliştirici yaklaşımı sayesinde süreç sahipleri ihtiyaç duydukları iyileştirmeleri daha hızlı hayata geçirebilmekte ve süreçlerin geliştirilmesinde daha etkin rol alabilmektedir. Bu durum süreç sahipliğinin güçlenmesine ve organizasyonel öğrenmenin desteklenmesine katkı sağlamaktadır (Muhammad vd., 2024).

3.2.3. Süreç Görünürlüğü ve Şeffaflık

LCNC tabanlı iş süreçleri yönetiminde süreçlerin dijital ortamda yürütülmesi, süreç performansının daha etkin izlenebilmesine olanak sağlamaktadır. Süreçlerin hangi aşamada bulunduğu, işlem süreleri, darboğazlar ve performans göstergeleri gerçek zamanlı olarak takip edilebilmektedir (Dumas vd., 2018).

Artan süreç görünürlüğü yöneticilerin karar alma süreçlerini desteklemekte ve süreç iyileştirme faaliyetleri için daha güçlü veri altyapısı oluşturmaktadır.

3.2.4. İş Birimleri ile BT Arasındaki İş Birliği

LCNC platformları iş birimleri ile BT ekipleri arasındaki geleneksel ayrımı azaltmaktadır. Ortak süreç modelleme araçları ve görsel geliştirme ortamları sayesinde taraflar arasında daha etkili iletişim kurulabilmektedir (Kirchhof vd., 2023). Bu durum iş gereksinimlerinin daha doğru anlaşılmasına ve geliştirilen çözümlerin kullanıcı beklentileriyle daha uyumlu olmasına katkı sağlamaktadır.

3.3. LCNC Tabanlı Süreç Dönüşümünün Değerlendirilmesi

LCNC platformları iş süreçlerinin dijitalleşmesinde önemli fırsatlar sunmaktadır. Hızlı geliştirme, süreç çevikliği, kullanıcı katılımı ve süreç görünürlüğü bu teknolojilerin öne çıkan avantajları arasında yer almaktadır (Binzer vd., 2024; Sanchis vd., 2020). Bununla birlikte süreç geliştirme faaliyetlerinin organizasyon geneline yayılması yeni yönetişim gereksinimlerini de beraberinde getirmektedir.

Özellikle süreç geliştirme faaliyetlerinin demokratikleşmesi, kontrol mekanizmalarının yeniden tanımlanmasını gerekli kılmaktadır. Güvenlik, veri yönetimi, standartlaşma ve denetlenebilirlik gibi konular LCNC tabanlı süreç dönüşümünün sürdürülebilirliği açısından kritik önem taşımaktadır (Viljoen vd., 2024).

Bu nedenle LCNC platformlarının organizasyonlarda başarılı biçimde uygulanabilmesi yalnızca teknolojik yeteneklere değil, aynı zamanda vatandaş geliştirici faaliyetlerini yönlendirecek uygun yönetişim mekanizmalarına da bağlıdır. Bu bağlamda bir sonraki bölümde LCNC ekosisteminin sunduğu fırsatlar ve beraberinde getirdiği riskler SWOT analizi çerçevesinde değerlendirilmektedir.

4. LCNC Ekosisteminde Fırsatlar ve Riskler: SWOT Analizi

LCNC platformlar, organizasyonların dijital dönüşüm süreçlerinde giderek daha önemli bir rol üstlenmektedir. Bu platformlar iş süreçlerinin daha hızlı geliştirilmesine, kullanıcı katılımının artırılmasına ve süreç çevikliğinin geliştirilmesine katkı sağlarken; aynı zamanda güvenlik, veri yönetimi ve yönetişim açısından çeşitli riskleri de beraberinde getirmektedir. Bu nedenle LCNC teknolojilerinin organizasyonlar üzerindeki etkilerinin bütüncül biçimde değerlendirilmesi önem taşımaktadır. SWOT analizi, bir teknolojinin veya stratejik yaklaşımın güçlü ve zayıf yönleri ile dış çevreden kaynaklanan fırsat ve tehditleri sistematik biçimde değerlendirmeye olanak sağlayan yaygın bir stratejik analiz aracıdır (Gürel & Tat, 2017).

Bu bölümde SWOT analizi, önceki bölümlerde tartışılan literatür bulgularının sistematik biçimde değerlendirilmesi amacıyla kullanılmıştır. Analiz kapsamında LCNC platformlarının iş süreçleri üzerindeki etkileri; organizasyonel çeviklik, süreç yönetimi, vatandaş geliştirici yaklaşımı ve BT yönetişimi perspektiflerinden ele alınmıştır.

4.1. LCNC Platformlarının SWOT Matrisi

LCNC platformlarının organizasyonlar üzerindeki etkileri yalnızca teknolojik avantajlarla sınırlı değildir. Bu platformlar süreç geliştirme faaliyetlerini hızlandırırken aynı zamanda yeni yönetsel, teknik ve organizasyonel riskleri de beraberinde getirmektedir. Bu nedenle LCNC ekosisteminin bütüncül biçimde değerlendirilebilmesi için güçlü ve zayıf yönlerin yanı sıra dış çevreden kaynaklanan fırsat ve tehditlerin birlikte ele alınması gerekmektedir. SWOT analizi, organizasyonların mevcut durumlarını sistematik biçimde değerlendirmelerine olanak sağlayan stratejik bir analiz aracı olarak yaygın şekilde kullanılmaktadır (Gürel & Tat, 2017). Bu çalışmada SWOT analizi, önceki bölümlerde incelenen literatür bulgularının sentezlenmesi amacıyla kullanılmış ve LCNC tabanlı iş süreçleri dönüşümünün güçlü yönleri, zayıf yönleri, fırsatları ve tehditleri belirlenmiştir. Elde edilen bulgular Tablo 4.1'de sunulmaktadır.

Tablo 4.1. LCNC Tabanlı İş Süreçleri Dönüşümünün SWOT Analizi

Güçlü yönler	**Zayıf yönler**
Süreç geliştirme hızının artması	Teknik borç oluşumu
Operasyonel çeviklik sağlaması	Platform bağımlılığı
Kullanıcı katılımının artması	Karmaşık süreçlerde sınırlı özelleştirme
Süreç görünürlüğünün iyileşmesi	Entegrasyon güçlükleri
BT iş yükünün azalması	Standartlaştırma sorunları
Düşük geliştirme maliyeti	Yetersiz teknik dokümantasyon
Fırsatlar	**Tehditler**
Yapay zeka destekli süreç geliştirme	Gölge BT oluşumu
Süreç madenciliği entegrasyonu	Güvenlik açıkları
Dijital dönüşüm stratejileri	Veri gizliliği riskleri
Hiperotomasyon uygulamaları	Denetlenebilirlik sorunları
Vatandaş geliştirici ekosistemleri	Düzenleyici uyum problemleri
Bulut tabanlı entegrasyon olanakları	Kontrol kaybı ve süreç parçalanması

Tablo 4.1 incelendiğinde LCNC platformlarının organizasyonlara önemli avantajlar sunduğu görülmektedir. Süreç geliştirme hızının artması, operasyonel çevikliğin güçlenmesi, kullanıcı katılımının desteklenmesi ve süreç görünürlüğünün iyileştirilmesi bu teknolojilerin öne çıkan güçlü yönleri arasında yer almaktadır. Bununla birlikte teknik borç oluşumu, platform bağımlılığı ve entegrasyon güçlükleri gibi yapısal sınırlılıklar LCNC uygulamalarının sürdürülebilirliği açısından dikkat edilmesi gereken unsurlar olarak ortaya çıkmaktadır.

Fırsatlar boyutunda yapay zekâ destekli süreç geliştirme, süreç madenciliği, hiperotomasyon ve vatandaş geliştirici ekosistemlerinin gelişimi öne çıkarken;

tehditler boyutunda gölge BT oluşumu, güvenlik açıkları, veri gizliliği riskleri ve düzenleyici uyum gereksinimleri dikkat çekmektedir. Bu bulgular, LCNC platformlarının başarılı biçimde uygulanabilmesi için yalnızca teknolojik yetkinliklerin değil, aynı zamanda etkili yönetişim mekanizmalarının da gerekli olduğunu göstermektedir. SWOT analizinin ortaya koyduğu bu değerlendirmeler, sonraki bölümde sunulan LCNC yönetişim modelinin teorik temelini oluşturmaktadır.

4.2. Güçlü Yönler ve Fırsatların Değerlendirilmesi

Literatürde LCNC platformlarının en önemli avantajlarından birinin süreç geliştirme sürelerini önemli ölçüde azaltması olduğu belirtilmektedir (Sanchis vd., 2020; Waszkowski, 2019). Görsel geliştirme araçları ve hazır bileşenler sayesinde süreçlerin daha kısa sürede tasarlanabilmesi organizasyonel çevikliği artırmaktadır. Özellikle sürekli değişen iş ortamlarında süreç güncellemelerinin hızlı biçimde gerçekleştirilebilmesi önemli bir rekabet avantajı oluşturmaktadır (Çelik, 2025).

LCNC platformlarının bir diğer önemli katkısı kullanıcı katılımını artırmasıdır. Vatandaş geliştirici yaklaşımı sayesinde süreç sahipleri geliştirme faaliyetlerine doğrudan katılabilmekte ve süreç gereksinimlerini daha etkin biçimde sisteme yansıtabilmektedir (Binzer & Winkler, 2024). Bu durum süreç sahipliğinin güçlenmesine ve organizasyonel öğrenmenin desteklenmesine katkı sağlamaktadır (Muhammad vd., 2024).

Fırsatlar açısından değerlendirildiğinde yapay zeka teknolojilerinin LCNC platformlarıyla bütünleşmesi dikkat çekmektedir. Üretken yapay zeka tabanlı yardımcı sistemlerin süreç tasarımını desteklemesi, süreç geliştirme faaliyetlerini daha geniş kullanıcı grupları için erişilebilir hale getirmektedir (Ajiboye, 2021; Çelik, 2025; Desmond vd., 2022). Benzer şekilde süreç madenciliği ve hiperotomasyon uygulamalarının LCNC ekosistemleriyle bütünleşmesi, süreç iyileştirme faaliyetlerinin daha veri odaklı yürütülmesine olanak sağlamaktadır (Berti vd., 2024).

4.3. Zayıf Yönler ve Tehditlerin Değerlendirilmesi

LCNC platformlarının sağladığı avantajlara rağmen bazı yapısal sınırlılıkları bulunmaktadır. Bunların başında teknik borç oluşumu gelmektedir. Kullanıcıların hızlı biçimde geliştirdiği uygulamalar başlangıçta işlevsel görünse de uzun vadede bakım ve sürdürülebilirlik sorunları ortaya çıkarabilmektedir (Binzer vd., 2024; Kirchhof vd., 2023). Ayrıca farklı iş birimleri tarafından geliştirilen uygulamaların zaman içerisinde çoğalması süreç karmaşıklığını artırabilmektedir.

Bir diğer önemli zayıflık platform bağımlılığıdır. Organizasyonların süreçlerini belirli bir LCNC sağlayıcısının teknolojik altyapısına dayandırması, uzun vadede tedarikçi bağımlılığı ve geçiş maliyetleri oluşturabilmektedir (Rokis & Kirikova, 2023).

Tehditler açısından değerlendirildiğinde Gölge BT oluşumu en önemli risklerden biri olarak öne çıkmaktadır. Merkezi BT birimlerinin kontrolü dışında geliştirilen uygulamalar veri bütünlüğü sorunlarına, güvenlik açıklarına ve entegrasyon problemlerine neden olabilmektedir (Behrens, 2009). Özellikle vatandaş geliştirici faaliyetlerinin uygun yönetişim mekanizmalarıyla desteklenmemesi durumunda bu risklerin artabileceği belirtilmektedir (Viljoen vd., 2024).

Veri gizliliği ve düzenleyici uyum da önemli tehdit alanları arasında yer almaktadır. Kişisel verilerin korunması, bilgi güvenliği ve kurumsal uyum gereksinimleri açısından değerlendirildiğinde kontrolsüz süreç geliştirme faaliyetleri organizasyonlar için ciddi riskler oluşturabilmektedir (Weill & Ross, 2004).

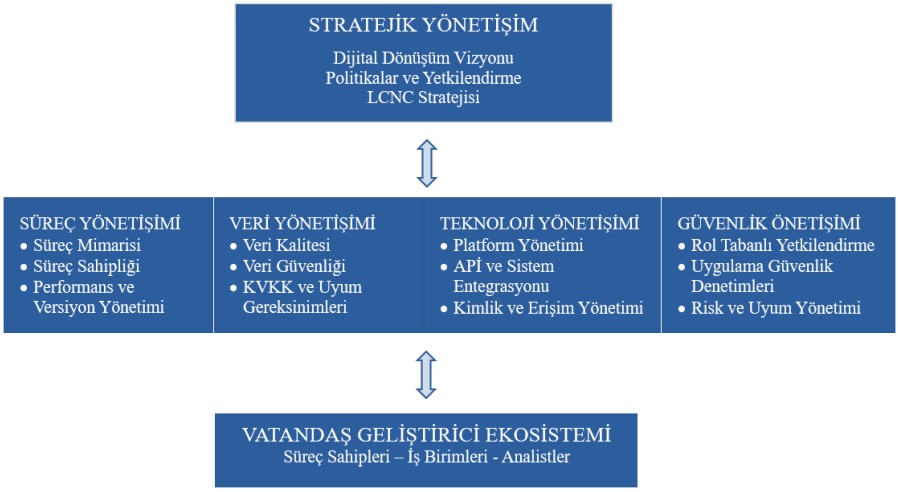
4.4. SWOT Bulgularının Stratejik Değerlendirmesi

SWOT analizi sonuçları, LCNC platformlarının iş süreçlerinin dijital dönüşümünde önemli fırsatlar sunduğunu göstermektedir. Ancak bu fırsatlardan sürdürülebilir biçimde yararlanılabilmesi için güçlü yönlerin fırsatlarla bütünleştirilmesi ve zayıf yönlerin tehditlere dönüşmesini engelleyecek mekanizmaların oluşturulması gerekmektedir.

Özellikle süreç çevikliği, kullanıcı katılımı ve hızlı geliştirme gibi güçlü yönler; yapay zeka destekli süreç geliştirme, süreç madenciliği ve hiperotomasyon gibi yeni teknolojik fırsatlarla birleştirildiğinde organizasyonların dijital dönüşüm kapasitesini önemli ölçüde artırabilir. Buna karşılık teknik borç, platform bağımlılığı ve entegrasyon sorunları gibi zayıf yönler; güvenlik açıkları, veri gizliliği riskleri ve Gölge BT oluşumu gibi tehditlerle birleştiğinde organizasyonel risk düzeyini artırabilmektedir.

Bu nedenle LCNC platformlarının kurumsal ortamlarda başarılı biçimde uygulanabilmesi yalnızca teknolojik yeteneklere değil; aynı zamanda etkin yönetişim mekanizmalarına, açık rol tanımlarına ve sürdürülebilir kontrol süreçlerine bağlıdır. SWOT analizinin ortaya koyduğu bu bulgular doğrultusunda, LCNC ekosistemleri için önerilen bütünleşik yönetişim modeli Şekil 4.1'de sunulmuştur.

Şekil 4.1. LCNC Ekosistemleri için Önerilen Bütünleşik Yönetişim Modeli



Şekil 4.1, LCNC ekosistemlerinde sürdürülebilir dijital dönüşümün sağlanabilmesi için önerilen bütünleşik yönetişim modelini göstermektedir. Model, vatandaş geliştirici yaklaşımının yaygınlaştığı organizasyonlarda süreç geliştirme faaliyetlerinin yalnızca teknolojik bir konu olarak değil, aynı zamanda yönetsel ve organizasyonel bir konu olarak ele alınması gerektiği varsayımına dayanmaktadır.

Modelin temelinde vatandaş geliştirici ekosistemi yer almaktadır. Süreç sahipleri, iş birimleri ve analistler, iş süreçlerine ilişkin bilgi ve deneyimleri doğrultusunda süreç geliştirme faaliyetlerinin doğrudan yürütücüsü konumundadır. LCNC platformlarının sunduğu görsel geliştirme araçları sayesinde bu kullanıcılar süreç tasarlayabilmekte, iş akışları oluşturabilmekte ve süreç iyileştirme faaliyetlerine aktif olarak katılabilmektedir.

Vatandaş geliştirici ekosisteminin etkin ve kontrollü biçimde çalışabilmesi dört yönetişim katmanı tarafından desteklenmektedir. Süreç yönetişimi, geliştirilen uygulamaların kurumsal süreç mimarisi ile uyumunu ve süreç performansının izlenmesini sağlamaktadır. Veri yönetişimi, veri kalitesinin korunması, veri sahipliğinin belirlenmesi ve düzenleyici gereksinimlere uyumun sağlanmasına odaklanmaktadır. Teknoloji yönetişimi, platform yönetimi, sistem entegrasyonları ve erişim altyapısının sürdürülebilir biçimde işletilmesini amaçlamaktadır. Güvenlik yönetişimi ise rol tabanlı yetkilendirme, uygulama güvenliği, risk yönetimi ve denetim faaliyetleri aracılığıyla LCNC ekosisteminin güvenliğini desteklemektedir.

Modelin en üst katmanında yer alan stratejik yönetişim, diğer tüm yönetişim alanlarını kurumsal hedefler doğrultusunda bütünleştiren çatı yapı olarak tasarlanmıştır. Dijital dönüşüm vizyonu, LCNC kullanım politikaları ve yetkilendirme mekanizmaları bu katman aracılığıyla belirlenmektedir. Böylece organizasyonlar bir yandan vatandaş geliştirici yaklaşımının sağladığı çeviklikten yararlanırken diğer yandan süreçlerin kontrolsüz biçimde yaygınlaşmasından kaynaklanabilecek güvenlik, uyum ve sürdürülebilirlik risklerini yönetebilmektedir.

Şekilde kullanılan çift yönlü ilişki, yönetişim mekanizmaları ile vatandaş geliştirici ekosistemi arasındaki karşılıklı etkileşimi ifade etmektedir. Stratejiler, politikalar ve standartlar üst katmanlardan aşağıya doğru aktarılırken; süreç ihtiyaçları, kullanıcı geri bildirimleri ve yenilik önerileri aşağıdan yukarıya doğru taşınmaktadır. Bu nedenle model, geleneksel merkezi BT kontrolü ile dağıtık vatandaş geliştirici yaklaşımı arasında denge kurmayı amaçlayan bütünleşik bir LCNC yönetişim çerçevesi olarak değerlendirilebilir.

5. LCNC Ortamlarında Yönetişim ve Gelecek Perspektifi

SWOT analizinde ortaya konulan bulgular, LCNC platformların organizasyonlara önemli fırsatlar sunduğunu, ancak bu fırsatların sürdürülebilir biçimde değerlendirilebilmesi için uygun yönetişim mekanizmalarına ihtiyaç duyulduğunu göstermektedir. Süreç geliştirme faaliyetlerinin organizasyon genelinde yayılması, geleneksel bilgi teknolojileri yönetimi anlayışının yeniden değerlendirilmesini gerektirmektedir. Özellikle vatandaş geliştirici yaklaşımının yaygınlaşması, süreç sahipliği, veri yönetimi, güvenlik ve standartlaşma gibi konuların daha kritik hale gelmesine neden olmaktadır (Binzer vd., 2024; Viljoen vd., 2024).

Geleneksel BT yönetişimi yaklaşımları büyük ölçüde merkezi bilgi teknolojileri departmanlarının kontrolü üzerine kurulmuştur (Weill & Ross, 2004). Ancak LCNC platformları süreç geliştirme faaliyetlerini daha dağıtık yapılara taşıdığından, yönetişim mekanizmalarının yalnızca teknik kontrol boyutuna odaklanması yeterli olmamaktadır. LCNC ekosistemlerinin başarılı olabilmesi için teknoloji yönetişimi, süreç yönetişimi ve veri yönetişiminin bütünleşik biçimde ele alınması gerektiği literatürde vurgulanmaktadır. (Binzer vd., 2024; Rokis & Kirikova, 2023).

5.1. LCNC Ortamları İçin Bütünleşik Yönetişim Yaklaşımı

LCNC ekosistemlerinde yönetişimin temel amacı, organizasyonel çevikliği korurken süreç geliştirme faaliyetlerinin kurumsal hedefler, güvenlik

gereksinimleri ve standartlarla uyumlu biçimde yürütülmesini sağlamaktır. Bu doğrultuda dört temel yönetişim alanı öne çıkmaktadır:

5.1.1. Stratejik Yönetişim

Stratejik yönetişim, LCNC kullanımının kurumsal hedefler ve dijital dönüşüm stratejileriyle uyumlu biçimde yürütülmesini ifade etmektedir. Bu kapsamda organizasyonların hangi süreçlerde LCNC kullanımına izin verileceğini, vatandaş geliştiricilerin yetki sınırlarını ve bilgi teknolojileri birimlerinin rollerini açık biçimde tanımlaması gerekmektedir (Weill & Ross, 2004).

5.1.2. Süreç Yönetişimi

Süreç yönetişimi, geliştirilen uygulamaların kurumsal süreç mimarisiyle uyumunu sağlamayı amaçlamaktadır. Süreç sahiplerinin belirlenmesi, süreç yaşam döngüsünün yönetilmesi, versiyon kontrolü ve süreç performansının izlenmesi bu kapsamda değerlendirilmektedir (Dumas vd., 2018). Özellikle farklı iş birimleri tarafından geliştirilen süreçlerin bütünleşik bir yapıda yönetilmesi süreç karmaşıklığının azaltılmasına katkı sağlayabilmektedir.

5.1.3. Veri Yönetişimi

LCNC platformlarının yaygınlaşmasıyla birlikte veri yönetimi daha kritik hale gelmektedir. Veri standartlarının oluşturulması, erişim yetkilendirmelerinin belirlenmesi, veri kalitesinin izlenmesi ve kişisel verilerin korunmasına yönelik mekanizmaların oluşturulması veri yönetişiminin temel unsurlarını oluşturmaktadır (Käss vd., 2023).

5.1.4. Teknoloji Yönetişimi

Teknoloji yönetişimi, LCNC platformlarının kurumsal sistemlerle entegrasyonu, güvenlik politikalarının uygulanması ve uygulama yaşam döngüsünün yönetilmesini kapsamaktadır. Özellikle API yönetimi, kimlik doğrulama mekanizmaları ve erişim kontrol sistemleri bu katmanda kritik öneme sahiptir (Rokis & Kirikova, 2023).

Bu dört bileşenin birlikte ele alınması, LCNC ekosistemlerinde çeviklik ve kontrol arasında sürdürülebilir bir denge kurulmasına katkı sağlayabilir.

5.2. Gelecek Perspektifi

LCNC platformlarının gelişimi, yalnızca süreç otomasyonu ile sınırlı kalmayıp daha akıllı ve veri odaklı süreç yönetimi yaklaşımlarına doğru ilerlemektedir. Özellikle yapay zeka teknolojilerinin LCNC platformlarına

entegrasyonu, gelecekte süreç geliştirme faaliyetlerinin niteliğini önemli ölçüde değiştirebilir. Üretken yapay zeka destekli sistemler sayesinde kullanıcıların doğal dil kullanarak süreç tasarlayabilmesi ve uygulama geliştirebilmesi mümkün hale gelmektedir (Desmond vd., 2022).

Bir diğer önemli gelişme alanı süreç madenciliği ile LCNC platformlarının bütünleşmesidir. Süreç madenciliği uygulamaları, süreçlerin gerçek çalışma biçimlerini analiz ederek iyileştirme fırsatlarının belirlenmesine katkı sağlamaktadır. Bu teknolojilerin LCNC platformlarıyla birlikte kullanılması, veri temelli süreç geliştirme anlayışını güçlendirebilir (Berti vd., 2024).

Hiperotomasyon yaklaşımı da LCNC ekosistemlerinin geleceğini şekillendiren önemli eğilimlerden biridir. Robotik süreç otomasyonu, yapay zeka, süreç madenciliği ve LCNC platformlarının birlikte kullanılmasıyla süreçlerin uçtan uca otomatikleştirilmesi mümkün hale gelmektedir. Bu yaklaşımın özellikle finans, sağlık, insan kaynakları ve kamu yönetimi gibi alanlarda yaygınlaşması beklenmektedir.

Bununla birlikte gelecekteki araştırmaların yalnızca teknolojik yeteneklere odaklanması yeterli olmayacaktır. Vatandaş geliştirici olgunluk düzeylerinin ölçülmesi, LCNC yönetişim modellerinin etkinliğinin değerlendirilmesi, süreç performansı üzerindeki etkilerin incelenmesi ve yapay zeka destekli süreç geliştirme ortamlarının organizasyonel sonuçlarının araştırılması önemli çalışma alanları olarak görünmektedir (Binzer vd., 2024; Viljoen vd., 2024).

Sonuç olarak LCNC platformlarının geleceği, teknolojik gelişmeler kadar bu teknolojilerin organizasyonel yapılar içerisinde nasıl yönetileceği ile de yakından ilişkilidir. Bu nedenle sürdürülebilir dijital dönüşümün sağlanabilmesi için çeviklik ile kontrol arasında dengeli bir yönetişim yaklaşımının benimsenmesi kritik önem taşımaktadır.

Kaynaklar

Acitelli, G., Agostinelli, S., Casciani, A., & Marrella, A. (2024). The role of trust in AI-augmented business process management systems. In K. Gdowska, M. T. Gómez-López, & J.-R. Rehse (Eds.), *Business Process Management Workshops: BPM 2024 International Workshops, Krakow, Poland, September 1–6, 2024, Revised Selected Papers* (pp. 5–17). Springer.

Ajiboye, K.J. (2021). The role of Low-Code/No-Code platforms in accelerating digital transformation in regulated industries. *International Journal of Science and Research Archive, 4*(1), 262-279. https://doi.org/10.30574/ijsra.2021.4.1.0159

Ajimati, M. O., Carroll, N. & Maher, M. (2025). Adoption of low-code and no-code development: A systematic literature review and future research agenda, *Journal of Systems and Software, 222*, 112300, https://doi.org/10.1016/j.jss.2024.112300.

Beerepoot, I., Di Ciccio, C., Reijers, H.A., Rinderle-Ma, S., Bandara, W., Burattin, A., Calvanese, D., Chen, T., Cohen, I., Depaire, B., et al. (2023). The biggest business process management problems to solve before we die. *Computers in Industry, 146,* Article 103837. https://doi.org/10.1016/j.compind.2022.103837

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. *Communications of the ACM, 52*(2), 124–129. https://doi.org/10.1145/1461928.1461960

Berti, A., Maatallah, M., Jessen, U., Sroka, M., & Ghannouchi, S. A. (2024). *Re-thinking process mining in the AI-based agents era.* (arXiv Preprint No. arXiv:2408.07720). arXiv. https://arxiv.org/abs/2408.07720

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A. & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*(2), 471–482. http://www.jstor.org/stable/43825919

Binzer, B., Elshan, E., Fürstenau, D. & Winkler, T. J. (2024). Establishing a low-code/no-code-enabled citizen development strategy. *MIS Quarterly Executive, 23*(3), 253–273. https://doi.org/10.17705/2msqe.00097

Czvetkó, T., Kummer, A., Ruppert, T. & Abonyi, J. (2022). Data-driven business process management-based development of Industry 4.0 solutions, *CIRP Journal of Manufacturing Science and Technology, 36*, 117-132, https://doi.org/10.1016/j.cirpj.2021.12.002.

Çelik, C. (2025). İş süreçleri geliştirme platformlarında karşılaştırmalı yaklaşımlar: teknoloji, analiz ve sektörel bir değerlendirme. *Sinop Üniversitesi Fen Bilimleri Dergisi, 10*(2), 530-548. https://doi.org/10.33484/sinopfbd.1658033

Davenport, T.H. (2023). MISQE insight: On the inevitability of citizen development, in: *MIS Quarterly Executive, 22*(4). https://aisel.aisnet.org/misqe/vol22/iss4/3

Desmond, M., Duesterwald, E., Isahagian, V., & Muthusamy, V. (2022). A no-code low-code paradigm for authoring business automations using natural language. Proceedings of the VLDB Endowment. https://doi.org/10.48550/arXiv.2207.10648

Dumas, M., La Rosa, M., Mendling, J. & Reijers, H. A. (2018). *Fundamentals of business process management* (2nd ed.). Springer. https://doi.org/10.1007/978-3-662-56509-4

France, R., & Rumpe, B. (2007). Model-driven development of complex software: A research roadmap. In *Future of Software Engineering (FOSE'07)*, (pp. 37–54), IEEE. https://doi.org/10.1109/FOSE.2007.14

Gök, B. (2026). An examination of employee perceptions in digital transformation in terms of demographic variables. *OPUS Journal of Society Research, 23*(2026), 1-20. https://doi.org/10.26466/opusjsr.1846996

Gürel, E., & Tat, M. (2017). SWOT analysis: A theoretical review. *The Journal of International Social Research, 10*(51), 994–1006. http://dx.doi.org/10.17719/jisr.2017.1832

Käss, S., Strahringer, S., & Westner, M. (2023). Practitioners' perceptions on the adoption of low-code development platforms. *IEEE Access, 11*, 29009–29034. https://doi.org/10.1109/ACCESS.2023.3258539

Kirchhof, J. C., Jansen, N., Rumpe, B., & Wortmann, A. (2023). Navigating the low-code landscape: A comparison of development platforms. In *2023 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)* (pp. 854–862). IEEE. https://doi.org/10.1109/MODELS-C59198.2023.00135

Lamanna, A. (2025). *A structured evaluation framework for low-code platform selection: a multi-criteria decision model for enterprise digital transformation*. (arXiv Preprint No. arXiv:2510.18590). arXiv. https://doi.org/10.48550/arXiv.2510.18590

Mendling, J., Pentland, B. T. & Recker, J. (2020). Building a complementary agenda for business process management and digital innovation. *European Journal of Information Systems, 29*(3), 208–219. https://doi.org/10.1080/0960085X.2020.1755207

Muhammad, S., Prybutok, V. R., Sinha, V. (2024). Citizen developers: The new accelerators for digital transformation. *Muma Business Review, 8*, 173–180. https://doi.org/10.28945/5426

Özan, M. (2021). Süreç yönetimi ve süreç iyileştirmenin işletme performansına etkilerinin analizi. *İşletme Araştırmaları Dergisi, 13*(2), 1144–1161. https://doi.org/10.20491/isarder.2021.1189

Özveri, O. & Kabak, M. (2016). Süreç yönetimi olgunluk modelleri ve bir organizasyonun ve süreç yönetimi olgunluğunun değerlendirilmesi. *Afyon Ko-*

catepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 18(1). https://izlik.org/JA54UD24AR

Özdem, H., & Bora, M. P. (2022). Türkiye'de robotik süreç otomasyonu. *Bilgisayar Bilimleri ve Teknolojileri Dergisi, 3*(1), 1-9. https://doi.org/10.54047/bibted.1008340

Rokis, K., & Kirikova, M. (2023). Exploring low-code development: A comprehensive literature review. *Complex Systems Informatics and Modeling Quarterly, 36*, 68–86. https://doi.org/10.7250/csimq.2023-36.04

Sahay, A., Indamutsa, A., Di Ruscio, D., & Pierantonio, A. (2020). Supporting the understanding and comparison of low-code development platforms. In *2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)* (pp. 171-178). IEEE. https://doi.org/10.1109/SEAA51224.2020.00036

Sanchis, R., García-Perales, Ó., Fraile, F. & Poler, R. (2020). Low-Code as enabler of digital transformation in manufacturing industry. *Applied Sciences, 10*(1), Article 12. https://doi.org/10.3390/app10010012

Sebetci, Ö., Günay, M. B. & Sebetci, E. (2018). İş süreç yönetimi (bpm) ve iş akış yönetimi (wfm) kavramlarına yaklaşım. *AJIT-e: Academic Journal of Information Technology, 9*(33), 115-126. https://doi.org/10.5824/1309-1581.2018.3.007.x

Serekov, D., Bissembayev, A., Iliev, T., Mukasheva, A., & Kang, J. W. (2025). Evaluating low-code development platforms: A MULTIMOORA approach. *Engineering Proceedings, 104*(1), 15. https://doi.org/10.3390/engproc2025104015

Şahinaslan, E. (2023). İş süreci optimizasyonu: Yöntem, teknoloji, riskler ve fırsatlar. *Akademik İzdüşüm Dergisi, 8*(2), 570-604. https://izlik.org/JA46WE72DK

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research, 122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Viljoen, A., Radić, M., Hein, A., Nguyen, J., & Krcmar, H. (2024). Governing citizen development to address low-code platform challenges. *MIS Quarterly Executive, 23*(3), 305–324. https://aisel.aisnet.org/misqe/vol23/iss3/6

Waszkowski, R. (2019). Low-code platform for automating business processes in manufacturing. *IEAC - PapersOnLine, 52*(10), 376–381. https://doi.org/10.1016/j.ifacol.2019.10.060

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Yönetim Bilişim Sistemleri Alanında Yenilikçi Çözümler ve Güncel Yaklaşımlar – IV

Editör:
Doç. Dr. Vahid SİNAP

ÖZGÜR YAYINLARI