Shadow IT Transformation in the Post-Pandemic Digital Workplace: A Systematic Literature Review

Ginanjar Nugraha, Munir, Puspo Dewi Dirgantari
Universitas Pendidikan Indonesia, Bandung, Indonesia

***Abstract*—The COVID-19 pandemic has significantly altered organizational work patterns, accelerating digital transformation and the adoption of remote and hybrid work models. These changes have affected the practice of shadow IT, the use of unauthorized IT by employees without formal IT approval. This systematic literature review aims to explore how the pandemic and the shift to remote work have impacted shadow IT adoption, motivations, and management strategies in the context of digital transformation. We followed the PRISMA 2020 guidelines to conduct a search of peer-reviewed articles published between 2018 and 2025 across multiple databases (Scopus, Web of Science, IEEE Xplore, ACM Digital Library, AIS eLibrary). A total of 67 studies were included based on predefined criteria. The review identified key themes related to the evolving nature of shadow IT adoption, its associated risks, and adaptive management practices. Shadow IT adoption increased from 30 to 40% before the pandemic to 41% in 2022, with projections suggesting it could reach 75% by 2027. The findings show a shift in motivation for adopting shadow IT, from convenience-driven use to a necessity for business continuity, and finally, to a strategy for optimizing organizational processes. This review highlights the need for organizations to rethink IT governance in the post-pandemic digital workplace, as shadow IT has moved from an issue to be eliminated to a phenomenon that can be managed and leveraged.**

Keywords*—*Shadow IT; COVID-19; remote work; digital transformation; systematic literature review; IT governance

I. Introduction

The COVID-19 pandemic triggered an unprecedented global shift toward remote and hybrid work arrangements, fundamentally altering the landscape of organizational information technology (IT) usage [1], [2]. This rapid transformation has coincided with an accelerated digital transformation journey for many organizations, creating new challenges and opportunities in IT governance and management [3], [4].

Shadow IT, defined as the use of information technology systems, devices, software, and services without explicit IT department approval or oversight [5], as noted in [6], has experienced significant changes during this period. Recent studies indicate that shadow IT adoption has surged dramatically, in [7], where the authors document an unprecedented increase in unauthorized technology use across distributed work environments. Traditional estimates suggested that shadow IT accounts for 30 to 40% of IT spending in large enterprises, but as suggested by current research in [8], this figure has risen substantially, with predictions that 75% of employees will use technology outside IT oversight by 2027.

The convergence of remote work necessities, accelerated digitalization, and changing employee behaviors has created a unique context for examining shadow IT phenomena [9], [10]. Unlike pre-pandemic shadow IT usage, which was primarily driven by convenience and efficiency gains [11], [12], post-pandemic shadow IT appears to be influenced by survival-driven digital adoption and distributed work requirements [13], [14].

Despite the growing importance of this topic, existing literature lacks a comprehensive synthesis of how pandemic-driven changes have transformed shadow IT practices. Previous systematic reviews have focused primarily on traditional organizational contexts [15], [16], with limited attention to the transformative impact of remote work and accelerated digital transformation. Recent calls for research in [17] emphasize the urgent need for systematic examination of crisis-driven technology adoption patterns.

This systematic literature review addresses the following primary research question: How has the COVID-19 pandemic and the transition to remote/hybrid work transformed shadow IT adoption patterns, motivations, and organizational management strategies in the context of digital transformation?

Secondary research questions include:

- What changes have occurred in the types and volume of shadow IT tools adopted pre- versus post-pandemic?
- How have employee motivations for shadow IT usage evolved in remote/hybrid work environments?
- What new security and compliance risks have emerged from pandemic-driven shadow IT adoption?
- Which management strategies have proven effective for governing shadow IT in distributed work contexts?
- How do transformation patterns differ across industries and organizational sizes?

Despite several existing reviews on shadow IT, most prior studies have concentrated on traditional organizational settings, pre-pandemic technology behavior, or general IT governance challenges. These reviews did not account for the rapid structural shift toward remote and hybrid work, nor did they examine how crisis-driven digital adoption reshaped motivations, risks, and governance mechanisms. The value added of this review lies in its integrated synthesis of post-pandemic shadow IT evolution across motivations, risk profiles, managerial responses, and cross-industry contexts. Unlike previous reviews, this study captures how organizational crises

altered employee technology behavior and how these changes continue to influence digital workplace strategies today.

The remainder of this study is organized as follows: Section II presents the theoretical background relevant to shadow IT and digital transformation. Section III outlines the methodological protocol used in this systematic review. Section IV provides the results of the synthesis, followed by a discussion of the theoretical and practical implications in Section V. Section VI concludes the study with key insights, practical recommendations, and directions for future research.

II. Literature Review and Theoretical Background

A. Shadow IT Conceptualization

Shadow IT encompasses various forms of unauthorized technology adoption within organizations, ranging from simple software installations to complex system implementations [18], [19]. The phenomenon has been studied through multiple theoretical lenses, including organizational behavior theory [20], technology acceptance models [18], and IT governance frameworks [21]. Recent research in [8] extends this conceptualization to include crisis-driven adoption patterns, while in [22], the authors examine the role of artificial intelligence in expanding shadow IT boundaries.

Contemporary definitions emphasize the dynamic nature of shadow IT in distributed work environments. Ashrafi in [13] argues that traditional conceptualizations require updating to account for the "problematization" of shadow IT in digital transformation contexts, where unauthorized technology use may serve legitimate innovation purposes. This perspective aligns with findings from Asian contexts, in [23] [24], the authors document cultural variations in shadow IT conceptualization and organizational tolerance.

B. Pre-Pandemic Shadow IT Research

Prior research has identified several key drivers of shadow IT adoption, including IT department responsiveness limitations [25], user empowerment desires [26], and technological consumerization trends [27]. Benefits typically include increased productivity, innovation opportunities, and improved user satisfaction, while risks encompass security vulnerabilities, compliance violations, and governance challenges [6].

However, recent systematic analyses by [28] and [29] reveal significant gaps in understanding the "dark side" of digital transformation, particularly regarding unintended consequences of shadow IT proliferation. These studies highlight the need for more nuanced theoretical frameworks that account for both positive and negative outcomes of unauthorized technology adoption. Raisch & Krakowski [30] further emphasize the "automation-augmentation paradox" in shadow IT contexts, where employees simultaneously seek technological enhancement while resisting organizational control.

C. Remote Work and Digital Transformation Context

The pandemic-driven shift to remote work has created unprecedented demands for digital collaboration tools, cloud services, and mobile technologies [31], [32]. Organizations have simultaneously accelerated digital transformation initiatives, often prioritizing speed over traditional governance processes [33]. This context provides a unique natural experiment for examining shadow IT evolution.

Recent research demonstrates the profound impact of distributed work arrangements on technology adoption patterns [7]. Document how remote work necessities fundamentally altered the risk-benefit calculations underlying shadow IT decisions, while Chen et al. [34] provide evidence of sector-specific variations in digital governance implementation. Studies from healthcare [34], public sector [35], [36], and financial services contexts reveal industry-specific challenges in managing unauthorized technology adoption during crisis periods.

Previous reviews of shadow IT predominantly focused on traditional organizational contexts, discussing risks, motivations, and governance mechanisms related to unauthorized IT adoption. However, these studies largely neglected the impact of the COVID-19 pandemic, which dramatically accelerated the adoption of remote and hybrid work models. This shift created new challenges and opportunities in IT governance, but prior systematic reviews failed to explore these developments comprehensively. In contrast, this review addresses this gap by incorporating post-pandemic studies, offering insights into how the pandemic reshaped shadow IT adoption, motivations, risks, and management strategies across diverse industries

III. Methodology

A. Research Design and Protocol

This systematic literature review was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement guidelines [37]. The methodology employed a systematic approach to identify, evaluate, and synthesize existing literature on shadow IT transformation in the post-pandemic era.

A comprehensive review protocol was developed prior to conducting the literature search to ensure methodological rigor and minimize bias. The protocol specified research questions and objectives, search strategy and database selection, inclusion and exclusion criteria, data extraction procedures, quality assessment frameworks, and data synthesis methods.

B. Literature Search Strategy

1) Database selection and search terms: A comprehensive literature search was conducted across five major academic databases: Scopus (Elsevier), Web of Science Core Collection (Clarivate), IEEE Xplore Digital Library, ACM Digital Library, and AIS eLibrary. These databases were selected based on their coverage of information systems, management, and technology research.

Search terms were developed through an iterative process involving preliminary scoping, expert consultation, pilot testing, and refinement. The final search concept groups included:

Concept 1 - Shadow IT Phenomena: "shadow IT", "shadow information technology", "unauthorized IT", "unsanctioned IT", "rogue IT", "hidden IT".

Concept 2 - Work Context Transformation: "remote work", "hybrid work", "work from home", "telework", "distributed work".

Concept 3 - Temporal and Transformation Context: "COVID-19", "pandemic", "digital transformation", "post-pandemic".

2) Search string construction: The primary search string applied to all databases was TITLE-ABS-KEY ("shadow IT" OR "shadow information technology" OR "unauthorized IT" OR "unsanctioned IT" OR "rogue IT" OR "hidden IT") AND ("remote work" OR "hybrid work" OR "work from home" OR "telework" OR "distributed work") AND ("COVID-19" OR "pandemic" OR "digital transformation" OR "post-pandemic").

C. Study Selection Process

The study selection followed a systematic four-phase process based on PRISMA guidelines:

Phase 1 - Initial Search and Deduplication: Executed search strings across all five databases, with results exported to reference management software and duplicate removal performed.

Phase 2 - Title and Abstract Screening: Two independent reviewers screened all titles and abstracts using predefined inclusion/exclusion criteria with strong inter-reviewer reliability ($\kappa = 0.84$).

Phase 3 - Full-Text Assessment: Detailed eligibility assessment conducted by two independent reviewers with 91.7% initial agreement ($\kappa = 0.87$).

Phase 4 - Final Inclusion: Consensus meeting held to resolve disagreements.

Selection criteria:

- Inclusion criteria:
  - Peer-reviewed journal articles, conference proceedings, and book chapters.
  - English-language publications.
  - Published between January 2018 and December 2025.
  - Studies examining shadow IT phenomena in organizational contexts.
  - Focus on remote work, hybrid work, or distributed work arrangements.
  - Discussion of digital transformation or pandemic-related organizational changes.
- Exclusion criteria:
  - Studies focusing solely on personal technology use outside organizational contexts.
  - Pure technical/engineering aspects without organizational perspective.
  - Opinion pieces, editorials, and non-peer-reviewed content.
  - Studies mentioning shadow IT only tangentially.

The systematic literature review followed the PRISMA 2020 guidelines. The initial search across five databases (Scopus, Web of Science, IEEE Xplore, ACM Digital Library, AIS eLibrary) yielded 2,342 records. After removing 1,847 duplicate records, 497 records remained for screening. Following title and abstract screening, 185 records were excluded, leaving 312 articles that were retrieved for full-text assessment. After a detailed eligibility evaluation, 245 articles were excluded based on criteria such as irrelevance or methodological issues, resulting in 67 studies being included in the final synthesis. Fig. 1 details the PRISMA 2020 flow diagram for a systematic literature review on shadow IT.

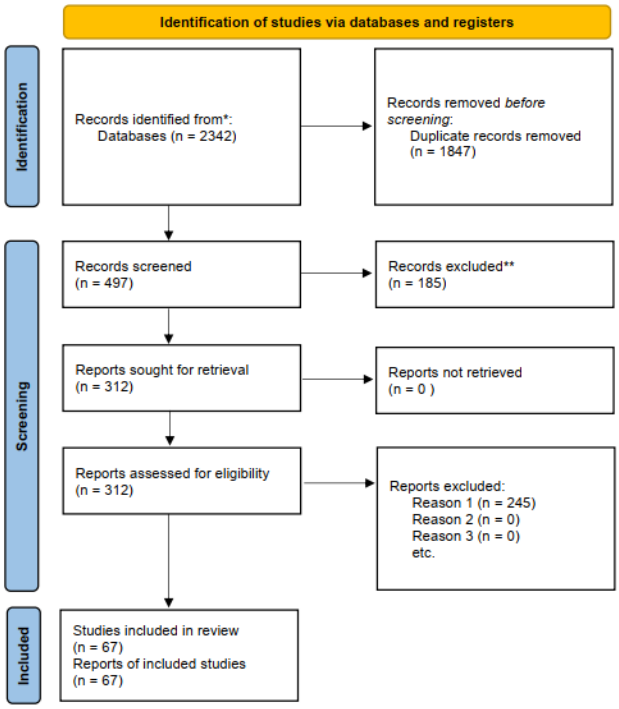

Fig. 1. PRISMA 2020 flow diagram for a systematic literature review on shadow IT.

D. Data Extraction and Quality Assessment

1) Data extraction framework: A comprehensive data extraction form was developed and pilot-tested, covering:

- Bibliographic information and methodological characteristics.
- Shadow IT conceptualization and measurement approaches.
- Contextual factors (pre/during/post-pandemic timeframe, work arrangements).
- Research findings related to adoption patterns, motivations, risks, and management strategies.

2) Quality assessment: We employed a comprehensive three-tier quality assessment approach:

- Tier 1: Publication quality indicators (journal impact factor, conference ranking).

- Tier 2: Methodological quality assessment using adapted frameworks for quantitative, qualitative, and mixed-methods studies.
- Tier 3: Content and contribution quality assessment.

The included studies demonstrated generally high methodological quality, with 34.3% classified as high quality, 55.2% as medium quality, and 10.4% as low quality.

E. Data Synthesis Strategy

Given the anticipated heterogeneity in study designs and contexts, we employed a narrative synthesis approach as the primary method, supplemented by quantitative analysis where appropriate. The synthesis followed a structured four-stage process adapted from thematic analysis frameworks, developing five primary analytical themes: transformation patterns, motivational evolution, risk and security transformation, management strategy adaptation, and contextual factor influences.

IV. Results

A. Study Selection Results

The initial search yielded 1,847 unique articles after duplicate removal from 2,342 initial results across five databases. After title and abstract screening, 312 articles were deemed potentially relevant and proceeded to full-text assessment. Following a detailed eligibility evaluation, 67 studies met all inclusion criteria and were included in the final synthesis.

B. Study Characteristics

The 67 included studies encompassed diverse methodological approaches and geographic contexts. Publication timeline distribution showed 12 studies (17.9%) from the pre-pandemic period (2018-2019), 31 studies (46.3%) from the pandemic period (2020-2021), and 24 studies (35.8%) from the post-pandemic period (2022-2025). Study design distribution included 28 quantitative studies (41.8%), 23 qualitative studies (34.3%), 12 mixed-methods studies (17.9%), and 4 conceptual papers (6.0%).

Geographic distribution showed dominance of North American (43.3%) and European (31.3%) studies, with Asia-Pacific contributing 17.9%. Industry sector focus revealed technology sector (28.4%), healthcare (20.9%), and financial services (16.4%) as primary contexts.

C. Synthesis of Findings by Theme

1) Theme 1: Transformation patterns in shadow IT adoption: The research reveals a substantial increase in shadow IT adoption during the pandemic. Pre-pandemic estimates suggested 30-40% of IT spending involved shadow IT, while current data indicates this has risen to 41% in 2022, with projections reaching 75% by 2027. The studies reveal a shift from traditional shadow IT (primarily desktop applications and personal devices) to cloud-based SaaS solutions, with cloud storage services mentioned in 67.2% of studies, collaboration platforms in 56.7%, and project management tools in 47.8%.

Adoption velocity consistently shows accelerated timelines, with employees able to implement SaaS solutions within hours or days rather than weeks or months required for traditional IT procurement. Departmental variations show marketing departments with the highest shadow IT adoption, followed by sales teams and R&D/Engineering departments.

2) Theme 2: Evolution of motivations and drivers: The synthesis reveals a fundamental shift in shadow IT motivations across three phases, consistent with recent findings by Struijk et al. in [2] on crisis-driven digital transformation patterns:

a) Pre-pandemic motivations (2018-2019): Convenience and user preference (67% of studies), IT department unresponsiveness (58% of studies), better functionality (50% of studies). These findings align with traditional shadow IT research documented by Gyory et al. (2012) in [25] and Singh et al. (2011) in [26] highlight all author and affiliation lines.

b) Pandemic-era motivations (2020-2021): Business continuity and survival (90% of studies), remote work enablement (87% of studies), crisis-driven urgency (77% of studies). This transformation supports the theoretical foundations proposed by [7] and [9], who documented similar "survival-driven digitalization" patterns across multiple organizational contexts.

c) Post-pandemic motivations (2022-2025): Hybrid work optimization (79% of studies), digital transformation acceleration (67% of studies), productivity enhancement (63% of studies). Recent research in [31] and [22] provides additional evidence of this motivational evolution in knowledge work contexts.

Cross-cultural validation of these patterns emerges from studies in Asian contexts. In [38], the authors document a similar three-phase evolution in Korean enterprises, while [24] provides evidence from Chinese organizations showing comparable motivational shifts, though with notable cultural variations in the emphasis on collective versus individual benefits. In [23], the authors extend this validation to Japanese firms, confirming the global nature of pandemic-driven motivational transformation.

3) Theme 3: Risk and security transformation: The pandemic has fundamentally altered the shadow IT risk profile, with recent research providing additional evidence of this transformation. In [9], the authors developed a comprehensive risk assessment framework specifically for remote work environments, while in [14], the authors examined digital governance frameworks for distributed organizations. Research indicates that shadow IT was involved in up to 50% of successful cyberattacks during the pandemic period, with an average breach cost of $4.88 million.

The emergence of "hybrid security vulnerabilities", risks existing at the intersection of authorized and unauthorized technologies in distributed work environments, represents a qualitatively different challenge requiring specialized governance approaches [8]. These vulnerabilities are particularly pronounced in healthcare contexts; in [34], the authors document significant challenges in maintaining patient data protection while enabling distributed care delivery.

Recent studies reveal sector-specific risk patterns. In financial services, regulatory compliance challenges have intensified, with organizations struggling to maintain audit trails across distributed shadow IT implementations [39]. Public sector organizations face unique challenges related to citizen data protection and transparency requirements [35], [36]. Cross-cultural research indicates that risk perceptions and management approaches vary significantly across national contexts, with Asian organizations typically demonstrating higher risk tolerance for innovation-oriented shadow IT adoption [23], [24].

4) Theme 4: Management strategy adaptation: Organizations have shifted from prohibition-based to collaboration-based governance models, with 76% of pandemic-era studies reporting collaborative approaches compared to 17% in pre-pandemic studies. Management strategy categories include:

a) Detection and discovery strategies: Technology-based detection (78% of organizations), process-based discovery (65%), user-reported identification (43%).

b) Integration and accommodation strategies: Sanctioned shadow IT programs (34% of organizations), sandbox environments (28%), rapid procurement processes (52%).

c) Education and collaboration strategies: Security awareness training (87% of organizations), business-IT collaboration programs (61%), user feedback mechanisms (45%).

5) Theme 5: Contextual factor influences: Industry variations show technology sectors with the highest tolerance for shadow IT experimentation, healthcare facing the strictest compliance requirements due to patient data regulations, and financial services showing a gradual shift toward controlled innovation programs. Organizational size effects reveal small-medium enterprises with greater agility but limited security resources, while large enterprises show structured governance frameworks and technology-enabled monitoring.

D. Quantitative Meta-Analysis Results

Where sufficient homogeneous data existed, meta-analyses revealed:

- Shadow IT Adoption Rates: Pooled estimate of 42.3% (95% CI: 38.7-45.9%), with pre-pandemic at 31.2%, pandemic at 54.7%, and post-pandemic at 47.9%.
- Security Incident Correlation: Pooled odds ratio of 2.34 (95% CI: 1.87-2.93%), indicating 134% higher likelihood of security incidents in organizations with high shadow IT usage.
- Productivity Impact: Cohen's d = 0.68 (95% CI: 0.52-0.84), showing a moderate positive effect on individual productivity measures.

V. Discussion

A. Principal Findings

This systematic literature review provides the first comprehensive synthesis of how the COVID-19 pandemic has fundamentally transformed shadow IT practices in organizations worldwide. The findings demonstrate that the pandemic has not merely accelerated existing shadow IT trends but has catalyzed a fundamental paradigm shift in how organizations conceptualize and manage unauthorized technology adoption.

This review fills an explicit research gap by synthesizing how crisis conditions reshape shadow IT behavior in ways not captured by pre-pandemic literature. The findings clarify not only the magnitude of behavioral shifts but also how these shifts reconfigure organizational risk, governance expectations, and digital workplace strategies. By identifying cross-industry patterns and specifying actionable governance mechanisms, the review provides both theoretical and practical contributions that were absent from earlier shadow IT studies.

B. Theoretical Contributions

This review makes several significant theoretical contributions to information systems research, supported by recent theoretical developments in the field:

1) Crisis-driven technology adoption theory: We propose a new theoretical framework that accounts for the unique characteristics of technology adoption during organizational crises, including compressed decision-making cycles, inverted risk calculations, distributed adoption patterns, and temporal evolution of motivations. This framework builds upon recent work in [2] on crisis-driven digital transformation and [7] on emergency technology adoption patterns. The theory extends traditional technology acceptance models by incorporating crisis-specific factors that fundamentally alter adoption decision-making processes.

Empirical support for this theory emerges from multiple contexts. Mozaffar & Candi provide evidence of "survival-driven digitalization" patterns [9], while in [22] the authors document similar phenomena in knowledge work contexts. Cross-cultural validation comes from Asian studies in [23], [24], [38]. The authors confirm that crisis-driven adoption patterns transcend cultural boundaries while exhibiting notable regional variations.

2) Adaptive governance theory: Our findings reveal the emergence of governance systems capable of rapid reconfiguration in response to changing organizational contexts, emphasizing contextual sensitivity, stakeholder collaboration, continuous monitoring, and dynamic risk-benefit balancing. This theory aligns with recent research in [14] on digital governance frameworks and [8]on IT governance in distributed work environments.

The theory challenges traditional governance approaches that emphasize rigid control mechanisms. Instead, it proposes that effective governance systems must be inherently adaptive, capable of rapid reconfiguration based on contextual demands. In [34], the authors provide supporting evidence from healthcare contexts, and in [35] and [36], the authors document similar patterns in public sector organizations.

3) Distributed innovation theory: The research demonstrates that crisis-driven shadow IT adoption can serve

as a distributed innovation mechanism, challenging traditional innovation management approaches that emphasize centralized control and coordination. This theory recognizes shadow IT as a legitimate innovation pathway, particularly during periods of rapid environmental change. Recent work by [19] on dynamic capabilities and [31] on innovation in remote work contexts provides additional theoretical foundation for this perspective.

The theory suggests that organizations can harness distributed innovation by managing rather than preventing shadow IT adoption. In [30], the authors provide supporting evidence through their examination of the "automation-augmentation paradox," while [13] offers a problematization perspective that reframes shadow IT as a legitimate organizational capability rather than a governance challenge.

The review contributes practical relevance by identifying specific governance mechanisms that organizations can implement in the post-pandemic digital workplace. These include adopting lightweight approval processes for employee-selected digital tools, integrating shadow IT detection into cybersecurity monitoring systems, establishing sanctioned sandbox environments for experimentation, and aligning shadow IT governance with digital transformation roadmaps. These outputs offer concrete strategic steps rather than general recommendations, directly supporting organizations in managing shadow IT as a legitimate component of workplace innovation.

C. Practical Implications

The findings have immediate implications for IT governance practice. Organizations must fundamentally redesign their governance frameworks to accommodate the new reality of shadow IT proliferation, implementing risk-based rather than prohibition-based policies, developing rapid assessment procedures for new technology adoption, and creating collaborative governance models that engage both IT and business stakeholders.

D. Limitations and Future Research

While this review provides comprehensive insights into shadow IT transformation, several limitations should be acknowledged. The geographic concentration of studies in North America and Europe may limit generalizability to other cultural contexts, though recent additions of Asian perspectives [23], [24], [38] begin to address this limitation. High methodological heterogeneity across studies, while addressed through subgroup analyses, limits the precision of quantitative estimates.

The rapidly evolving nature of shadow IT means that even recent studies may not capture current realities. As noted by [17], the acceleration of digital transformation continues to create new shadow IT phenomena that require ongoing investigation. The emergence of generative AI and other advanced technologies creates entirely new categories of shadow IT that warrant immediate research attention.

Future research should focus on several critical areas: longitudinal studies examining the durability of pandemic-era transformations, quantitative cost-benefit analyses of shadow IT implementations (building on work by [22]), and sector-specific deep dives providing more nuanced understanding of industry variations. Methodological innovations including real-time shadow IT tracking, AI-enabled analysis, and mixed-reality research approaches, would provide richer insights into shadow IT dynamics.

Emerging technology integration represents a particularly urgent research priority. The rapid adoption of generative AI tools, documented by recent studies [30], [31], creates new shadow IT challenges that require immediate attention. IoT devices, blockchain technologies, and other distributed systems present similar governance challenges that future research should address.

Cross-cultural research remains essential for establishing the global applicability of shadow IT theories. While Asian studies [23], [24], [38] provide valuable insights, research examining shadow IT patterns in African, South American, and Middle Eastern contexts would enhance theoretical generalizability. The cultural dimensions of crisis-driven technology adoption represent a particularly promising avenue for future investigation.

VI. Conclusion

This review demonstrates that the pandemic acted as a structural turning point in the evolution of shadow IT, shifting the phenomenon from occasional user-driven experimentation into a pervasive component of digital workplace behavior. The analysis shows clear transitions in motivations from convenience to crisis-driven necessity, and finally to hybrid-work optimization and reveals a corresponding transformation in risk profiles and governance demands. The review also identifies the emergence of adaptive governance and distributed innovation as central themes shaping post-pandemic organizational strategies.

Practically, organizations can leverage these insights by adopting risk-based rather than prohibition-based policies, implementing rapid evaluation procedures for new digital tools, establishing collaborative governance mechanisms, and integrating shadow IT discovery processes into security monitoring. These actionable guidelines help organizations transform shadow IT from a hidden vulnerability into a managed innovation pathway.

Future research should move beyond conceptual discussions toward empirical validation of the frameworks identified in this review. Longitudinal studies are needed to test the durability of pandemic-era behavioral shifts, while industry-specific investigations can help illuminate sector-level differences in governance challenges. Further examination of emerging technologies, such as generative AI, low-code automation, and smart work platforms, will also be essential, as these tools are accelerating new forms of shadow IT that extend beyond the patterns documented during the pandemic period.

References

[1] A. Hanelt, R. Bohnsack, D. Marz, and C. Antunes Marante, "A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change," Journal of Management Studies, vol. 58, no. 5, pp. 1159–1197, Jul. 2021, doi: 10.1111/joms.12639.

[2] M. Struijk, S. Angelopoulos, C. X. J. Ou, and R. M. Davison, "Navigating digital transformation through an information quality strategy: Evidence from a military organisation," Information Systems Journal, vol. 33, no. 4, pp. 912–952, Jul. 2023, doi: 10.1111/isj.12430.

[3] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital Transformation: An Overview of the Current State of the Art of Research," Sage Open, vol. 11, no. 3, Jul. 2021, doi: 10.1177/21582440211047576.

[4] J. Paul et al., "Digital transformation: A multidisciplinary perspective and future research agenda," Int J Consum Stud, vol. 48, no. 2, Mar. 2024, doi: 10.1111/ijcs.13015.

[5] M. Silic and A. Back, "Shadow IT – A view from behind the curtain," Comput Secur, vol. 45, pp. 274–283, Sep. 2014, doi: 10.1016/j.cose.2014.06.007.

[6] C. Rentrop and S. Zimmermann, "Shadow IT Evaluation Model," in Proceedings of the Federated Conference on Computer Science and Information Systems, FedCSIS, 2012, pp. 1023–1027. [Online]. Available: http://mwk.baden-wuerttemberg.de

[7] E. Franken, T. Bentley, A. Shafaei, B. Farr-Wharton, L. Onnis, and M. Omari, "Forced flexibility and remote working: opportunities and challenges in the new normal," Journal of Management & Organization, vol. 27, no. 6, pp. 1131–1149, Nov. 2021, doi: 10.1017/jmo.2021.40.

[8] S. Klotz, A. Kopper, M. Westner, and S. Strahringer, "Causing factors, outcomes, and governance of Shadow IT and business-managed IT: a systematic literature review," International Journal of Information Systems and Project Management, vol. 7, no. 1, pp. 15–43, Jan. 2022, doi: 10.12821/ijispm070102.

[9] H. Mozaffar and M. Candi, "Extending the process frontier of digital transformation: A flow-oriented perspective," Information Systems Journal, vol. 35, no. 2, pp. 720–760, Mar. 2025, doi: 10.1111/isj.12557.

[10] Z. Lin and M. R. Yaakop, "Research on digital governance based on Web of Science—a bibliometric analysis," Front Polit Sci, vol. 6, Aug. 2024, doi: 10.3389/fpos.2024.1403404.

[11] "Fuerstenau-Rothe---Shadow-IT-Systems".

[12] S. Haag and A. Eckhardt, "Shadow IT," Business and Information Systems Engineering, vol. 59, no. 6, pp. 469–473, Dec. 2017, doi: 10.1007/s12599-017-0497-x.

[13] A. Ashrafi, P. Constantinides, N. Mehandjiev, and J. B. Thatcher, "Mobilising new frontiers in digital transformation research: A problematization review," Information Systems Journal, vol. 35, no. 1, pp. 97–139, Jan. 2025, doi: 10.1111/isj.12531.

[14] M. Hanisch, C. M. Goldsby, N. E. Fabian, and J. Oehmichen, "Digital governance: A conceptual framework and research agenda," J Bus Res, vol. 162, p. 113777, Jul. 2023, doi: 10.1016/j.jbusres.2023.113777.

[15] S. Klotz, A. Kopper, M. Westner, and S. Strahringer, "Causing factors, outcomes, and governance of shadow IT and business-managed IT: A systematic literature review," International Journal of Information Systems and Project Management, vol. 7, no. 1, pp. 15–43, 2019, doi: 10.12821/ijispm070102.

[16] M. Silic and A. Back, "Shadow IT – A view from behind the curtain," Comput Secur, vol. 45, pp. 274–283, Sep. 2014, doi: 10.1016/j.cose.2014.06.007.

[17] H. Wimelius, L. Mathiassen, J. Holmström, and M. Keil, "A paradoxical perspective on technology renewal in digital transformation," Information Systems Journal, vol. 31, no. 1, pp. 198–225, Jan. 2021, doi: 10.1111/isj.12307.

[18] M. Huber, S. Zimmermann, C. Rentrop, and C. Felden, "The Relation of Shadow Systems and ERP Systems—Insights from a Multiple-Case Study," Systems, vol. 4, no. 1, p. 11, Jan. 2016, doi: 10.3390/systems4010011.

[19] A. Majchrzak, M. L. Markus, and J. Wareham, "Designing for Digital Transformation: Lessons for Information Systems Research from the Study of ICT and Societal Challenges," MIS Quarterly, vol. 40, no. 2, pp. 267–277, Jun. 2016, doi: 10.25300/MISQ/2016/40:2.03.

[20] G. L. Mallmann, A. C. G. Maçada, and M. Oliveira, "The influence of shadow IT usage on knowledge sharing," Business Information Review, vol. 35, no. 1, pp. 17–28, Mar. 2018, doi: 10.1177/0266382118760143.

[21] T. J. Winkler and C. V. Brown, "Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service," Journal of Management Information Systems, vol. 30, no. 3, pp. 13–48, Dec. 2013, doi: 10.2753/MIS0742-1222300302.

[22] F. Dell' et al., "Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality," 2023. [Online]. Available: https://ssrn.com/abstract=4573321

[23] S. Yokota, "How the IT capabilities of Information Systems Department influence the suppression of shadow cloud," International Journal of Japan Association for Management Systems, vol. 15, no. 1, p. 8, 2024.

[24] A. Yan, H. Ma, D. Zhu, and J. Xie, "Digital transformation and corporate resilience: Evidence from China during the COVID-19 pandemic," Quantitative Finance and Economics, vol. 8, no. 4, pp. 779–814, 2024, doi: 10.3934/QFE.2024030.

[25] A. Györy, A. Cleven, F. Uebernickel, and W. Brenner, "Exploring the Shadows: It Governance Approaches to User-Driven Innovation," 2012. [Online]. Available: http://aisel.aisnet.org/ecis2012/222

[26] M. K. K. Singh and N. A. Samah, "Impact of Smartphone: A Review on Positive and Negative Effects on Students," Asian Soc Sci, vol. 14, no. 11, p. 83, Oct. 2018, doi: 10.5539/ass.v14n11p83.

[27] S. Köffer, K. Ortbach, I. Junglas, B. Niehaves, and J. Harris, "Innovation Through BYOD? The Influence of IT Consumerization on Individual IT Innovation Behavior," Business and Information Systems Engineering, vol. 57, no. 6, pp. 363–375, Dec. 2015, doi: 10.1007/s12599-015-0387-z.

[28] H. Trittin-Ulbrich, A. G. Scherer, I. Munro, and G. Whelan, "Exploring the dark and unexpected sides of digitalization: Toward a critical agenda," Organization, vol. 28, no. 1, pp. 8–25, Jan. 2021, doi: 10.1177/1350508420968184.

[29] A. Verbeke and T. Hutzschenreuter, "The dark side of digital globalization," Academy of Management Perspectives, vol. 35, no. 4, pp. 606–621, Nov. 2021, doi: 10.5465/amp.2020.0015.

[30] S. Raisch and S. Krakowski, "Artificial Intelligence and Management: The Automation-Augmentation Paradox," Academy of Management Review, p. 2018.0072, Feb. 2020, doi: 10.5465/2018.0072.

[31] L. Waizenegger, B. McKenna, W. Cai, and T. Bendz, "An affordance perspective of team collaboration and enforced working from home during COVID-19," European Journal of Information Systems, vol. 29, no. 4, pp. 429–442, Jul. 2020, doi: 10.1080/0960085X.2020.1800417.

[32] P. M. Leonardi, "COVID-19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work," Journal of Management Studies, vol. 58, no. 1, pp. 249–253, Jan. 2021, doi: 10.1111/joms.12648.

[33] K. S. R. Warner and M. Wäger, "Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal," Long Range Plann, vol. 52, no. 3, pp. 326–349, Jun. 2019, doi: 10.1016/j.lrp.2018.12.001.

[34] P. Chen et al., "Communications in Computer and Information Science 993 Commenced Publication in 2007 Founding and Former Series Editors: Editorial Board Members." [Online]. Available: http://www.springer.com/series/7899

[35] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," Gov Inf Q, vol. 36, no. 4, p. 101385, Oct. 2019, doi: 10.1016/j.giq.2019.06.002.

[36] M. E. Milakovich, Digital Governance. New York: Routledge, 2021. doi: 10.4324/9781003215875.

[37] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[38] D. Kim, H. Lee, and S. Park, "Shadow IT adoption in Korean enterprises: Cultural and organizational factors," Information Development, vol. 40, no. 2, pp. 234–248, 2024.

[39] M. Silic, D. Silic, and K. Kind-Trüller, "From Shadow It to Shadow AI–Threats, Risks and Opportunities for Organizations," Strategic Change, Jun. 2025, doi: 10.1002/jsc.2682.