Received: June 5, 2026
Revised: July 17, 2026
Accepted: July 23, 2026
Published: August 27, 2026

Elicit Journal of Economics and Management Studies
eISSN: 3121-634X
pISSN: 3093-0529

https://elicitpublisher.com

REVIEW PAPER

Digital Transformation and the Rise of Shadow IT: Implications for Organisational Complexity and Cyber Governance

Zakaria Alrababah[1]

Affiliations
[1]Naseem International School, Bahrain

ORCID Identifiers

Zakaria Alrababah
0000

DOI

10.65820/ejems-2vol2-issue2-2026

Abstract

Purpose: This study examines how digital transformation contributes to the emergence of Shadow IT and Shadow AI, synthesising evidence on the factors driving unauthorised technology adoption, its implications for organisational complexity and cyber governance, and the governance strategies proposed to address these challenges.

Methods: A systematic literature review was conducted in accordance with the PRISMA guidelines, synthesising evidence from 25 peer-reviewed studies across diverse organisational and industrial contexts. The evidence was synthesised through thematic analysis to identify recurring patterns relating to the conceptualisation of Shadow IT, adoption drivers, organisational consequences, cyber governance risks, and organisational responses. The findings were interpreted using the Technology–Organisation–Environment (TOE) framework and Diffusion of Innovation (DOI) theory.

Results: The review found that digital transformation, combined with restrictive governance processes, unmet operational needs, and the widespread availability of cloud computing and generative AI, encourages the adoption of unauthorised technologies. Shadow IT increases organisational complexity by creating fragmented technology infrastructures, data silos, duplicated information, and reduced accountability. These conditions weaken cyber governance through reduced visibility, data security vulnerabilities, compliance risks, and challenges associated with autonomous AI systems.

Novelty and Contribution: The study develops an integrated conceptual framework that explains how digital transformation drives Shadow IT adoption, links unauthorised technology use to organisational complexity and cyber governance risks, and identifies governance mechanisms that balance innovation, security, and compliance

Social and Practical Implications: The findings support the development of governance practices that improve collaboration between business units and IT departments while strengthening cybersecurity, regulatory compliance, and responsible use of digital and AI technologies in contemporary organisations.

Keywords: Digital transformation; Shadow IT; Shadow AI; Cyber governance; Organisational complexity

*Corresponding author

E-mail address: zakakariah16@nisbah.com

How to cite this article:

Zakaria, A. (2026). Digital Transformation and the Rise of Shadow IT: Implications for Organisational Complexity and Cyber Governance. *Elicit Journal of Economics and Management Studies*, *2*(2), 26-45. https://doi.org/10.65820/ejems-2vol2-issue2-2026

1 Introduction

Digital transformation involves the integration of advanced digital technologies into all operational and strategic facets of an organisation (Sebastian, 2026). This process alters product development, service delivery, and internal workflows, fundamentally changing how business units collaborate, allocate resources, and execute decisions (Küçükoğlu & Kabakuş, 2025). Historically, centralised information technology departments managed software procurement, infrastructure deployment, and data governance (Shunmugasundaram et al., 2026). The widespread transition to cloud computing, software-as-a-service platforms, and mobile architectures has permanently altered this distribution of control (Orthi et al., 2023).

Remote and hybrid work arrangements have further individualised data processing and software adoption (Castellano et al., 2022). Workers routinely use third-party collaboration applications, cloud storage systems, and messaging platforms to execute their daily tasks (Scalabrin Bianchi et al., 2022). These technologies are frequently adopted without the formal approval or knowledge of the organisation's central IT department (Shunmugasundaram et al., 2026). The use of non-sanctioned/third-party software enables business units to bypass official procurement channels entirely, favouring tools that offer immediate utility over those mandated by corporate policy (Kopper et al., 2020). Consequently, Shadow IT, defined as the unauthorised deployment, management, and use of software, hardware, or digital services (Haag & Eckhardt, 2024), has emerged as a pervasive and unintended consequence of digital transformation (Shunmugasundaram et al., 2026).

Organisations implement digital transformation strategies to increase operational agility, accelerate market responsiveness, and enhance overall flexibility (Zhao et al., 2025). Paradoxically, the pursuit of these necessary business objectives creates conditions that encourage the adoption of unauthorised technologies (Shunmugasundaram et al., 2026). Centralised IT governance frameworks frequently rely on rigid, time-consuming approval processes that conflict with the immediate functional requirements of business units (Silic et al., 2025). When official enterprise systems prove inflexible, highly complex, or slow to adapt, employees turn to Shadow IT as a practical workaround to maintain productivity and achieve departmental goals (Furstenau et al., 2017). The normalisation of self-service business analytics and user-led deployment further entrenches this behaviour across corporate structures (Castellano et al., 2022).

While such workarounds yield immediate, localised productivity gains (Haag & Eckhardt, 2024), the proliferation of unvetted systems introduces severe organisational complexity (Shunmugasundaram et al., 2026). Decentralised technology adoption fragments the enterprise architecture, leading to isolated data silos, redundant applications, and inconsistent workflow integrations (Devasthali & Gupta, 2024). Departments rely on hidden networks of applications that remain entirely invisible to central management. This structural fragmentation impedes enterprise-wide standardisation, limits resource optimisation, and complicates future technological upgrades (Fürstenau et al., 2021).

More critically, the unchecked expansion of Shadow IT weakens established cyber governance frameworks (Silic et al., 2025). Unsanctioned applications routinely evade security audits, access management controls, and compliance protocols (Klotz et al., 2019). This operational opacity exposes organisations to substantial cybersecurity threats, including data exfiltration, malware infections, and breaches of stringent regulatory requirements such as the General Data Protection Regulation (Haag & Eckhardt, 2024). Non-human identities, opaque decision-making processes, and invisible automation associated with emerging Shadow AI systems further exacerbate these vulnerabilities (Shunmugasundaram et al., 2026; Silic et al., 2025). Traditional IT governance models, designed for static, centrally controlled environments, prove highly inadequate for managing the probabilistic risks posed by decentralised technology adoption (Saeed et al., 2023).

While existing scholarship extensively documents the technical vulnerabilities, ethical principles, and regulatory compliance requirements associated with unapproved technologies, substantial gaps remain regarding the behavioural and organisational mechanisms driving decentralised adoption (Sebastian, 2026; Shunmugasundaram et al., 2026). Current research predominantly evaluates traditional Shadow IT through rigid governance frameworks, frequently neglecting the specific implications of autonomous systems operating with high concealability and non-human identities (Waters-Lynch et al., 2025).

This systematic review synthesises current literature examining the relationship between digital transformation initiatives and the corresponding proliferation of Shadow IT. The analysis identifies the specific mechanisms through which unauthorised technology adoption increases organisational complexity, particularly regarding fragmented data

architectures, redundant resource allocation, and decentralised operational control. The review evaluates the implications for cyber governance, detailing the security vulnerabilities, data privacy concerns, and compliance failures associated with unsanctioned systems.

Furthermore, the study critically analyses the governance responses proposed within the academic and practitioner literature. The synthesis assesses strategies designed to reconcile the tension between maintaining strict cybersecurity controls and enabling the technological autonomy required for business unit innovation. The scope of this review encompasses literature situated at the intersection of organisational and management studies, information systems research, cybersecurity, and technology governance. The analysis integrates both empirical investigations and conceptual frameworks to capture the complex sociotechnical nature of unauthorised technology use. Evidence is drawn from a broad spectrum of industry contexts, including manufacturing, financial services and healthcare. Including studies from multiple sectors ensures the findings reflect diverse organisational realities and varying regulatory pressures.

The systematic literature review is guided by the following research questions:

1. How has the literature conceptualised Shadow IT in the context of digital transformation?
2. What factors drive Shadow IT adoption?
3. How does Shadow IT increase organisational complexity?
4. What cyber governance risks are associated with Shadow IT?
5. What governance strategies are proposed in the literature?

1.2 Theoretical Background

Theoretical perspectives offer essential foundations for analysing how and why Shadow IT proliferates within digitally transforming organisations. The Technology–Organisation–Environment (TOE) framework provides a multidimensional structure for interpreting the various factors that influence the adoption, implementation, and governance of digital technologies (Xu, 2025). In terms of enterprise digital transformation, this framework delineates three distinct yet interacting dimensions that shape technology use (Zheng et al., 2026). The technological paradigm consists of both internal and external technologies available to a firm, assessing aspects such as existing system infrastructure, technological compatibility, and the accessibility of emerging solutions like cloud computing, low-code platforms, and artificial intelligence (AI) tools (N'Dri & Su, 2024). While the organisational aspect considers internal characteristics, including firm size, formal and informal structural connections, existing IT capabilities, and the degree of management support (Xu, 2025). The environmental aspect addresses external conditions, capturing the influence of competitive pressures, regulatory constraints, market structures, and the broader technological support or vendor ecosystem (N'Dri & Su, 2024).

Complementing the macro-level insights of the TOE framework, the Diffusion of Innovations (DOI) theory explains the behavioural and cognitive mechanisms driving the spread of new technologies among individuals (Mandal & Bag, 2024). In terms of Shadow IT, DOI clarifies why employees and business units autonomously adopt unauthorised tools rather than relying on central IT departments (Thuan et al., 2025). The theory identifies five key attributes influencing adoption rates. Relative advantage assesses the degree to which employees perceive an unapproved tool as superior or more efficient than sanctioned enterprise systems (Thuan et al., 2025). Compatibility measures how well the technology aligns with existing work practices, prior experiences, and operational needs. Complexity concerns the perceived difficulty of operating the tool; simpler, consumer-grade applications typically experience rapid adoption (Panxhi et al., 2025; Thuan et al., 2025). Trialability reflects the extent to which users can test a technology on a limited basis without significant commitment, an attribute closely associated with modern software applications (Fatorachian & Ramesh, 2025). Finally, observability refers to the visibility of the innovation's results, which can encourage informal peer-to-peer diffusion across departments (Thuan et al., 2025).

Together, the TOE framework and DOI theory will serve as the primary theoretical lenses for interpreting the findings of this systematic review, offering a comprehensive basis for explaining the emergence, adoption, and complex cyber governance implications of Shadow IT.

2 Methodology

2.1 Review Design

To generate a rigorous and current synthesis of scholarship on digital transformation, Shadow IT, and cyber governance, this study adopted a systematic literature review (SLR) design. An SLR provides a structured, transparent, and reproducible method for locating, appraising, and consolidating existing research on a defined subject (Akinson et al., 2025; Lebona et al., 2025). Given its established suitability for organising review procedures of this kind, the PRISMA 2020 guidelines were followed throughout the review process (Page et al., 2021).

2.2 Sources of Evidence

Two major bibliographic databases, Scopus and Web of Science, were chosen to retrieve the literature underpinning this review. This combination was selected because the two platforms jointly span an extensive cross-section of peer-reviewed, high-quality scholarship across disciplines. Scopus was chosen for its wide-ranging disciplinary indexing, while Web of Science was included for its more selective citation coverage, which helps mitigate gaps and reduce bias that might arise from relying on a single index (Falcão & Roseira, 2022).

2.3 Search Strategy

Search terms were developed around the review's core constructs, namely digital transformation, Shadow IT, Shadow AI, unauthorised technology use, cyber governance, and organisational complexity. These terms were linked using Boolean logic to maximise retrieval accuracy while keeping the scope aligned with the study's aims. The combination of the keywords and Boolean operators includes;

"digital transformation" AND "shadow IT"

"Shadow IT" AND governance

"Shadow IT" AND cybersecurity

"Digital transformation" AND "organisational complexity"

"unauthorized technology adoption" AND "cyber governance"

Only English-language, peer-reviewed, full-text articles were retrieved. This process yielded 225 records overall, comprising 131 from Scopus and 94 from Web of Science.

2.4 Eligibility Parameters

Records were evaluated against the following criteria for inclusion:

i. Published between 2016 and 2026, capturing a ten-year window of relevant scholarship
ii. Written in English
iii. Published in peer-reviewed journals
iv. Either empirical or conceptual in nature
v. Substantively related to digital transformation, Shadow IT, Shadow AI, organisational complexity, or cyber governance

Conversely, records were removed from consideration if they were duplicate entries, originated from non-academic outlets, or addressed subject matter unconnected to the review's focus.

2.5 Selection Process

The selection process unfolded across sequential filtering stages. Of the 225 records initially retrieved, 36 duplicate entries were removed, leaving 189 records for title-and-abstract screening. This stage eliminated a further 78 records that did not satisfy the eligibility parameters, resulting in 111 records carried forward for full-text assessment. During full-text review, 35 items were removed for being review papers, books, or conference proceedings rather than peer-reviewed journal articles, and a further 51 were excluded because their findings fell outside the substantive scope of

this review. This left a final sample of 25 articles, which formed the basis of the synthesis reported in this study. Two reviewers carried out the screening independently at each stage, with any disagreement settled through joint discussion until agreement was reached. Figure 1 shows the full PRISMA flow diagram.

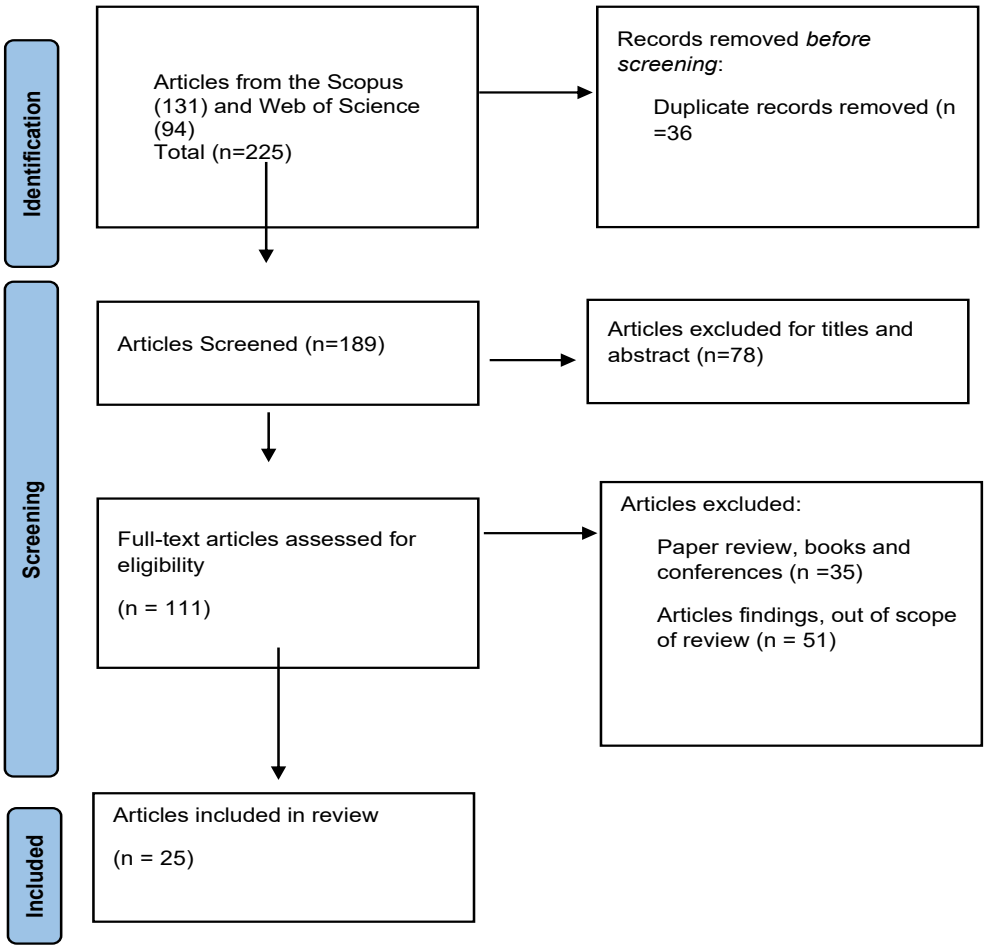

Figure 1 PRISMA flow diagram

2.6 Coding and Synthesis Procedure

The included articles were analysed using a staged, thematic coding approach. Evidence from each study was first mapped against the review's guiding questions to build a framework for interpretation. Passages addressing Shadow IT drivers, sources of organisational complexity, cyber governance vulnerabilities, and governance responses were then extracted, condensed, and sorted according to shared meaning and relevance, allowing recurring patterns to surface across the dataset. These codes were subsequently consolidated into broader themes, which were iteratively refined through comparison across sources before being integrated into the conceptual model presented later in this paper (Section 3.3).

2.7 Assessment of Study Quality

Rather than applying a standardised appraisal instrument, the quality of the included studies was judged manually by two reviewers working independently. Each reviewer considered the soundness of the methodological approach, the clarity with which findings were reported, and the degree of relevance to the review's aims. Any differences in judgement between reviewers were reconciled through discussion rather than through formal scoring.

3 Results

3.1 Descriptive characteristics of the studies

A total of 25 articles (Table 1) met the inclusion criteria and were included in the review. The studies examined issues related to shadow IT, shadow AI, governance, cybersecurity, digital transformation, and technology adoption across different organisational and industrial settings.

Publication Trends by Year

The publication pattern indicates growing scholarly interest in the topic over time (Figure 2). Only one study was published in 2017, followed by two studies in 2019, three in 2020, one in 2021, two in 2022, two in 2023, four each in 2024 and 2025, and six in 2026. The increasing number of publications from 2024 onwards suggests rising attention to governance challenges associated with emerging digital technologies, particularly shadow AI and cybersecurity risks.

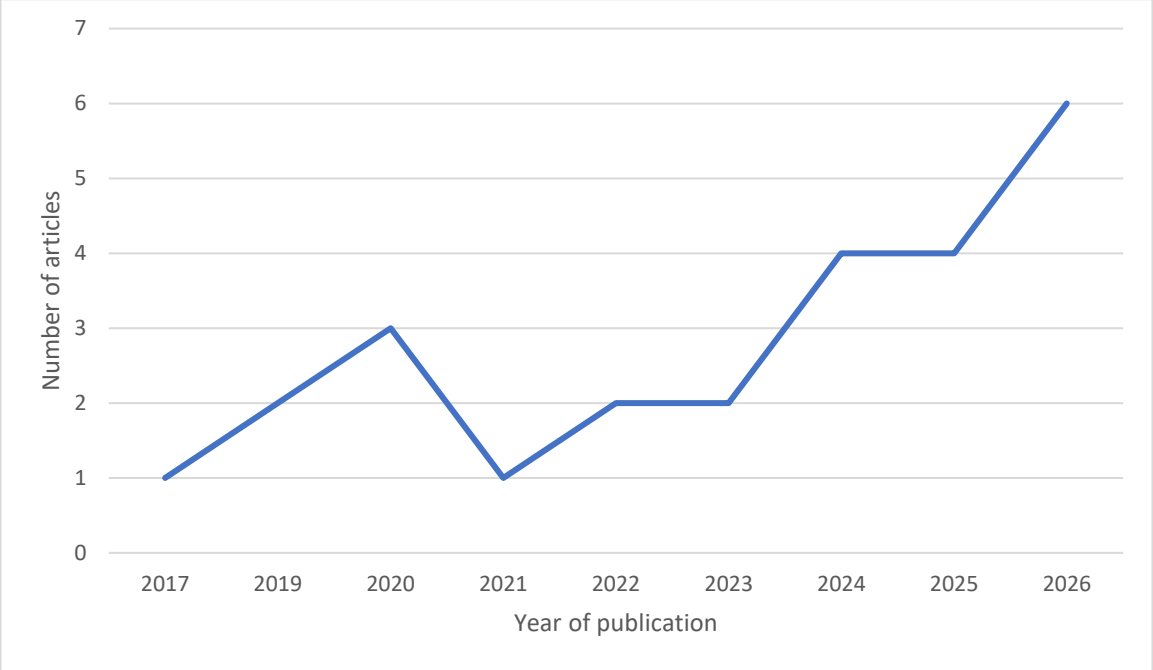

Figure 2 Distribution of articles by year of publication

Geographical Distribution

The studies covered a diverse range of geographical contexts. Germany appeared most frequently, either as a standalone setting or in multi-country studies, reflecting strong research activity in shadow IT and governance. Other country-specific studies were conducted in China, Indonesia, India, Australia, Nigeria, the United States, Italy, Austria, Switzerland, and Serbia. Several studies adopted global perspectives or did not specify a geographical focus, indicating the broad relevance of the topic across regions.

Sector Distribution

Research was concentrated in multiple industries: manufacturing, finance, healthcare, information technology, biotechnology, legal services, consumer IoT, and electric vehicle manufacturing. Studies focusing on multiple industries represented the largest category, highlighting the cross-sectoral nature of shadow IT and shadow AI phenomena. Manufacturing and finance were also frequently examined due to their increasing reliance on digital technologies and associated governance challenges.

Table 1 Data extraction table

S/N	Author(s), Year	Country	Sector	Method	Theory	Key Focus	Key Findings
1	Shunmugasundaram et al. (2026)	N/S	Multiple industries	SLR & Conceptual	Agency, Sociotechnical	Shadow AI Governance	Traditional IT governance is inadequate; governance-by-design is required for AI ecosystems.
2	Sebastian (2026)	N/S	Multiple industries	Survey	DART	Shadow AI Risk	Policies and training reduce risks, while efficiency drives AI reliance.
3	Kasmo et al. (2025)	Indonesia	N/S	Qualitative document review	Absorptive Capacity Theory and Actor-Network Theory	Digital Transformation & ESG	Integrating ESG and cybersecurity improves resilience and strategy execution.
4	Rakovic et al. (2020)	Germany, Serbia	Manufacturing	SLR & Case Study	N/S	Shadow IT in ERP	Excel and Access dominate shadow IT, creating recurring risks.
5	Orthi et al. (2023)	N/S	IT	DSR	Cybersecurity Governance Principles	AI-driven cyber threat intelligence	Treating cyber threat intelligence as a managerial resource improves governance alignment.
6	Alfian et al. (2026)	Indonesia	Legal/Digital Communication	Qualitative - normative-juridical approach	N/S	AI & Legal Governance	AI adoption requires stronger legal and data protection frameworks.
7	Abed (2024)	Global	Consumer IoT	SLR	TAM, UTAUT, DOI	IoT Adoption	Usefulness, ease of use, and trust drive IoT adoption.
8	Digalwar et al. (2024)	India	Manufacturing SMEs	Survey	N/S	Industry 4.0 Readiness	SMEs prioritise technology assessment and ROI considerations.

9	Ahmad et al. (2020)	Australia	N/S	Case Study	Organisational Learning	Security Management	Integration of security and response teams improves learning and defence.
10	Haag & Eckhardt (2024)	Global	Multiple Industries	Interviews	N/S	Shadow IT Management	Managing rather than eliminating shadow IT is more effective.
11	Malik (2025)	USA	Finance, Healthcare, Manufacturing	Mixed Methods	N/S	Governance Maturity	Mature governance reduces incidents and improves threat detection.
12	Furstenau et al. (2017)	Germany	Financial Services	Interviews	Sociotechnical	Shadow Systems	Shadow systems reshape power relations and IT-business alignment.
13	Waters-Lynch et al. (2025)	N/S	N/S	Qualitative - Conceptual	Dynamic Capability	Shadow User Innovation	Trust encourages disclosure of covert AI innovations.
14	Castellano et al. (2022)	Germany, Italy	Finance	Experimental Survey	Dynamic Capabilities, Deterrence	Shadow IT Decisions	Cyber-aware executives may still engage in shadow IT.
15	Silic et al. (2025)	Global	Multiple Industries	Mixed Methods	Digital Shadow Risk Theory	Shadow AI Adoption	Employees use AI without governance awareness, increasing risks.
16	Scalabrin Bianchi et al. (2022)	Europe, N. America	IT	SLR & DSR	N/S	Shadow IT Benefits	Controlled integration of shadow IT can support innovation.
17	Klotz et al. (2019)	N/S	Multiple	SLR	N/S	Shadow IT Research	Research focus has shifted from causes to governance.

18	Ogedengbe et al. (2024)	Nigeria	Multiple	Survey, SmartPLS	Strain Theory	Cloud Shadow IT	Work overload and cognitive strain drive unauthorised IT use.
19	Kopper et al. (2020)	Germany, Austria, Switzerland	Multiple	QCA	N/S	Shadow IT Outcomes	Overt IT initiatives perform better than covert shadow systems.
20	Liang et al. (2026)	China	Manufacturing	DSR	Human-Centred AI	AI Use Cases	Shadow IT reveals unmet needs that inspire AI innovation.
21	Chateau-Dégat & Mayrhofer (2026)	Germany	Biotechnology	Case Study	Knowledge-Based View	Acquisitions & Shadow IT	Shadow IT can facilitate post-acquisition integration.
22	Fürstenau et al. (2021)	Germany	Multiple	QCA	Configurational	Shadow IT Governance	Outcomes depend on contextual governance mechanisms.
23	Saeed et al. (2023)	Global	Finance, Healthcare	SLR	N/S	Cybersecurity & DT	Digital transformation creates sector-specific security risks.
24	Sillic (2019)	USA	Multiple Industries	Survey, PLS	Inertia Theory	Non-compliant Behaviour	Cognitive inertia encourages continued shadow IT use.
25	Zhao et al. (2025)	China	EV Manufacturing	fsQCA	TOE	Firm Performance	Performance depends on combined technological and organisational factors.

NOTE: N/S = Not stated, SLR = Systematic literature review, DART = Digital shadow AI risk framework , AI = Artificial intelligence, ESG = Economic, social and governance, ERP = enterprise resource planning, TAM = Technology Adoption Model, UTAUT = Unified Theory of Acceptance and Use of Technology, DOI = Diffusion of Innovation, IoT = Internet of things, IT = Information technology, DSR = Design science research, QCA = Qualitative Comparative Analysis, DT = Digital technology, fsQCA = Fuzzy-set Qualitative Comparative Analysis.

Methodological Distribution

The review identified a diverse methodological profile. Qualitative approaches were the most common, comprising case studies, interviews, conceptual papers, document reviews, and design science research. Quantitative studies primarily employed surveys, experimental surveys, PLS-SEM, QCA, and fsQCA techniques to examine determinants and outcomes of technology use. Mixed-methods designs were less common but were used to investigate governance maturity and shadow AI adoption (Malik, 2025; Sillic, 2019). Several studies also employed systematic literature reviews, either as standalone methods or combined with conceptual and design-oriented approaches.

Theoretical Distribution

Theoretical foundations varied considerably across the studies. Dynamic Capability Theory and sociotechnical perspectives were among the most frequently applied frameworks. Other theories included the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), Diffusion of Innovation (DOI), Organisational Learning Theory, Knowledge-Based View, Strain Theory, Inertia Theory, Technology–Organisation–Environment (TOE) framework, Absorptive Capacity Theory, Actor-Network Theory, Agency Theory, and Deterrence Theory. Several studies did not employ an explicit theoretical framework, reflecting the emerging and practice-oriented nature of research on shadow IT and shadow AI governance.

3.2 Thematic findings

To address the research questions, findings from the included studies were synthesised through thematic analysis. This process involved identifying recurring patterns and concepts in the literature and grouping them into major themes. The thematic structure facilitated the systematic organisation and interpretation of evidence, thereby deepening understanding of the drivers, implications, and governance challenges associated with Shadow IT in the context of digital transformation.

Theme 1: Digital transformation as a driver of Shadow IT

Findings from the literature indicate that digital transformation initiatives frequently fail to align with operational realities, generating structural conditions that drive Shadow IT adoption (Kasmo et al., 2025). As organisations shift towards decentralised and agile operating models, employees face increased pressure to execute tasks quickly and respond to dynamic market demands (Shunmugasundaram et al., 2026). Centralised information technology departments often lack the responsiveness or specific business knowledge required to support these evolving digital workplace demands (Furstenau et al., 2017). Consequently, users experience unmet functional requirements, viewing formal enterprise systems as rigid, complex, or insufficient for their daily workflow (Scalabrin Bianchi et al., 2022). When official IT approval processes and procurement cycles are perceived as too slow, employees frequently bypass formal channels to maintain operational efficiency (Silic et al., 2025).

This behavioural shift is heavily facilitated by the consumerisation of IT. The presence of a high number of mobile devices, Software-as-a-Service (SaaS), and cloud computing provides business units with easily accessible, low-cost alternatives to enterprise systems (Klotz et al., 2019; Silic et al., 2025). The reviewed studies show strong convergence regarding cloud architectures, noting that they lower the technical barriers to entry and enable employees to procure technology without IT department assistance (Waters-Lynch et al., 2025). More recently, researchers have identified an evolution towards AI-enabled workarounds, commonly termed "Shadow AI" (Shunmugasundaram et al., 2026). Employees increasingly integrate generative artificial intelligence, low-code machine learning tools, and autonomous agents into their routines to automate tasks and enhance decision-making (Sebastian, 2026). Unlike traditional Shadow IT, which typically involves static software applications, these AI-driven systems introduce adaptive and semi-autonomous functionalities that execute tasks with minimal human oversight (Shunmugasundaram et al., 2026). The frictionless concealability of browser-based AI services allows users to experiment, iterate, and generate outputs entirely outside of managerial visibility (Waters-Lynch et al., 2025).

While the specific technologies range from simple spreadsheets to complex autonomous agents, the underlying driver remains consistent across the literature. Together, unmet operational demands, restrictive central IT governance, and the accessibility of consumer-grade digital and AI tools create an environment where the continuous expansion of unsanctioned systems becomes an embedded feature of modern organisational practice.

Theme 2: Drivers of Shadow IT adoption

The literature consistently identifies perceived relative advantage and ease of use as primary drivers of Shadow IT adoption (Shunmugasundaram et al., 2026). Employees frequently evaluate unauthorised tools against formal enterprise systems, favouring the former for their user-friendly interfaces, processing speed, and immediate operational benefits (Rakovic et al., 2020). Compatibility with existing work routines further accelerates this adoption. When formal information systems present rigid constraints or demand extensive process adaptations, users turn to shadow solutions that align seamlessly with their specific daily workflows and specialised functional requirements (Rakovic et al., 2020).

Technological characteristics such as trialability and observability strongly influence diffusion patterns within organisations. The capability to quickly test and iterate software or cloud-based applications without formal IT procurement allows employees to validate solutions against immediate operational bottlenecks (Waters-Lynch et al., 2025). Following successful local trials, these solutions often experience informal diffusion across teams. Research highlights a robust social dimension to this spread, where the visibility of peer usage and the informal exchange of functional workarounds create self-sustaining networks of shadow IT practice (Haag & Eckhardt, 2024).

An emerging pattern in the literature points to a paradigm shift driven by AI-enabled workarounds, notably generative AI (Shunmugasundaram et al., 2026). Employees increasingly deploy consumer-grade AI platforms, intelligent assistants, and low-code machine learning tools to automate cognitive tasks and accelerate decision-making outside formal organisational governance (Waters-Lynch et al., 2025). The literature contrasts these AI tools with traditional Shadow IT, noting that modern generative AI combines high task generativity with frictionless concealability (Waters-Lynch et al., 2025). Features such as natural-language malleability, individual adoptability, and minimal technical footprints eliminate traditional implementation barriers. Consequently, knowledge workers can independently construct complex prompt chains or analytical wrappers without peer coordination or IT approval (Waters-Lynch et al., 2025). While earlier iterations of Shadow IT often surfaced through peer visibility and social networks, highly concealable AI tools allow employees to capture individual productivity gains while remaining entirely undetected by formal oversight mechanisms. Table 2 summarises drivers of Shadow IT Adoption.

Table 2 Drivers of Shadow IT Adoption Identified in the Literature

Driver	Description	Example	Source
Unmet functional requirements	Enterprise systems lack required features or flexibility, prompting employees to develop alternative solutions.	Excel spreadsheets, Access databases, custom workflows	Rakovic et al. (2020); Fürstenau et al. (2021)
Task expediency and efficiency	Employees adopt external tools to complete tasks faster and bypass lengthy IT processes.	Generative AI, time-tracking apps, low-code tools	Sebastian (2026); Silic et al. (2025)
Weak business–IT alignment	Limited communication and trust between IT and business units encourage independent technology adoption.	Vendor applications, market data tools, customised CRM workflows	Fürstenau et al. (2021); Haag & Eckhardt (2024)
Work overload and cognitive strain	High workloads and inadequate support drive employees toward familiar unauthorised tools.	WhatsApp, Google Drive, personal email	Ogedengbe et al. (2024)
Easy access and concealability	Cloud and AI technologies are inexpensive, accessible, and difficult to monitor.	ChatGPT, Slack, Dropbox	Waters-Lynch et al. (2025)
Need for agility	Departments require rapid adaptation that centralised IT systems cannot provide.	Trading systems, analytics tools, and board computer systems	Fürstenau et al. (2021); Shunmugasundaram et al. (2026)

IT and procedural inertia	Rigid policies and outdated systems encourage employees to bypass formal channels.	Self-service analytics, macro-enabled spreadsheets	Castellano et al. (2022); Sillic (2019)

Theme 3: Shadow IT and Organisational Complexity

Studies demonstrate that the proliferation of Shadow IT fundamentally increases structural complexity within organisations. As business units independently procure unauthorised applications, cloud services, and artificial intelligence tools, the overarching IT landscape becomes highly fragmented (Devasthali & Gupta, 2024). Studies consistently report that these decentralised technologies operate in functional silos, featuring diverse architectures that exhibit poor interoperability with official enterprise systems. This fragmentation directly diminishes standardisation and impedes the seamless execution of cross-departmental workflows, frequently resulting in a loss of operational synergy (Devasthali & Gupta, 2024; Klotz et al., 2019).

A prominent manifestation of this complexity is the deterioration of enterprise data integrity. The deployment of unsanctioned applications routinely leads to data duplication, as employees manually extract and manage information outside centrally governed databases (Rakovic et al., 2020). Because these shadow systems lack automated synchronisation with core infrastructure, local datasets quickly become outdated, incomplete, or inaccurate (Rakovic et al., 2020). The resulting data inconsistencies generate competing versions of the truth across different departments, which compromises the reliability of analytical reporting and undermines effective decision-making (Klotz et al., 2019). The literature agrees that managing these redundant data architectures requires significant, often unplanned, administrative effort.

The recent integration of generative AI and autonomous software agents into the shadow IT ecosystem further compounds these coordination challenges. Unlike traditional, static software workarounds, modern AI tools introduce adaptive and opaque decision-making processes into routine workflows (Alfian et al., 2026). Researchers observe that this algorithmic opacity severely weakens organisational accountability. When employees independently deploy AI systems, executives struggle to map where these technologies operate, how algorithmic outputs influence business processes, and who holds ownership over the final decisions (Shunmugasundaram et al., 2026). This ambiguity creates substantial management obstacles, particularly when assigning responsibility for operational failures or compliance violations. Furthermore, because these tools are often maintained by single individuals without formal documentation, organisations face severe continuity risks if those key personnel depart (Klotz et al., 2019). Ultimately, the continuous self-procurement of digital tools erodes central oversight, embedding systemic coordination challenges deeply into the organisational structure.

Theme 4: Shadow IT and Cyber Governance Risks

Studies consistently identify reduced visibility as a primary governance risk of unsanctioned systems (Shunmugasundaram et al., 2026). Shadow IT and artificial intelligence create operational blind spots that conceal active data flows and system inventories from centralised IT departments, preventing comprehensive risk assessments (Scalabrin Bianchi et al., 2022).

Unmanaged systems introduce severe access control and identity management challenges. Agentic AI exacerbates this by introducing non-human identities capable of self-authenticating and accessing sensitive databases without human intervention. Traditional cybersecurity architectures fail to govern these autonomous entities, increasing vulnerability to privilege escalation and unauthorised lateral movement (Shunmugasundaram et al., 2026).

Studies emphasise that shadow systems significantly elevate data security risks, including intellectual property loss and prompt injection attacks (Sebastian, 2026; Silic et al., 2025). Employees frequently input confidential information into unauthorised third-party platforms, resulting in unintentional data disclosure (Scalabrin Bianchi et al., 2022). This decentralised adoption of cloud services operates outside formal compliance protocols (Devasthali & Gupta, 2024). Third-party vendors compound these vulnerabilities, as organisations lack visibility into the security protocols of external providers, limiting their ability to enforce consistent data governance (Malik, 2025). Consequently, shadow IT routinely violates data protection regulations, such as the GDPR and data residency requirements, exposing firms to regulatory penalties (Sebastian, 2026).

Furthermore, undocumented systems restrict incident detection and response capabilities. When security breaches occur, the separation between shadow system users and formal incident response teams prevents rapid diagnosis and recovery (Ahmad et al., 2020). Studies identify systemic policy non-compliance driven by conflicts between official IT restrictions and individual task efficiency (Waters-Lynch et al., 2025). Employees justify these actions by citing the rigidity of official IT procedures. While some evidence suggests strict policies deter shadow IT usage, contrasting findings indicate employees often neutralise sanctions by prioritising personal work norms over formal cybersecurity directives (Shunmugasundaram et al., 2026; Waters-Lynch et al., 2025).

The uncontrolled proliferation of Shadow IT compromises enterprise resilience by fracturing accountability, expanding attack surfaces, and rendering centralised cyber governance frameworks ineffective.

Theme 5: Organisational Responses and Governance Strategies

Studies reveal a consensus that traditional, restrictive IT policies are insufficient for managing unauthorised technology adoption within highly interconnected infrastructures (Alfian et al., 2026; Silic et al., 2025). Early organisational responses relied heavily on prohibition and punitive measures, operating under the assumption that centralisation could entirely prevent security breaches (Silic et al., 2025). Evidence indicates that blanket bans often fail to curtail informal technology use and can inadvertently drive such practices deeper underground (Waters-Lynch et al., 2025). While some scholars maintain that stringent enforcement mechanisms are necessary for high-risk applications (Castellano et al., 2022), a growing body of research advocates moving away from reactive suppression. Adaptive cyber governance models focus on controlled enablement, allowing employees to employ specific tools under defined parameters (Haag & Eckhardt, 2024).

Managing organisational complexity requires integrating security operations with broader decision-making frameworks. Several studies propose co-governance or business-managed IT models, where functional departments and central IT units share task responsibilities (Klotz et al., 2019; Orthi et al., 2023). In these structures, central IT provides baseline infrastructure, vendor management, and security standards, while business units retain the flexibility to tailor applications to local requirements (Kopper et al., 2020). To operationalise this shared oversight, organisations implement strategies such as policy-as-code, continuous telemetry monitoring, and secure sandbox environments (Waters-Lynch et al., 2025). Targeted training programmes complement these structural adjustments by aligning employee behaviour with organisational risk appetites (Sebastian, 2026). When informal applications are identified, evaluation processes determine whether the system should be decommissioned, replaced, or formally integrated into the corporate architecture (Fürstenau et al., 2021).

Sustaining operational resilience in digital environments depends on the capacity to negotiate the tension between central control and decentralised agility. Effective management of Shadow IT requires balancing technological innovation, employee autonomy, and governance oversight. Table 3 highlights the strategies prioritised by organisations to tackle Shadow IT.

Table 3 Organisational Responses and Governance Strategies to Shadow IT

Context	Challenge	Response	Outcome	sources
General Enterprise	Hidden AI use	Training and AI sandboxes	Safe innovation	Sebastian (2026)
Multinationals	Strategy–technology misalignment	ESG and cybersecurity integration	Resilience	Kasmo et al. (2025)
Manufacturing	Spreadsheet-based shadow IT	Training and integration	Better governance	Rakovic et al. (2020)
IT Project Management	Cybersecurity silos	AI-driven CTI	Proactive risk management	Orthi et al. (2023)
Multiple Industries	Employee workarounds	Improved UX and incentives	Reduced shadow IT	Haag & Eckhardt (2024)

Cloud Enterprises	Cloud governance failures	Automated governance	Improved compliance	Malik (2025)
Financial Services	Weak IT control	Compliance and oversight	Reduced risk	Furstenau et al. (2017)
Corporate Finance	Executive shadow IT	Accountability measures	Fewer breaches	Castellano et al. (2022)
High-Compliance Sectors	AI governance gaps	AI training and registries	Compliant AI adoption	Silic et al. (2025)

3.3 Conceptual Model

The conceptual framework below (Figure 3) illustrates the process through which digital transformation creates the conditions for the emergence and expansion of Shadow IT and, increasingly, Shadow AI within contemporary organisations. Grounded in the Technology–Organisation–Environment (TOE) framework and Diffusion of Innovation (DOI) theory, the model explains how technological advancements, organisational characteristics, and environmental pressures interact to influence employee adoption of unauthorised technologies. The TOE framework highlights how factors such as cloud computing, generative AI, SaaS platforms, digital maturity, employee autonomy, business–IT alignment, and competitive pressures shape the organisational context in which Shadow IT emerges (Xu, 2025; N'Dri & Su, 2024). Complementing this perspective, DOI theory explains why employees adopt unauthorised tools based on their perceived relative advantage, compatibility with work routines, ease of use, trialability, and observability (Thuan et al., 2025). As organisations pursue digital transformation through process automation, AI-enabled work practices, remote work arrangements, and data-driven decision-making, employees increasingly seek flexible and efficient technologies that can satisfy immediate operational needs, often outside formal governance structures.

The framework further demonstrates how Shadow IT adoption acts as a mediating mechanism linking digital transformation to organisational complexity and cyber governance challenges. Consistent with the findings of this review, the adoption of unauthorised applications, self-procured SaaS tools, personal cloud storage systems, and generative AI platforms contributes to technology fragmentation, data silos, accountability ambiguities, and reduced organisational visibility (Klotz et al., 2019; Devasthali & Gupta, 2024; Shunmugasundaram et al., 2026). These conditions subsequently increase cyber governance risks, including data leakage, regulatory non-compliance, weak access controls, governance blind spots, and challenges associated with autonomous AI agents. In response, as previously discussed, the framework identifies adaptive governance approaches, co-governance models, continuous monitoring, secure sandbox environments, employee training, and AI governance mechanisms as key organisational responses. Therefore, the framework directly addresses the study's objectives by explaining how digital transformation drives Shadow IT adoption, identifying the factors that facilitate its diffusion, illustrating its consequences for organisational complexity and cyber governance, and highlighting governance strategies that can balance innovation, agility, security, and compliance within digitally transforming organisations.

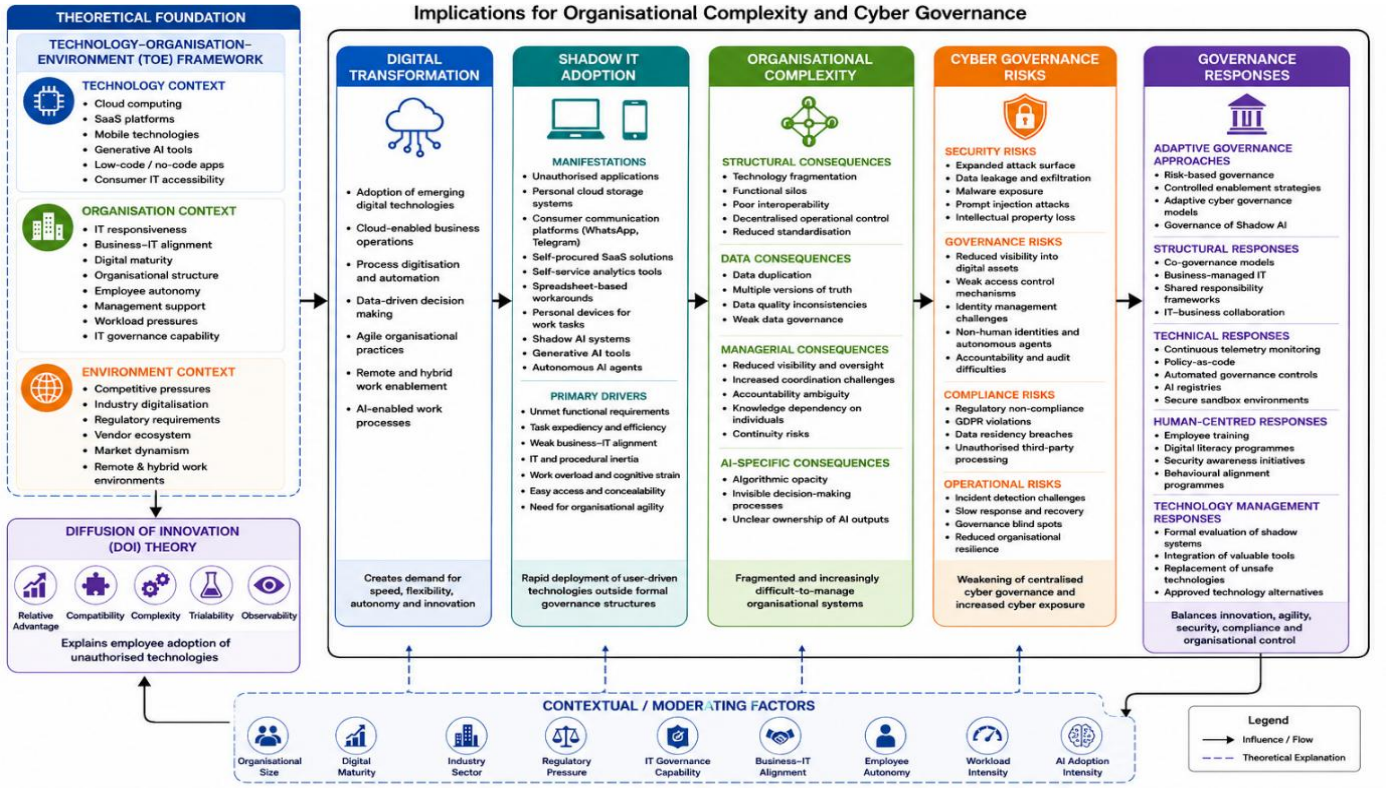

Figure 3 Conceptual framework of digital transformation and the rise of shadow IT: implications for organisational complexity and cyber governance.

4 Discussion

The adoption of unsanctioned applications generates profound structural complexity by fracturing the enterprise architecture into functional silos (Devasthali & Gupta, 2024; Klotz et al., 2019). When business units independently procure cloud services and generative artificial intelligence tools, they bypass formal integration protocols and create non-interoperable environments (Waters-Lynch et al., 2025). This decentralisation manifests directly as technological fragmentation, where disparate systems diminish standardisation and impede cross-departmental coordination (Devasthali & Gupta, 2024). Organisations subsequently experience widespread data duplication, as shadow solutions require manual data management without automated synchronisation, resulting in inconsistent datasets (Rakovic et al., 2020). The resulting opacity obscures active data flows and system inventories from centralised oversight, severely reducing administrative visibility (Scalabrin Bianchi et al., 2022; Shunmugasundaram et al., 2026). Furthermore, integrating adaptive AI tools introduces acute governance ambiguity, blurring accountability for algorithmic outputs and complex business decisions (Alfian et al., 2026; Shunmugasundaram et al., 2026).

This systematic literature review indicates that the severity of these outcomes varies considerably across different organisational settings (Silic et al., 2025). In highly centralised environments, the proliferation of shadow systems rapidly degrades operational synergy and creates substantial administrative friction (Klotz et al., 2019). Conversely, enterprises employing adaptive co-governance models often exhibit a greater capacity to manage structural variations, selectively absorbing local workarounds into the broader architecture without suffering equivalent coordination breakdowns (Fürstenau et al., 2021; Kopper et al., 2020).

These observations strengthen the proposed conceptual model by showing that unsanctioned technology adoption acts as a structural catalyst rather than a localised behavioural anomaly (Kasmo et al., 2025). The evidence demonstrates that decentralised tools inherently disrupt formal processes and introduce opaque decision-making pathways (Waters-Lynch et al., 2025). Ultimately, organisational complexity functions as the primary intermediary mechanism linking initial shadow IT adoption to deteriorating enterprise security and weakened cyber governance (Shunmugasundaram et al., 2026).

Theoretically, the Technology–Organisation–Environment (TOE) framework explains the interacting conditions driving unauthorised technology adoption (N'Dri & Su, 2024; Xu, 2025). Technologically, the widespread availability, compatibility, and concealability of cloud applications, Software-as-a-Service platforms, and generative artificial intelligence tools lower entry barriers (Waters-Lynch et al., 2025). These affordances enable employees to independently trial solutions aligning seamlessly with specific workflows, achieving immediate operational benefits outside formal oversight (Rakovic et al., 2020).

Organisationally, technological affordances intersect with systemic constraints (Kasmo et al., 2025). When central information technology departments demonstrate limited responsiveness, lack specialised business knowledge, or enforce slow procurement cycles, personnel face significant gaps between operational needs and approved systems (Furstenau et al., 2017; Silic et al., 2025). Such governance weaknesses and perceived system rigidity structurally encourage departments to bypass formal channels (Scalabrin Bianchi et al., 2022).

Environmentally, external demands accelerate this behaviour (Thuan et al., 2025). Market dynamism, competitive pressures, and agile operating models compel employees to respond rapidly to evolving conditions (Shunmugasundaram et al., 2026). When formal governance cannot match industry digitalisation, reliance on unofficial tools expands. Collectively, the TOE dimensions demonstrate how accessible technology, restrictive internal governance, and urgent environmental pressures embed Shadow IT into enterprise operations, exposing cyber governance vulnerabilities.

On the other hand, DOI theory clarifies why personnel bypass formal enterprise infrastructure for unauthorised digital tools (Thuan et al., 2025). Official information systems frequently present high operational complexity and demand extensive process adaptations, prompting employees to seek alternatives offering distinct relative advantages (Rakovic et al., 2020). Consumer-grade applications and generative artificial intelligence provide immediate processing speed, superior interfaces, and direct alignment with daily workflows (Shunmugasundaram et al., 2026). This high degree of compatibility ensures shadow technologies satisfy immediate productivity demands more effectively than rigid central governance (Furstenau et al., 2017).

The informal spread of these tools depends heavily on trialability and observability. Employees independently test cloud-based platforms to resolve local bottlenecks without initiating formal procurement cycles (Waters-Lynch et al., 2025). When initial trials yield concrete operational benefits, the visibility of successful workarounds among colleagues triggers informal diffusion networks (Haag & Eckhardt, 2024). Personnel observe peers' use and exchange functional solutions, establishing self-sustaining patterns of unauthorised technology adoption. DOI theory shows that unauthorised adoption is a predictable, user-driven response to the friction between corporate governance and practical workplace demands (N'Dri & Su, 2024).

5 Conclusion

This systematic literature review examines the role of digital transformation in the rise of Shadow IT and its implications for organisational complexity and cyber governance. The evidence suggests that digital transformation creates an environment in which employees resort to using unauthorised technologies when formal systems cannot meet operational needs, procurement processes are slow, or business agility is required. Cloud services, software-as-a-service platforms and generative AI have further lowered the barriers to independent technology adoption, expanding Shadow IT from traditional software into increasingly autonomous AI-enabled applications. The review also found that Shadow IT creates organisational complexity through disjointed technology infrastructures, data silos, duplication of information, reduced interoperability and lack of clarity in accountability for digital processes. These structural changes reduce the visibility of the organisation and increase the risks of cyber governance, such as data leakage, non-compliance with regulations, weak access controls and challenges in monitoring autonomous AI systems. The literature also indicates that a restrictive approach to governance is not enough to tackle these challenges simultaneously. Additional support for adaptive governance models that blend central oversight with controlled employee autonomy via co-governance arrangements, ongoing monitoring, secure sandbox environments, targeted training and structured assessment of unauthorised technologies. In this conceptual frame, we synthesise the relationships by elaborating on the conditions (technological, organisational, environmental) that promote Shadow IT adoption, how this adoption leads to organisational complexity and cyber governance risks, and how adaptive governance mechanisms can balance innovation, operational agility, security and regulatory compliance for digitally transforming organisations.

Practical Implications

In practice, organisations should recognise that the use of unauthorised technology is often driven by unmet operational requirements rather than deliberate policy breach. A governance approach that relies only on prohibition is unlikely to prevent Shadow IT adoption. Instead, organisations can improve cyber resilience by enhancing collaboration between business units and IT departments, streamlining technology approval processes, creating safe spaces for technology experimentation, and investing in ongoing employee awareness and training. This allows organisations to promote innovation while guaranteeing the right security, transparency and regulatory compliance in workplaces that are becoming more digital.

Implications for Managerial Practice and Policy

The study reveals that managers need to transition from constraining governance models to flexible, adaptive ones that align operational agility with cybersecurity needs. Business units and central IT departments should jointly share responsibility for technology governance, through co-governance arrangements that enhance communication, improve business–IT alignment and reduce incentives for unauthorised technology adoption. Organisations should also develop structured processes for evaluating shadow applications to decide whether they should be integrated, replaced or decommissioned. From a policy perspective, governance frameworks should include continuous monitoring, secure sandbox environments, AI-specific governance mechanisms, and employee training for better compliance while fostering responsible digital innovation.

Implications for Theory Development

The review, by blending the Technology–Organisation–Environment (TOE) framework with Diffusion of Innovation (DOI) theory, adds to the understanding of Shadow IT. The synthesis shows that Shadow IT emerges from the interplay of technological availability, organisational constraints, and external environmental pressures, whereas individual adoption is driven by perceptions of relative advantage, compatibility, ease of use, trialability, and observability. The proposed conceptual framework also conceptualises Shadow IT as the mechanism that connects digital transformation to organisational complexity and cyber governance outcomes, thereby providing a foundation for future empirical testing in various organisational contexts.

Limitations and Suggestions for Future Research

This review is based on the evidence drawn from 25 published studies and therefore reflects the scope and characteristics of the available literature. The studies included represent a variety of sectors, geographical contexts, methodologies and theoretical perspectives, which may limit direct comparison across findings. Moreover, much of the recent literature focuses on emerging types of Shadow AI, suggesting that knowledge in this area is still evolving.

Future research should empirically validate the proposed conceptual framework in industries with different regulatory requirements and digital maturity. Comparative studies of traditional Shadow IT versus new Shadow AI, as well as longitudinal studies of adaptive governance approaches, would enhance understanding of how organisations can maintain innovation while reinforcing cyber governance in digitally transforming environments.

Funding

This study was not supported by any grants from funding bodies in the public, private, or not-for-profit sectors. The authors declare that no financial support was received for the research, authorship, and publication of this article.

Data Availability

The datasets used and/or analysed during the current study are available from the corresponding author on request.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration of Use of Generative AI

AI tools were used only for grammar and formatting. No part of the study's methods, analysis, or results was generated by AI. The authors take full responsibility for the work.

References

Abed, S. S. (2024). Literature Review of Theory-Based Empirical Research Examining Consumers' Adoption of IoT. In S. K. Sharma, Y. K. Dwivedi, B. Metri, B. Lal, & A. Elbanna (Eds.), Transfer, Diffusion and Adoption of Next-Generation Digital Technologies (pp. 3–14). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50204-0_1

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organisational learning. Journal of the Association for Information Science and Technology, 71(8), 939–953. https://doi.org/10.1002/asi.24311

Akinson, A. O., Obasanya, A., Raimi, B. O., & Oshoba, A. O. (2025). Does Economic Literacy Matter for Firm Performance and Competitive Advantage: A Systematic Review. Elicit Journal of Economics and Management Studies, 1(1), 1-16. https://doi.org/10.65820/ejems-1vol1-issue1-2025

Alfian, A. A., Ayuningtias, F. T., & Tajuddin, M. H. bin. (2026). Artificial Intelligence, Digital Communication, and Legal Transformation: Toward Adaptive Cyber Governance in Indonesia. Kanuun: Journal of Sharia, Law, and Digital Society, 59–74. https://doi.org/10.66277/kanuun.v1i1.20

Castellano, N., Felden, C., & Pinsker, R. (2022). Shadow IT Behavior of Financial Executives in Germany and Italy as an Antecedent to Internal Data Security Breaches. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2022.765

Chateau-Dégat, F., & Mayrhofer, U. (2026). Managing Shadow IT in Cross-Border Acquisitions: A Case Study of a German Multinational. Management International Review, 66(2), 387–407. https://doi.org/10.1007/s11575-025-00611-6

Devasthali, S., & Gupta, G. (2024). Embracing Change from Shadow IT to Collaborative IT Models. In S. K. Sharma, Y. K. Dwivedi, B. Metri, B. Lal, & A. Elbanna (Eds.), Transfer, Diffusion and Adoption of Next-Generation Digital Technologies (Vol. 699, pp. 365–378). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50204-0_31

Digalwar, A. K., Singh, S. R., Pandey, R., & Sharma, A. (2024). Industry 4.0 Implementation: Evidence from Indian Industries. In S. K. Sharma, Y. K. Dwivedi, B. Metri, B. Lal, & A. Elbanna (Eds.), Transfer, Diffusion and Adoption of Next-Generation Digital Technologies (pp. 23–34). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50204-0_3

Falcão, D., & Roseira, C. (2022). Mapping the socially responsible consumption gap research: Review and future research agenda. International Journal of Consumer Studies, 46(5), 1718-1760. https://doi.org/10.1111/ijcs.12803

Fatorachian, H., & Ramesh, S. (2025). Leveraging digital transformation platforms to strengthen market position in India's textile industry. Cogent Business & Management, 12(1), 2527220. https://doi.org/10.1080/23311975.2025.2527220

Furstenau, D., Rothe, H., & Sandner, M. (2017). Shadow Systems, Risk, and Shifting Power Relations in Organizations. Communications of the Association for Information Systems, 41(1). https://doi.org/10.17705/1CAIS.04103

Fürstenau, D., Rothe, H., & Sandner, M. (2021). Leaving the Shadow: A Configurational Approach to Explain Post-identification Outcomes of Shadow IT Systems. Business & Information Systems Engineering, 63(2), 97–111. https://doi.org/10.1007/s12599-020-00635-2

Haag, S., & Eckhardt, A. (2024). Dealing Effectively with Shadow IT by Managing Both Cybersecurity and User Needs. MIS Quarterly Executive, 23(4). https://aisel.aisnet.org/misqe/vol23/iss4/5

Kasmo, A. B. P., Mor, S., Nugroho, L., Rohadi, M., & Purnama, A. (2025). Integrating Corporate Strategy with Digital Transformation, Cybersecurity, and Sustainability. Jurnal Lemhannas RI, 13(1), 52–68. https://doi.org/10.55960/jlri.v13i1.1062

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.

Kopper, A., Westner, M., & Strahringer, S. (2020). From Shadow IT to Business-managed IT: A qualitative comparative analysis to determine configurations for successful management of IT by business entities. Information Systems and E-Business Management, 18(2), 209–257. https://doi.org/10.1007/s10257-020-00472-6

Küçükoğlu, U., & Kabakuş, A. K. (2025). Revisiting the Technology–Organization–Environment Framework: Disruptive Technologies as Catalysts of Digital Transformation in the Turkish Banking Sector. Sustainability, 17(23), 10787. https://doi.org/10.3390/su172310787

Lebona, R., Mphunyane, M. Z. M., Mochekele, M., & Thamae, L. (2025). Redesigning Learning Spaces in Higher Institutions for the Post-Pandemic Era: A Systematic Review. Elicit Journal of Education Studies, 1(1), 44-59. https://doi.org/10.65820/ejes-4vol1-issue1-2025

Liang, Q., Crowston, K., & Gou, J. (2026). How to Come Up with AI Use Case Ideas? —An Ideation Technique Development Based on Analysis of Shadow IT Usage. Information Systems Frontiers. https://doi.org/10.1007/s10796-025-10676-1

Malik, G. (2025). CYBERSECURITY GOVERNANCE AND RISK MANAGEMENT FOR DIGITAL TRANSFORMATION. International Journal of Applied Mathematics, 38(10s), 2532–2561. https://doi.org/10.12732/ijam.v38i10s.1139

Mandal, K., & Bag, S. (2024). Bridging Realities: Understanding the Factors Influencing Visitor Satisfaction and Authentic Experiences in Virtual Tourism. In S. K. Sharma, Y. K. Dwivedi, B. Metri, B. Lal, & A. Elbanna (Eds.), Transfer, Diffusion and Adoption of Next-Generation Digital Technologies (Vol. 699, pp. 161–177). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50204-0_14

N'Dri, A. B., & Su, Z. (2024). Successful configurations of technology–organization–environment factors in digital transformation: Evidence from exporting small and medium-sized enterprises in the manufacturing industry. Information & Management, 61(7), 104030. https://doi.org/10.1016/j.im.2024.104030

Ogedengbe, F. A., Abdul Talib, Y. Y., & Rusly, F. H. (2024). Influence of structural factors on employee cloud shadow IT usage during COVID-19 lockdown: A strain theory perspective. Cognition, Technology & Work, 26(1), 63–81. https://doi.org/10.1007/s10111-023-00748-0

Orthi, S. M., Chakraborty, P., Siam, M. A., Shan-A-Alahi, A., Zaiem, A. A., Hasan, S. N., Kaur, J., Mahmud, F., & Goffer, M. A. (2023). AI-Driven Cyber Threat Intelligence as a Management Information System: Integrating Cybersecurity Governance and IT Project Management for Organisational Resilience. The Eastasouth Journal of Information System and Computer Science, 1(02), 194–213. https://doi.org/10.58812/esiscs.v1i02.873

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ, 72. https://doi.org/10.1136/bmj.n71

Panxhi, M., Thanasi-Boçe, M., & Hoxha, J. (2025). Digital transformation, entrepreneurial competence, and future job prospects in engineering education. Cogent Education, 12(1), 2526429. https://doi.org/10.1080/2331186X.2025.2526429

Rakovic, L., Duc, T. A., & Vukovic, V. (2020). Shadow IT and ERP: Multiple Case Studies in German and Serbian Companies. Journal of East European Management Studies, 25(4), 730–752.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Business Resilience: Issues and Recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

Scalabrin Bianchi, I., Vaquina, A., Pereira, R., Dinis Sousa, R., & Dávila, G. A. (2022). A Benefit Dependency Network for Shadow Information Technology Adoption, Based on Practitioners' Viewpoints. Informatics, 9(4), 95. https://doi.org/10.3390/informatics9040095

Sebastian, G. (2026). Digital shadow AI risk theory (DART): A framework for managing data disclosure and privacy risks of AI tools at work. Technological Forecasting and Social Change, 229, 124697. https://doi.org/10.1016/j.techfore.2026.124697

Shunmugasundaram, M., Gangadharan, S., Dave, R., Kala, S., & Michael, O. P. (2026). Shadow AI as the new Shadow IT: Governance blind spots in autonomous enterprise systems. EDPACS, 1–20. https://doi.org/10.1080/07366981.2026.2679653

Silic, M., Silic, D., & Kind-Trüller, K. (2025). From Shadow IT to Shadow AI–Threats, Risks and Opportunities for Organizations. Strategic Change, jsc.2682. https://doi.org/10.1002/jsc.2682

Sillic, M. (2019). Critical impact of organisational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. Computers & Security, 80, 108–119. https://doi.org/10.1016/j.cose.2018.09.012

Thuan, L. T., Tam, N. T., Trang, N. T. N., Trang, L. T. T., Huyen, K. N., & Huong, N. T. (2025). Digital transformation and sustainable business growth: Evidence from SMEs in Vietnam's Mekong Delta. International Journal of Advanced and Applied Sciences, 12(6), 223–233. https://doi.org/10.21833/ijaas.2025.06.022

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, 1–17. https://doi.org/10.1080/14479338.2025.2519546

Xu, K. (2025). Promotion path of digital transformation in China's manufacturing industry based on the technology-organisation-environment framework. Journal of Business Economics and Management, 26(5), 1090–1111. https://doi.org/10.3846/jbem.2025.24959

Zhao, Y., Meng, Q., & Li, Z. (2025). Performance Enhancement Pathways for Electric Vehicle Manufacturing Companies Driven by Digital Transformation—A Configuration Analysis Based on the TOE Framework. Systems, 13(8), 680. https://doi.org/10.3390/systems13080680

Zheng, Y., Dou, X., & Wang, X. (2026). What drives the digital transformation of farmers' cooperatives? An empirical analysis based on the TOE framework. Agricultural and Food Economics, 14(1), 3. https://doi.org/10.1186/s40100-026-00453-2