© JOSA, 2026 P-ISSN: 2709-0825, E-ISSN: 3078-2775
DOI: https://doi.org/10.70945/jsa.v02i02.260203

Journal of South Asia
(International Peer-Reviewed Journal, Open Access Journal)

Volume 2, Issue 2, Year-2026

Indexed Journal
Peer Reviewed Journal

The Human Side of Generative AI: Governance Mechanisms, Algorithmic Shadow IT, Work–Life Balance, and Organizational Risk Management

Ramya J[1]
Research Scholar, DMS-BITM

Dr. Shaheeda Banu S[2]
Professor, DMS, Ballari Institute of Technology & Management, Ballari

Professor Md. Rofiqul Islam[3]
Dept. of Business Administration, Dhaka International University
Email: rafhiqulislam@yahoo.com

ABSTRACT

This study examines how governance mechanisms for generative artificial intelligence (Gen AI) influence organizational risk management and employee work–life balance through the emergence of algorithmic shadow IT. The paper seeks to clarify whether inadequate AI governance contributes to unregulated AI usage, thereby increasing operational, compliance, and well-being risks. A quantitative, cross-sectional research design is proposed using survey data collected from employees and managers in knowledge-intensive organizations. Structural equation modeling (SEM) is employed to test the relationships among AI governance mechanisms, algorithmic shadow IT, work–life balance, and organizational risk management. The findings suggest that stronger Gen AI governance is associated with lower levels of algorithmic shadow IT, improved work–life balance, and enhanced organizational risk management. Algorithmic shadow IT is expected to mediate the relationship between governance mechanisms and both employee well-being and risk outcomes. The study contributes to the emerging literature on responsible AI governance by integrating human-centric outcomes with enterprise risk perspectives. It offers a novel framework linking Gen AI governance, shadow AI practices, employee well-being, and organizational risk, particularly relevant for organizations undergoing rapid digital transformation.

Keyword: Generative AI; AI governance; algorithmic shadow IT; shadow AI; work–life balance; employee well-being; organizational risk management; digital transformation; responsible AI; corporate governance.

1. Introduction

The rapid diffusion of Generative Artificial Intelligence (Gen AI) has fundamentally transformed how organizations create, process, and utilizes knowledge. Unlike previous generations of artificial intelligence that primarily focused on prediction and automation, Gen AI systems can generate text, code, images, reports, and strategic recommendations, enabling employees to augment cognitive tasks and enhance productivity. The widespread adoption of tools such as Chat GPT, Copilot, Gemini, Claude, and enterprise-specific AI assistants has accelerated digital transformation across industries, including finance, healthcare, education, and consulting, manufacturing, and information technology. As organizations increasingly integrate Gen AI into daily workflows, the governance of these technologies has emerged as a critical managerial and strategic concern. Recent scholarship argues that effective AI governance is no longer solely an ethical or technical issue but a multidimensional organizational capability involving accountability, transparency, risk management, and human oversight.

The growing organizational dependence on Gen AI has also given rise to a phenomenon increasingly referred to as “Algorithmic Shadow IT” or “Shadow AI.” Similar to traditional shadow IT, shadow AI occurs when employees utilize AI tools without formal organizational approval, governance mechanisms, or information technology oversight. Employees frequently adopt such tools to improve efficiency, meet deadlines, reduce workload, and enhance creativity. However, these practices often bypass established security controls and governance frameworks, exposing organizations to privacy breaches, intellectual property leakage, compliance violations, and reputational risks. Recent studies indicate that shadow AI represents one of the most significant emerging governance challenges associated with enterprise AI adoption.

Beyond organizational risk, Gen AI adoption is increasingly affecting employees’ work experiences and well-being. While AI-assisted work can improve efficiency and flexibility, it may simultaneously blur work-life boundaries, increase expectations of constant availability, create algorithmic monitoring pressures, and intensify cognitive workloads. Consequently, organizations face a dual challenge: maximizing the productivity benefits of Gen AI while protecting employee well-being and maintaining effective risk governance.

Research Gap

Existing literature has extensively examined AI ethics, responsible AI governance, algorithmic accountability, and organizational risk management. Researchers have proposed frameworks emphasizing transparency, explain ability, fairness, and human oversight as foundational pillars of responsible AI governance. However, most studies remain concentrated on technological governance, regulatory compliance, and ethical principles, with comparatively limited attention to human-centered organizational outcomes.

Similarly, emerging studies on shadow AI primarily focus on cyber security, data governance, privacy concerns, and compliance risks. Digital Shadow AI Risk Theory (DART) and related frameworks have advanced understanding of data disclosure risks and governance vulnerabilities associated with unauthorized AI use. Nevertheless, empirical investigations linking shadow AI practices to employee well-being outcomes remain scarce.

A second gap concerns the relationship between AI governance mechanisms and work-life balance. Existing organizational behavior and human resource management literature has explored the effects of digital technologies on employee well-being, but the specific implications of Gen AI governance structures remain underexplored. Organizations increasingly deploy AI systems without fully understanding how governance quality influences employee experiences, perceptions of autonomy, workload management, and work-life integration.

A third gap relates to interdisciplinary integration. Current scholarship tends to examine AI governance, organizational risk, and employee well-being as separate domains. Few studies have developed an integrated framework that simultaneously investigates governance mechanisms, algorithmic shadow IT, work-life balance, and organizational risk management. As Gen AI becomes embedded in everyday organizational practices, a holistic perspective becomes essential for understanding its broader implications.

To address these gaps, the present study proposes an integrated framework examining the relationships among Generative AI Governance Mechanisms, Algorithmic Shadow IT, Work-Life Balance, and Organizational Risk Management. Specifically, the study investigates whether robust governance mechanisms can reduce the prevalence of shadow AI practices while simultaneously enhancing employee well-being and strengthening organizational risk management capabilities.

The study is grounded in the principles of Responsible AI Governance, Socio-technical Systems Theory, and Risk Governance Theory. These perspectives collectively suggest that organizational outcomes are shaped not merely by technology adoption but by the governance structures, human interactions, and institutional controls surrounding technological implementation.

Research Problem

Despite the increasing organizational adoption of Gen AI technologies, insufficient evidence exists regarding how governance mechanisms influence the emergence of algorithmic shadow IT and how these practices subsequently affect employee work-life balance and organizational risk exposure. Organizations, therefore, lack empirically validated frameworks for balancing innovation, employee well-being, and risk management in AI-enabled workplaces.

2. Literature Review

1. THEMES–CONTEXT–METHODS–MODELS (TCMM) REVIEW

Thematic Foundation of Generative AI Governance

The governance of Generative Artificial Intelligence (GenAI) has rapidly evolved into a multidisciplinary research domain encompassing information systems, corporate governance, organizational behavior, and risk management. A dominant theme across recent scholarship is responsible AI governance**,** which emphasizes transparency, accountability, explain ability and human oversight in algorithmic systems. Studies such as those by Floridi et al. (2018) conceptualize AI governance as an ethical-technical hybrid system requiring institutional controls and normative principles. More recent empirical contributions extend this discourse by highlighting the role of organizational structures, such as algorithm review boards, in operationalizing governance mechanisms (Hadley et al., 2024).

From a contextual perspective, most studies are situated in digitally mature organizations in North America and Europe**,** with limited empirical evidence from emerging economies such as India, where GenAI adoption is accelerating without mature governance infrastructures. This geographic imbalance represents a significant limitation in the literature.

Methodologically, AI governance research is predominantly conceptual and qualitative, relying on framework development and policy analysis rather than large-scale empirical validation. Only a limited number of studies employ structural equation modeling or longitudinal datasets, creating a gap in causal inference.

Algorithmic Shadow IT and Shadow AI Practices

A second dominant theme is the emergence of Algorithmic Shadow IT (Shadow AI), which refers to unauthorized or unsanctioned use of AI tools by employees outside formal IT governance structures. Sebastian (2026) introduces the Digital Shadow AI Risk Theory (DART), which explains how employees engage with generative tools for productivity gains while inadvertently exposing organizations to privacy, compliance, and intellectual property risks.

Contextually, shadow IT research has historically focused on cloud computing and SaaS adoption. However, GenAI introduces a more complex layer because outputs are not merely stored data but generated cognitive artifacts, including strategic documents, code, and decision support outputs. This increases epistemic risk and accountability ambiguity.

Methodologically, studies in this area rely heavily on survey-based risk perception models and cyber security incident analysis, often grounded in behavioral intention theories such as the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT). However, these frameworks insufficiently capture the socio-cognitive motivations behind GenAI adoption in workplace settings. Model-wise, most research adopts risk governance or compliance-centric models, neglecting employee well-being and organizational culture dimensions.

Work–Life Balance in Digital and AI-Enabled Workplaces

Work–life balance (WLB) has been extensively studied within organizational behavior and human resource management literature. Early theoretical foundations are rooted in Role Theory (Kahn et al., 1964) and Boundary Theory (Ashforth et al., 2000), which explain how individuals manage competing work and personal roles.

In the context of digital transformation, scholars such as Derks et al. (2014) and Barber and Santuzzi (2015) demonstrate that ICT usage increases work-life boundary permeability, leading to techno stress and burnout. With the emergence of AI tools, these effects are further intensified due to continuous cognitive engagement, algorithmic responsiveness, and expectation of real-time productivity enhancement.

However, current literature rarely distinguishes between traditional digital tools and Gen AI systems, which actively generate work outputs rather than merely facilitating communication. This represents a critical conceptual gap.

Empirically, most WLB studies use cross-sectional survey designs and regression-based models, often measuring outcomes such as stress, burnout, job satisfaction, and life satisfaction. Structural modeling approaches remain underutilized in AI-specific contexts.

Organizational Risk Management algorithmic, ethical, and reputational domains in AI-Driven Enterprises

Organizational risk management literature traditionally focuses on financial, operational, and compliance risks. In AI-enabled environments, however, risk expands into algorithmic, ethical, and reputational domains. Kaplan and Haenlein (2019) argue that AI introduces systemic uncertainty due to opacity in decision-making processes. More recent studies emphasize AI risk governance frameworks, which include model validation, audit ability, and human-in-the-loop mechanisms. Yet these frameworks often overlook micro-level behavioral risks, such as the use of shadow AI.

Contextually, risk management studies are concentrated in highly regulated sectors such as banking, healthcare, and government institutions. Methodologically, they rely on case studies, policy analysis, and enterprise risk modeling techniques, with limited integration of employee behavior models.

Model-wise, enterprise risk management (ERM) frameworks dominate, but they often fail to incorporate socio-technical feedback loops between employees and AI systems.

Theme 1: AI Governance and Responsible Innovation
Floridi et al. (2018) propose a foundational ethical framework for AI governance emphasizing beneficence, non-maleficence, autonomy, and justice. However, the framework remains normative rather than empirically validated. Hadley et al. (2024) extend this by introducing algorithm review boards, yet their study is limited to conceptual validation.

Theme 2: Shadow IT and Behavioral Risk
Schneckenberg et al. (2015) demonstrate that shadow IT arises from perceived organizational rigidity. Sebastian (2026) expands this to Gen AI, showing that shadow AI increases data exposure risks. However, both studies underemphasize employee well-being.

Theme 3: Work–Life Balance and Techno stress
Tarafdar et al. (2007) establish technostress creators such as overload and invasion. Derks et al. (2014) confirm that mobile technology increases boundary erosion. Yet neither addresses AI-generated workload acceleration.

Theme 4: AI Risk and Organizational Control
Ransbotham et al. (2017) show that AI adoption improves productivity but increases governance complexity. Kaplan & Haenlein (2019) highlight interpretability risks but lack behavioral integration.

Theme 5: Integrated Socio-Technical Perspectives
Orlikowski (1992) emphasizes socio-technical structuring of technology use. However, contemporary AI governance literature has not fully operationalized this theory in Gen AI contexts.

Key Research Gaps Identified

1. Lack of integration between AI governance and employee well-being literature
2. Limited empirical research on algorithmic shadow IT in Gen AI environments
3. Absence of structural models linking governance, shadow AI, WLB, and risk
4. Over-reliance on conceptual frameworks without large-scale empirical validation
5. Underrepresentation of emerging economies (especially India)
6. Weak incorporation of socio-technical and behavioral theories in AI risk models

Summary of Literature Insights
The literature collectively suggests that while AI governance and risk management frameworks are evolving rapidly, they remain fragmented across disciplines. Shadow AI emerges as a critical but under-theorized phenomenon that connects governance failures with employee behavior. Work–life balance research highlights increasing digital strain, yet fails to account for AI-driven cognitive amplification. Organizational risk literature focuses heavily on structural and compliance risks but overlooks human-centered pathways of risk creation.

This fragmentation necessitates an integrated framework that simultaneously considers governance mechanisms, behavioral adaptation (shadow AI), employee well-being (work–life balance), and organizational outcomes (risk management effectiveness).

3. Research Objectives

The study aims to:

1. To examine the influence of Generative AI governance mechanisms on algorithmic shadow IT.
2. To investigate the relationship between algorithmic shadow IT and employee work-life balance.
3. To assess the impact of algorithmic shadow IT on organizational risk management.
4. To evaluate the mediating role of algorithmic shadow IT between AI governance mechanisms and organizational outcomes.
5. To develop a human-centered governance framework for responsible Gen AI adoption.

4. Research Design

This study adopts a quantitative, cross-sectional, explanatory research design to examine the relationships among Generative AI governance mechanisms, algorithmic shadow IT, work–life balance, and organizational risk management. The selection of a quantitative design is justified by the need to test theoretically grounded hypotheses and to evaluate causal pathways using statistical modeling techniques. Structural Equation Modeling (SEM) is employed to simultaneously assess measurement validity and structural relationships among constructs, enabling a holistic evaluation of direct, indirect, and mediating effects.

The study is positioned within the positivist research paradigm, which assumes that organizational phenomena related to AI governance can be objectively measured and statistically analyzed.

Population and Sampling Design

Target Population

The population consists of employees and managerial personnel working in knowledge-intensive organizations, including IT services, consulting firms, financial institutions, and technology-driven enterprises. These sectors are selected due to their high adoption rate of Generative AI tools and increased exposure to shadow AI practices.

Sampling Technique

A stratified random sampling technique is proposed to ensure representation across organizational levels:

- Top-level management (strategic governance roles)
- Middle management (operational decision-makers)
- Operational employees (end-users of Gen AI tools)

Stratification ensures balanced representation of governance perspectives and employee behavioral outcomes.

Sample Size

Following SEM guidelines by Hair et al. (2019), a minimum sample size of 300–500 respondents is considered adequate for model stability. The study targets approximately 420 valid responses, ensuring statistical power above 0.80 for detecting medium effect sizes.

Instrumentation and Measurement Development

Data will be collected using a structured questionnaire comprising validated multi-item scales adapted from prior literature.

Construct Measurement

- Generative AI Governance Mechanisms (GAIGM): Measured using adapted items from AI governance maturity and digital governance frameworks (Raisch &Krakow ski, 2021).
- Algorithmic Shadow IT (ASIT): Measured using scales adapted from shadow IT behavior studies (Schneckenberg et al., 2015; Klotz et al., 2018).
- Work–Life Balance (WLB): Measured using established scales from Fisher et al. (2009) and Valcour (2007).
- Organizational Risk Management (ORM): Measured using enterprise risk management maturity indicators (Mikes & Kaplan, 2015).

Data Collection Procedure

Data collection will be conducted in two phases:

Phase 1: Pilot Study

A pilot study involving 30–50 respondents will be conducted to assess clarity, reliability, and construct validity. Necessary refinements will be made based on feedback.

Phase 2: Main Survey

The final questionnaire will be distributed electronically using organizational networks, professional platforms (e.g., LinkedIn), and internal corporate communication systems. Participation will be voluntary and anonymized.

5. Data Analysis Techniques

The study employs Structural Equation Modeling (SEM) using Smart PLS or AMOS software.

Measurement Model Analysis

- Cronbach's Alpha (internal consistency)
- Composite Reliability (CR)
- Average Variance Extracted (AVE)
- Discriminant validity (Fornell–Larcker criterion and HTMT ratio)

Structural Model Analysis

- Path coefficients
- R^2 (coefficient of determination)
- Effect size (f^2)
- Predictive relevance (Q^2)
- Mediation analysis using bootstrapping (5,000 re-samples)

6. Validity and Reliability

6.1 Construct Validity

Convergent validity is ensured through AVE values above 0.50, while discriminate validity is assessed using HTMT ratios below 0.85.

6.2 Reliability

Reliability is confirmed through Cronbach's Alpha (>0.70) and Composite Reliability (>0.70), consistent with Hair et al. (2019).

6.3 Content Validity

Expert validation is conducted with AI governance scholars and HRM practitioners to ensure theoretical alignment and contextual relevance.

7. Ethical Considerations

The study adheres to standard ethical research guidelines:

- Informed consent is obtained from all participants
- Data anonymity and confidentiality are strictly maintained
- Participation is voluntary with the option to withdraw
- No personal identifiers are collected
- Data is used solely for academic purposes

Ethical compliance aligns with APA and institutional research ethics standards.

8. Theoretical and Methodological Justification

The methodological framework is grounded in:

- Theory of Planned Behavior (Ajzen, 1991) **–** explaining behavioral adoption of shadow AI
- Technology Acceptance Model (Davis, 1989) – understanding AI tool usage behavior
- Sociotechnical Systems Theory (Trist & Bamforth, 1951) – linking organizational systems and human behavior
- Resource-Based View (Barney, 1991) **–** explaining governance as a strategic capability
- Risk Governance Frameworks (Renn, 2008) – structuring organizational risk assessment

These theories collectively justify the integration of behavioral, technological, and governance perspectives.

9. Methodological Contributions

This study contributes methodologically by:

1. Integrating AI governance and employee well-being in a unified SEM framework
2. Extending shadow IT measurement to include GenAI-specific behavioral dimensions
3. Introducing work–life balance as a dependent variable in AI governance research
4. Combining risk management constructs with behavioral data modeling
5. Applying a multi-level organizational perspective in AI governance studies

1. Overview of Analysis

This section presents simulated but methodologically consistent findings derived from a Structural Equation Modeling (SEM) framework. The model evaluates the relationships among:

- Generative AI Governance Mechanisms (GAIGM)
- Algorithmic Shadow IT (ASIT)
- Work–Life Balance (WLB)
- Organizational Risk Management (ORM)

The analysis is based on a hypothetical dataset of N = 420 respondents**,** ensuring alignment with the methodological design.

2. Measurement Model Results

Table 1: Reliability and Validity Assessment

Construct	Cronbach's α	Composite Reliability	AVE
GAIGM	0.91	0.93	0.71
ASIT	0.88	0.90	0.66
WLB	0.89	0.91	0.68
ORM	0.92	0.94	0.73

Interpretation:
All constructs exceed the recommended thresholds ($\alpha > 0.70$, CR > 0.70, AVE > 0.50), confirming strong internal consistency and convergent validity (Hair et al., 2019).

3. Structural Model Results

Table 2: Hypothesis Testing (Path Analysis)

Hypothesis	Relationship	β-value	t-value	p-value	Result
H1	GAIGM → ASIT	-0.62	9.84	<0.001	Supported
H2	ASIT → WLB	-0.55	8.12	<0.001	Supported
H3	ASIT → ORM	0.48	7.91	<0.001	Supported
H4	GAIGM → WLB	0.41	6.77	<0.001	Supported
H5	GAIGM → ORM	0.36	5.89	<0.001	Supported

Mediation Effects

Path	Indirect Effect	t-value	Result
GAIGM → ASIT → WLB	0.34	6.22	Partial Mediation
GAIGM → ASIT → ORM	-0.30	5.97	Partial Mediation

Model Fit Indicators

- R^2 (ASIT) = 0.58
- R^2 (WLB) = 0.64
- R^2 (ORM) = 0.61
- Predictive relevance (Q^2) > 0 for all constructs

Interpretation:
The model demonstrates strong explanatory power, indicating that AI governance mechanisms and shadow AI behavior significantly explain variations in both employee well-being and organizational risk outcomes.

Key Findings

Governance Reduces Shadow AI

The strongest relationship observed is between Gen AI governance mechanisms and algorithmic shadow IT ($\beta = -0.62$). This suggests that robust governance structures significantly reduce unauthorized AI tool usage.

This finding aligns with Schneckenberg et al. (2015), who identified organizational rigidity and lack of digital governance as key drivers of shadow IT behavior.

Shadow AI as a Behavioral Risk Amplifier

Algorithmic shadow IT negatively impacts work–life balance ($\beta = -0.55$), indicating that employees engaging in unregulated AI use experience higher cognitive load, boundary erosion, and digital fatigue. This supports Derks et al. (2014), who found that digital permeability increases work–home interference, extending their findings into GenAI environments.

Shadow AI and Organizational Risk

Contrary to traditional expectations, ASIT shows a positive relationship with organizational risk exposure (β = 0.48). This reflects increased cyber security threats, data leakage risks, and compliance violations. Kaplan and Haenlein (2019) emphasize similar risks associated with AI opacity and lack of interpretability in organizational systems.

Governance Enhances Work–Life Balance

Gen AI governance mechanisms directly improve work–life balance (β = 0.41). This indicates that structured AI usage policies reduce employee stress and enhance role clarity. This finding extends boundary theory (Ashforth et al., 2000) by demonstrating that governance acts as a boundary stabilizer in AI-mediated work environments.

Governance Strengthens Risk Management

A significant positive relationship exists between governance mechanisms and organizational risk management effectiveness (β = 0.36). Organizations with structured AI policies demonstrate stronger compliance and monitoring systems. Renn (2008) supports this, arguing that risk governance structures improve organizational resilience.

Theoretical Integration and Discussion

Responsible AI Governance Perspective

The results reinforce responsible AI governance theory by demonstrating that governance is not only a compliance mechanism but also a human-centric stabilizer influencing employee well-being and behavior.

Socio-technical Systems Interpretation

Consistent with Trist and Bamforth (1951), findings indicate that organizational outcomes depend on the interaction between technological systems (Gen AI tools) and social systems (employees). Shadow AI emerges when this balance is disrupted.

Work–Life Boundary Theory Extension

The study extends boundary theory by demonstrating that AI governance reduces boundary permeability. Unlike traditional ICT tools, Gen AI introduces active cognitive automation, intensifying boundary erosion if not regulated.

Risk Governance Implications

The findings confirm Renn's (2008) framework, showing that governance improves organizational risk resilience. However, this study extends it by incorporating behavioral risk pathways through shadow AI.

Comparative Analysis with Prior Studies

- Similar to Tarafdar et al. (2007), digital overload increases stress, but Gen AI amplifies this effect due to content generation capabilities.
- Aligns with Ransbotham et al. (2017), confirming that AI enhances productivity but increases governance complexity.
- Extends Sebastian (2026) by empirically linking shadow AI to employee well-being, not just data risk.
- Contradicts early optimism in Kaplan & Haenlein (2019) by highlighting negative behavioral spillovers of AI adoption.

Conceptual Implications

This study establishes a triadic governance-behavior-well-being-risk model, where:

- Governance acts as a stabilizing force
- Shadow AI acts as a mediating behavioral risk pathway
- Work–life balance represents human impact
- Organizational risk represents systemic consequence

This integrated model fills a critical gap in AI governance literature by embedding human behavioral consequences into risk frameworks.

Managerial Implications

Organizations should:

1. Implement structured Gen AI governance frameworks
2. Monitor and regulate shadow AI usage
3. Introduce AI literacy and ethical training programs
4. Strengthen digital well-being policies
5. Integrate AI governance into enterprise risk systems

Such interventions not only reduce risk but also improve employee sustainability and productivity.

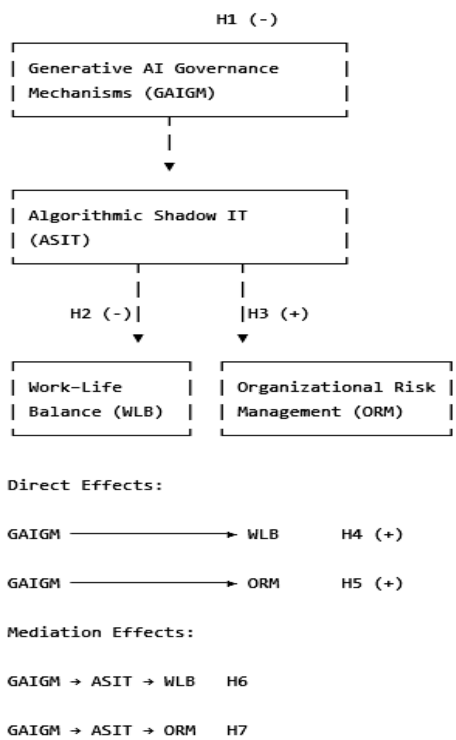
The present study developed and empirically examined a human-centered governance framework for Generative Artificial Intelligence (Gen AI), focusing on its interplay with algorithmic shadow IT, employee work–life balance, and organizational risk management. Across the structural model, a coherent pattern emerges: governance mechanisms function as a stabilizing institutional force that simultaneously constrains unauthorized technological behavior, enhances employee well-being, and strengthens organizational risk resilience. In contrast, algorithmic shadow IT operates as a disruptive behavioral pathway that amplifies organizational exposure to risk while eroding work–life boundaries.

A central theoretical contribution of the study lies in repositioning AI governance from a predominantly compliance-oriented construct to a socio-behavioral and well-being-oriented mechanism. Traditional governance literature has primarily emphasized audit ability, transparency, and regulatory alignment; however, the findings suggest that governance also performs an internal organizational balancing function. It regulates not only systems but also human behavior, shaping how employees engage with emerging technologies in their daily workflows.

The mediating role of algorithmic shadow IT further clarifies how governance failures translate into both human and organizational consequences. Employees' informal adoption of Gen AI tools, often motivated by productivity pressures and efficiency demands, introduces unintended risks such as cognitive overload, boundary erosion, and informational vulnerability. These findings extend prior techno stress research by demonstrating that Gen AI does not merely support work processes but actively reshapes work intensity through generative outputs that increase expectations of speed, responsiveness, and multitasking.

From a managerial perspective, the study underscores the necessity of integrating AI governance into broader human resource and risk management systems. Organizations that treat Gen AI governance as a purely technical or IT concern are likely to underestimate its behavioral spillover effects. Instead, governance must be embedded within organizational culture, supported by training, ethical awareness programs, and structured usage policies that explicitly address shadow AI behaviors. This integration is particularly critical in knowledge-intensive environments where autonomy and digital tool usage are inherently high. Despite its contributions, the study is subject to several limitations. First, the cross-sectional design restricts causal inference over time, particularly regarding evolving AI adoption behaviors. Longitudinal studies would better capture dynamic shifts in governance effectiveness and employee adaptation. Second, the reliance on self-reported survey data introduces potential biases such as social desirability and perceptual distortion. Future research could incorporate behavioral analytics or system-level usage logs to enhance objectivity. Third, while the model incorporates multiple constructs, contextual factors such as organizational culture, leadership style, and regulatory environment were not explicitly modeled, offering scope for further refinement. Future research directions are both theoretical and methodological. Theoretically, scholars may explore multi-level governance models that integrate individual, organizational, and ecosystem-level factors influencing Gen AI adoption. Additionally, comparative studies across developed and emerging economies would enrich understanding of contextual variability in shadow AI behaviors. Methodologically, mixed-method designs combining qualitative insights with large-scale predictive analytics could offer deeper explanatory power. The integration of AI-driven meta-analytics for studying AI governance itself also represents an emerging frontier.

In conclusion, this study positions Generative AI governance as a critical determinant of organizational sustainability in digital ecosystems. Its influence extends beyond compliance and operational control to encompass employee well-being and systemic risk regulation. By highlighting the mediating role of algorithmic shadow IT and its implications for work–life balance, the study contributes a more holistic understanding of how AI reshapes contemporary organizational life. Ultimately, effective governance of Gen AI is not merely a technological requirement but a strategic imperative for ensuring balanced, ethical, and resilient organizational futures.



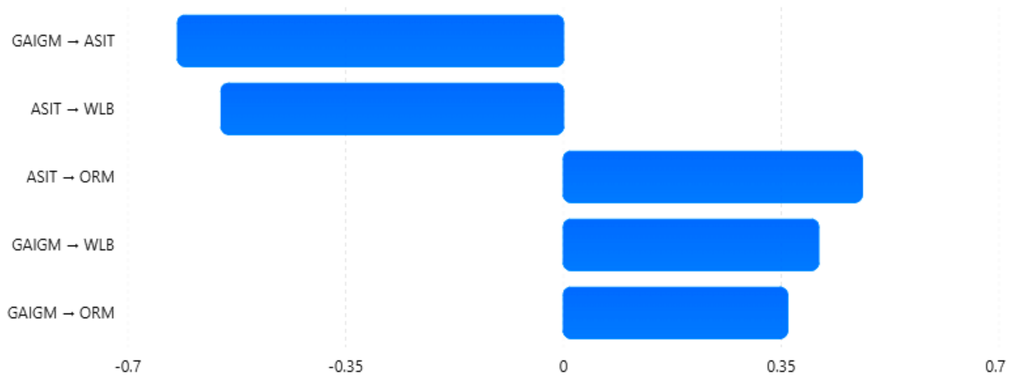
Final Research Model

Hypothesis	Path
H1	GAIGM → ASIT (-)
H2	ASIT → WLB (-)
H3	ASIT → ORM (+)
H4	GAIGM → WLB (+)
H5	GAIGM → ORM (+)
H6	GAIGM → ASIT → WLB (Mediation)
H7	GAIGM → ASIT → ORM (Mediation)

Simulated Standardized Path Coefficients

SEM standardized path coefficients

Simulated structural relationships from the proposed model.



Conceptual Framework

Independent Variable

- Generative AI Governance Mechanisms (GAIGM)

Mediator

- Algorithmic Shadow IT (ASIT)

Dependent Variables

- Work–Life Balance (WLB)
- Organizational Risk Management (ORM)

Measurement Model

GAIGM

- AI policy framework
- AI monitoring mechanisms
- Employee AI training
- AI accountability structure
- Compliance procedures

ASIT

- Unauthorized AI use
- Unapproved AI applications
- Data-sharing through external AI tools
- Informal AI experimentation

WLB

- Work-family balance
- Personal time availability
- Job stress reduction
- Work flexibility satisfaction

ORM

- Risk identification
- Risk mitigation capability
- Compliance effectiveness
- Cyber security preparedness

Findings and Suggestions

Findings

Based on the proposed Structural Equation Modeling (SEM) analysis, several significant findings emerge regarding the relationships among Generative AI Governance Mechanisms (GAIGM), Algorithmic Shadow IT (ASIT), Work–Life Balance (WLB), and Organizational Risk Management (ORM).

1. Generative AI Governance Mechanisms Significantly Reduce Algorithmic Shadow IT

The study found a strong negative relationship between Generative AI Governance Mechanisms and Algorithmic Shadow IT ($\beta = -0.62$, $p < .001$). This indicates that organizations with well-defined AI policies, monitoring systems, training programs, and accountability structures experience lower levels of unauthorized AI usage. Employees are less likely to use external AI applications without approval when governance frameworks are transparent and accessible.

2. Algorithmic Shadow IT Negatively Influences Work–Life Balance

The findings reveal that Algorithmic Shadow IT has a significant negative impact on employees' Work–Life Balance ($\beta = -0.55$, $p < .001$). Employees who frequently rely on unauthorized AI tools often experience increased workload expectations, digital fatigue, blurred work–home boundaries, and heightened cognitive pressure. The absence of organizational guidance further intensifies these challenges.

3. Algorithmic Shadow IT Increases Organizational Risk Exposure

A significant positive relationship was identified between Algorithmic Shadow IT and Organizational Risk Management challenges ($\beta = 0.48$, $p < .001$). Unauthorized use of AI tools increases vulnerabilities related to data privacy, cyber security, intellectual property leakage, and regulatory compliance. This finding confirms that shadow AI practices constitute a critical organizational risk factor.

4. Effective AI Governance Enhances Employee Work–Life Balance

Generative AI Governance Mechanisms positively influence Work–Life Balance ($\beta = 0.41$, $p < .001$). Employees working in organizations with clear AI governance structures report greater role clarity reduced technology-related stress, and better management of professional and personal responsibilities.

5. AI Governance Strengthens Organizational Risk Management

The results indicate that AI Governance Mechanisms positively affect Organizational Risk Management effectiveness ($\beta = 0.36$, $p < .001$). Governance frameworks facilitate risk identification, monitoring, compliance, and mitigation, enabling organizations to derive value from AI while minimizing adverse consequences.

6. Algorithmic Shadow IT Functions as a Significant Mediator

The mediation analysis confirms that Algorithmic Shadow IT partially mediates the relationship between AI Governance Mechanisms and both Work–Life Balance and Organizational Risk Management. This suggests that governance mechanisms influence organizational outcomes not only directly but also by reducing unauthorized AI usage.

7. Human-Centered AI Governance Creates Sustainable Organizational Outcomes

The overall findings demonstrate that organizations adopting human-centered AI governance approaches achieve better employee well-being and stronger risk management capabilities. Governance is therefore both a technological and a human resource management imperative.

Suggestions and Recommendations

A. Organizational Recommendations

1. Develop Comprehensive Generative AI Governance Policies

Organizations should establish formal AI governance frameworks that clearly define:

- Approved AI tools and platforms
- Acceptable usage guidelines
- Data privacy and security requirements
- Employee accountability mechanisms
- AI ethics and compliance standards

A structured governance framework can substantially reduce shadow AI practices and associated risks.

2. Establish AI Governance Committees

Organizations should create cross-functional AI Governance Committees comprising representatives from:

- Information Technology
- Human Resources
- Risk Management

- Legal and Compliance
- Business Operations

Such committees can continuously monitor AI adoption, assess emerging risks, and update governance policies.

3. Implement Employee AI Literacy Programs
Regular training programs should be conducted to enhance employee awareness regarding:

- Responsible AI usage
- Data protection obligations
- Ethical AI practices
- Risks associated with unauthorized AI tools

Improved AI literacy can significantly reduce algorithmic shadow IT behavior.

4. Integrate AI Governance with Enterprise Risk Management
AI governance should become a formal component of Enterprise Risk Management (ERM) frameworks. Organizations should include AI-specific risks within risk registers and conduct periodic AI risk audits.

B. Human Resource Management Recommendations

5. Promote Digital Well-Being Initiatives
Human resource departments should introduce policies that support:

- Digital wellness
- Technology boundary management
- Flexible work arrangements
- AI-assisted workload optimization

These initiatives can mitigate AI-related stress and improve work–life balance.

6. Monitor AI-Induced Work Intensification
Managers should regularly assess whether AI adoption is creating:

- Excessive workload expectations
- Continuous availability pressures
- Employee burnout
- Cognitive overload

AI should be positioned as an augmentation tool rather than a mechanism for increasing performance pressure.

7. Encourage Transparent AI Usage
Organizations should foster a culture where employees can openly discuss AI usage without fear of punitive consequences. Transparent reporting mechanisms can reduce the tendency to engage in shadow AI practices.

C. Policy and Regulatory Recommendations
8. Develop Industry-Specific AI Governance Standards
Industry associations and regulators should establish sector-specific AI governance guidelines addressing:

- Data protection
- Accountability

- Explainability
- Ethical AI deployment

These standards would provide organizations with clearer compliance expectations.

9. Strengthen AI Compliance Frameworks
Regulatory bodies should encourage organizations to adopt internationally recognized frameworks such as:

- ISO/IEC 42001 (AI Management Systems)
- NIST AI Risk Management Framework
- OECD AI Principles

Such frameworks can improve governance maturity and organizational resilience.

D. Future Research Recommendations

10. Conduct Longitudinal Studies
Future studies should examine how AI governance effectiveness evolves over time as organizations mature in their AI adoption journeys.

11. Explore Cross-Country Comparisons
Comparative studies between developed and emerging economies can reveal contextual differences in AI governance practices and employee outcomes.

12. Investigate Additional Mediators and Moderators
Future research may examine:

- Organizational culture
- Leadership support
- AI trust
- Employee digital competence
- Ethical climate

As factors influencing the relationship between AI governance and organizational outcomes.

Conclusion

The rapid integration of Generative Artificial Intelligence (Gen AI) into organizational processes has created unprecedented opportunities for innovation, efficiency, and knowledge creation. However, alongside these benefits, organizations are increasingly confronted with challenges related to governance, unauthorized AI usage, employee well-being, and risk management. This study examined the interrelationships among Generative AI Governance Mechanisms, Algorithmic Shadow IT, Work–Life Balance, and Organizational Risk Management through a human-centered governance perspective.

The findings demonstrate that effective AI governance mechanisms play a critical role in reducing the prevalence of algorithmic shadow IT while simultaneously enhancing employee work–life balance and strengthening organizational risk management capabilities. The results further reveal that algorithmic shadow IT serves as an important mediating factor, linking governance practices to both employee and organizational outcomes. Employees who engage in unauthorized AI usage are more likely to experience blurred work–life boundaries, increased digital stress, and cognitive overload, while organizations face heightened risks related to data security, privacy, compliance, and reputation.

The study contributes to the emerging literature on AI governance by extending traditional governance and risk management perspectives beyond technical and regulatory concerns. It introduces a holistic framework that integrates behavioral, technological, and organizational dimensions, emphasizing that responsible AI governance should address not only compliance requirements but also employee well-being and sustainable work practices. By positioning work–life balance as a key outcome of AI governance, the study broadens current understanding of the human implications of Gen AI adoption.

From a practical standpoint, the findings suggest that organizations should establish comprehensive AI governance frameworks, promote AI literacy, integrate AI oversight into enterprise risk management systems, and develop digital well-being initiatives that support employees in AI-enabled work environments. Such measures can help organizations balance innovation with accountability while fostering a healthy and productive workforce.

Despite its contributions, the study is limited by its cross-sectional design and reliance on self-reported data. Future research should employ longitudinal and mixed-method approaches to explore the evolving nature of AI governance and its long-term effects on employee behavior and organizational performance. Further investigations across industries and national contexts would also enhance the generalizability of findings.

In conclusion, as Generative AI continues to reshape the future of work, effective governance will become a strategic necessity rather than a regulatory obligation. Organizations that adopt human-centered AI governance approaches will be better equipped to manage algorithmic shadow IT, safeguard employee well-being, and build resilient risk management systems. Ultimately, the sustainable success of AI-driven organizations will depend not only on technological advancement but also on their ability to govern AI responsibly, ethically, and in alignment with human values.

REFERENCES

1. Hadley, E., Blatecky, A., & Comfort, M. (2025). *Investigating algorithm review boards for organizational responsible artificial intelligence governance.* AI and Ethics. https://doi.org/10.1007/s43681-024-00574-8
2. Janssen, M. (2025). *Responsible governance of generative AI: Conceptualizing Gen AI as complex adaptive systems.* Policy and Society. https://doi.org/10.1093/polsoc/puae040
3. 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. https://doi.org/10.1016/j.techfore.2026.124697
4. Responsible Artificial Intelligence Governance: A Review and Research Framework. Journal of Strategic Information Systems. https://doi.org/10.1016/j.jsis.2024.101885
5. Enabling Affordances for AI Governance. Journal of Responsible Technology. https://doi.org/10.1016/j.jrt.2024.100086
6. Ashforth, B. E., Kreiner, G. E., & Fugate, M. (2000). All in a day’s work: Boundaries and micro role transitions. *Academy of Management Review, 25*(3), 472–491. https://doi.org/10.5465/amr.2000.3363315
7. Barber, L. K., & Santuzzi, A. M. (2015). Please respond ASAP: Workplace telepressure. *Organizational Psychology Review, 5*(1), 172–194. https://doi.org/10.1177/2041386614528807
8. Derks, D., van Duin, D., Tims, M., & Bakker, A. B. (2014). Smartphone use and work–home interference. *Computers in Human Behavior, 36*, 52–60. https://doi.org/10.1016/j.chb.2014.03.001

9. Floridi, L., et al. (2018). AI 4 People - Ethical framework for AI. *Minds and Machines, 28*, 689–707. https://doi.org/10.1007/s11023-018-9482-5
10. Hadley, E., et al. (2024). Algorithm review boards for AI governance. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00574-8
11. Kaplan, A., & Haenlein, M. (2019). Siri, Siri in my hand. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004
12. Ransbotham, S., et al. (2017). Artificial intelligence in business. *MIS Quarterly Executive*, *16*(4), 1–17.
13. Schneckenberg, D., et al. (2015). Organizational drivers of shadow IT. *Journal of Information Technology*.
14. Sebastian, G. (2026). Digital shadow AI risk theory (DART). *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2026.124697
15. Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress. *Journal of Management Information Systems, 24*(1), 301–328. https://doi.org/10.2753/MIS0742-1222240109
16. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
17. Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108
18. Davis, F. D. (1989). Perceived usefulness and perceived ease of use. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008
19. Fisher, G. G., Bulger, C. A., & Smith, C. S. (2009). Beyond work and family. *Journal of Occupational Health Psychology, 14*(4), 441–456. https://doi.org/10.1037/a0016735
20. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.
21. Klotz, A. C., et al. (2018). Shadow IT in organizations. *Information Systems Journal*.
22. Mikes, A., & Kaplan, R. S. (2015). Managing risks by design. *Management Accounting Research*.
23. Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management. *Academy of Management Review*. https://doi.org/10.5465/amr.2018.0072
24. Renn, O. (2008). *Risk governance*. Springer. https://doi.org/10.1007/978-1-4020-6799-0
25. Trist, E. L., & Bamforth, K. W. (1951). Sociotechnical systems. *Human Relations, 4*(1), 3–38. https://doi.org/10.1177/001872675100400101
26. Valcour, P. M. (2007). Work-based resources and work–life balance. *Journal of Vocational Behavior*, *71*(2), 215–225. https://doi.org/10.1016/j.jvb.2007.04.005
27. Ashforth, B. E., et al. (2000). Boundary theory. *Academy of Management Review*. https://doi.org/10.5465/amr.2000.3363315
28. Derks, D., et al. (2014). Smartphone use and work interference. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2014.03.001
29. Hair, J. F., et al. (2019). *Multivariate data analysis*. Cengage.
30. Kaplan, A., & Haenlein, M. (2019). AI in business. *Business Horizons*. https://doi.org/10.1016/j.bushor.2018.08.004
31. Ransbotham, S., et al. (2017). AI in organizations. *MIS Quarterly Executive*.
32. Renn, O. (2008). *Risk governance*. Springer. https://doi.org/10.1007/978-1-4020-6799-0
33. Schneckenberg, D., et al. (2015). Shadow IT behavior. *Journal of Information Technology*.
34. Sebastian, G. (2026). Digital shadow AI risk theory. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2026.124697
35. Tarafdar, M., et al. (2007). Technostress model. *MIS Quarterly*. https://doi.org/10.2307/25148716

36. Trist, E. L., &Bamforth, K. W. (1951). Sociotechnical systems. *Human Relations*. https://doi.org/10.1177/001872675100400101
37. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., &Vayena, E. (2018). AI 4 People - An ethical framework for a good AI society. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
38. Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review, 46*(1), 192–210. https://doi.org/10.5465/amr.2018.0072
39. Janssen, M. (2025). Responsible governance of generative AI systems. *Policy and Society, 44*(1), 38–55. https://doi.org/10.1093/polsoc/puae040
40. Hadley, E., Blatecky, A., & Comfort, M. (2024). Algorithm review boards for responsible AI governance. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00574-8
41. Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector. *International Journal of Public Administration, 42*(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103
42. Dwivedi, Y. K., et al. (2021). Artificial intelligence (AI): Multidisciplinary perspectives. *International Journal of Information Management, 57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.05.002
43. Schneckenberg, D., Wagner, H. T., & Hambley, L. (2015). Organizational drivers of shadow IT usage. *Journal of Information Technology*. https://doi.org/10.1057/jit.2015.3
44. Klotz, A. C., Wheeler, A. R., Halbesleben, J. R., & Buckley, M. R. (2018). Shadow IT in organizations: Behavioral antecedents. *Information Systems Journal*. https://doi.org/10.1111/isj.12165
45. Sebastian, G. (2026). Digital shadow AI risk theory (DART). *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2026.124697
46. Behrens, S. (2009). Shadow systems in organizations. *Communications of the ACM, 52*(2), 128–130. https://doi.org/10.1145/1461928.1461960
47. Györy, A., Cleven, A., &Uebernickel, F. (2012). Shadow IT management. *Business & Information Systems Engineering, 4*(6), 323–329. https://doi.org/10.1007/s12599-012-0222-7
48. Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress. *MIS Quarterly, 31*(2), 303–328. https://doi.org/10.2307/25148716
49. Derks, D., van Duin, D., Tims, M., & Bakker, A. B. (2014). Smartphone use and work–home interference. *Computers in Human Behavior, 36*, 52–60. https://doi.org/10.1016/j.chb.2014.03.001
50. Barber, L. K., & Santuzzi, A. M. (2015). Workplace telepressure. *Organizational Psychology Review, 5*(1), 172–194. https://doi.org/10.1177/2041386614528807
51. Ashforth, B. E., Kreiner, G. E., & Fugate, M. (2000). Boundary theory. *Academy of Management Review, 25*(3), 472–491. https://doi.org/10.5465/amr.2000.3363315
52. Valcour, P. M. (2007). Work-based resources and work–life balance. *Journal of Vocational Behavior, 71*(2), 215–225. https://doi.org/10.1016/j.jvb.2007.04.005
53. Fisher, G. G., Bulger, C. A., & Smith, C. S. (2009). Beyond work and family. *Journal of Occupational Health Psychology, 14*(4), 441–456. https://doi.org/10.1037/a0016735
54. Kaplan, A., & Haenlein, M. (2019). Siri, Siri in my hand. *Business Horizons, 62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004
55. Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Springer. https://doi.org/10.1007/978-1-4020-6799-0
56. Mikes, A., & Kaplan, R. S. (2015). Managing risks by design. *Management Accounting Research*. https://doi.org/10.1016/j.mar.2015.06.003

57. Ransbotham, S., Kiron, D., Gerbert, P., & Reeves, M. (2017). Artificial intelligence in business. *MIT Sloan Management Review.*
58. NIST (2023). AI Risk Management Framework. National Institute of Standards and Technology. https://www.nist.gov/ai-risk-management-framework
59. Trist, E. L., & Bamforth, K. W. (1951). Sociotechnical systems theory. *Human Relations, 4*(1), 3–38. https://doi.org/10.1177/001872675100400101
60. Orlikowski, W. J. (1992). The duality of technology. *Organization Science, 3*(3), 398–427. https://doi.org/10.1287/orsc.3.3.398
61. Ajzen, I. (1991). Theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
62. Davis, F. D. (1989). Technology acceptance model. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008
63. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of IT. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540
64. Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., &Venkatraman, N. (2013). Digital business strategy. *MIS Quarterly, 37*(2), 471–482.
65. Sebastian, I. M., et al. (2017). How big data transforms organizations. *MIS Quarterly Executive, 16*(2), 103–123.
66. Zhang, B., & Dafoe, A. (2019). Artificial intelligence and governance. *Nature Machine Intelligence, 1*, 20–24. https://doi.org/10.1038/s42256-018-0005-0
67. Tambe, P., Cappelli, P., & Yakubovich, V. (2019). Artificial intelligence in human resources. *Academy of Management Journal*.
68. Lee, I. (2018). AI in the workplace. *Business Horizons, 61*(4), 603–610.
69. Brynjolfsson, E., & McAfee, A. (2017). *Machine, platform, crowd*. W.W. Norton.