IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 April 2025, accepted 13 May 2025, date of publication 19 May 2025, date of current version 27 May 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3571537

RESEARCH ARTICLE

Relationships Among Organizational-Level Maturities in Artificial Intelligence, Cybersecurity, and Digital Transformation: A Survey-Based Analysis

BURAK KUBILAY AND BARIS CELIKTAS
Computer Science Engineering Department, Işik University, 34398 Istanbul, Türkiye
Corresponding author: Burak Kubilay (23SIBE5012@isik.edu.tr)

ABSTRACT The rapid development of digital technology across industries has highlighted the growing need for enhanced competencies in Artificial Intelligence (AI), Cyber security (CS), and Digital Transformation (DT). While there is extensive research on each of these domains in isolation, few studies have investigated their relationship and joint impact on organizational maturity. This study aims to address this gap by analyzing the relationships among the maturity levels of AI, CS, and DT at the organizational level using Structural Equation Modeling (SEM) and descriptive statistical methods. A mixed-methods design combines quantitative survey data with synthetic modeling techniques to assess organizational preparedness. The findings demonstrate significant bidirectional correlations among AI, CS, and DT, with technology and finance being more advanced than government and education. The research highlights the necessity of an integrated AI-CS strategy and provides actionable recommendations to increase investments in these domains. In contrast to the preceding fragmented evaluations, the current research establishes a comprehensive, empirically grounded framework that acts as a strategic reference point for digital resilience. Follow-up studies will involve collecting real-world industry data in support of empirical validation and predictive ability in measuring AI and CS maturity. This research adds to the existing literature by filling the gaps among fragmented digital maturity models and providing a consistent empirical base for organizations to thrive in an evolving technological environment.

INDEX TERMS Artificial intelligence, cybersecurity, digital resilience, digital transformation, organizational maturity.

I. INTRODUCTION

In the current era of rapid digitalization, organizations across varied industries are increasingly relying on AI, CS, and DT to sustain their competitive edge, guarantee business continuity, and realize strategic triumph [1], [2], [3]. Each of the three areas has been a key enabler of innovation and business success. Nevertheless, the level of maturity expressed by organizations in adopting and integrating the technologies is considerably disparate across industries, geographical regions, and organizational sizes. This gap is defined by such determinants as strategic alignment, infrastructure readiness, leadership characteristics, and governance culture [3], [4], [5]. Organizational maturity is the degree to which an organization is ready, capable, and competent to exploit emerging technologies to achieve defined business goals [6]. AI maturity (AIM) encompasses not just the technical deployment of AI, but also its strategic, ethical, and operational inclusion in decision systems [4], [7]. Cybersecurity maturity (CSM) deals with the processes of risk management, threat detection, and incident response planning for protecting digital assets and maintaining business continuity [8], [9]. Digital transformation maturity (DTM), on the other hand, means the capability of an organization to adopt digital strategies, upgrade its infrastructure, increase automation, and develop a culture of prioritizing digital initiatives [10], [11], [12], [13], [14], [15]. Despite the growing importance of these factors, existing literature often examines AI adoption [4], computer science models [3], [8], and DT approaches [16], [17] separately. Although previous studies habitually examine

The associate editor coordinating the review of this manuscript and approving it for publication was Mostafa M. Fouda.

TABLE 1. Comparison of existing maturity models and identified shortcomings.

Model / Research Paper	Siloed Approaches	Lack of Empirical Validation	Limited Exploration of Interdependencies	Industry-Specific Insights
Our Study				
Deloitte Digital Maturity Model (DMM) [10]	✓			
Gartner AI Maturity Model [12]	✓			
Zhu et al. (2025) [13]	✓		✓	
Zakiuddin et al. (2024) [15]	✓		✓	
ISO 42001 [23]	✓			
ISO 27001 [24]	✓	✓		
NIST Cybersecurity Framework (CSF) [25]	✓	✓		
CMMI Institute (2018) [26]	✓	✓		
Capgemini Digital Mastery Framework [27]	✓			
Westerman et al. (2014) [28]	✓		✓	✓
Blondiau et al. (2016) [29]	✓		✓	
Gölzer & Fritzsche (2017) [30]	✓		✓	✓
Teichert (2024) [31]	✓		✓	
Lee et al. (2024) [32]	✓		✓	✓
Chen et al. (2024) [33]		✓	✓	
Cammarano et al. (2024) [34]		✓	✓	
Zhu et al. (2024) [35]		✓	✓	✓
Jäkel et al. (2024) [36]			✓	✓

Note: A checkmark (✓) indicates that the corresponding study exhibits the specified limitation. Our study overcomes these shortcomings, and thus no checkmarks are shown for it.

these fields separately [18], [19], [20], [21], a significant gap remains in understanding their interdependencies and the organizational determinants—including industry, geographical location, and organizational size—that together influence maturity levels [5], [6]. Furthermore, while standards such as ISO 42001 for AI management, ISO 27001 for CS, and COBIT for IT governance provide structured frameworks, their combined impact on organizational maturity is poorly investigated [5], [6], [13].

To address this gap, this study provides a comprehensive assessment of organizational maturity in AI, CS, and DT. To bridge the identified research gap and guide the empirical analysis, this study establishes the following research objectives:

1) Determine the degree of maturity for AI, CS, and DT in organizations.
2) Analyze the interactions and synergies among AI, CS, and DT maturity domains.
3) Examine the impact of organizational factors, including size, industry, and geographical location, on maturity levels.
4) Discuss the significance of adherence to recognized standards, such as ISO 42001 and ISO 27001, on organizational maturity outcomes.

A mixed-methods design is employed, combining quantitative survey data with qualitative findings to enable a detailed exploration of organizational readiness [22]. The study also incorporates qualitative insights extracted from open-ended survey responses, complementing the structured survey data for a holistic organizational maturity evaluation.

The study makes important contributions to academic and practitioner communities by providing a consolidated maturity model and actionable guidelines for organizations looking to develop their AI, CS, and DT capabilities [5], [6].

II. RELATED WORKS

A number of maturity models have been proposed to assess AI, CS, and DT maturity. However, these models fail to provide an integrated perspective because of their isolation, lack of empirical support, limited investigation of interdependencies, and sparse industry-specific findings. Table 1 illustrates prominent limitations in existing frameworks.

A. SILOED APPROACHES

Many maturity models assess AI, CS, or DT independently, failing to consider their interdependence and combined impact on organizational strategy; a number of widely used frameworks are characteristic of this limitation. Deloitte Digital Maturity Model (DMM) [10] is focused on DT but not specifically on AI governance or CS concerns, while the Gartner AI Maturity Model [12] is focused on AI adoption but not on CS threats or DT considerations. In addition, Zhu et al. [13] discusses DT maturity in organizations but does not fully integrate AI and CS into its evaluation framework, and Zakiuddin et al. [15] is primarily on DT of services in the public sector but lacks a systematic AI-CS-DT integration process. Moreover, ISO 42001 [23] provides AI governance standards but does not deal with CS threats or DT infrastructure, whereas ISO 27001 [24] deals with CS controls but not with AI governance or DT concerns. Likewise, NIST CSF [25] offers a risk-based approach to CS but excludes AI risk or DT factors, and CMMI Institute (2018) [26] deals with process maturity but not with AI-specific security threats or CS advancements. Furthermore, Capgemini Digital Mastery Framework [27] evaluates DT capabilities but lacks an AI-CS integration model, while Westerman et al. [28] addresses business transformation but without including AI-induced CS threats. Similarly, Blondiau et al. [29] addresses a hospital-focused maturity model that cannot be applied across industries, and

Gölzer and Fritzsche [30] accounts for data-driven maturity in manufacturing but without considering AI or CS aspects. Additionally, Teichert [31] assesses service provider maturity but not AI-CS dependencies, and Lee et al. [32] assesses DT maturity in manufacturing but not a formal AI-CS integration model. Lacking an end-to-end AI-CS-DT perspective, these models are unable to offer one unified maturity measure, leading to fragmented decision-making and unsuccessful DT efforts.

B. LACK OF EMPIRICAL VALIDATION

Many maturity models are well recognized and conceptually strong but lack empirical validation to demonstrate their efficacy in practical application in AI-CS-DT integration, and most such frameworks have never been rigorously tested in various industries, with knowledge gaps in practice.ISO 27001 [24] and NIST CSF [25] are being broadly applied in industry, yet there is limited empirical research on their effectiveness in countering AI-driven threats. While these frameworks are extensively used by organizations for compliance, their use in AI-CS-DT maturity is yet to be studied extensively in scholarly literature. CMMI Institute (2018) [26] is process maturity and organizational capability focused but lacks empirical validation for AI or DT incorporation, and Chen et al. [33] offers a probabilistic optimization model for DT maturity assessment but lacks industry testing in real-world settings for validation of effectiveness. Cammarano et al. [34] explains how the adoption of DT affects business strategy but without empirical validation in a number of industries, whereas Zhu et al. [35] proposes a construction industry-specific DT maturity model, although no comprehensive tests have been conducted to validate its adaptability in different industry contexts. In order to provide feasibility for practical application, it is essential that future maturity models are validated using real case studies with different industries, geographical regions, and organizational setups. Furthermore, empirical validation will refine these models towards more accurate estimation of AI-CS-DT maturity according to real business requirements and regulatory needs.

C. INSUFFICIENT ANALYSIS OF INTERRELATIONS

Although a few maturity models try connecting AI, CS, and DT, they do not incorporate their interrelations into a combined framework. Furthermore, an overwhelming majority of the models concentrate on one or two domains without striving to establish a holistic relationship among AI, CS, and DT, thereby restricting their potential in guiding organizations through complete digital maturity. Zhu et al. [13] recognizes the relationship between DT and organizational resilience but does not develop an integral AI-CS-DT integration model, not dealing with CS threats, while Zakiuddin et al. [15] deals with the application of AI in digital service automation but does not incorporate CS concerns in its model. Westerman et al. [28] stresses the need for alignment among AI, CS, and DT but lacks a formal governance structure for digitalization-based security threats, and Blondiau et al. [29] describes how DT maturity improves operational efficiency but does not model AI or CS dependence in its investigation. Gölzer and Fritzsche [30] recognizes data security as a challenge for DT but fails to provide an AI-CS-DT integration strategy, while Teichert [31] takes into account organizational governance as an aspect of DT but fails to investigate the impact of AI adoption on CS risks or the effect of CS practices on DT success. Chen et al. [33] uses probabilistic analysis on DT maturity assessment but fails to connect AI governance and CS frameworks, whereas Lee et al. [32] explores AI applications for smart factories but treats CS as a standalone problem rather than an integrated one. Cammarano et al. [34] analyze how business strategy is influenced by the uptake of DT but omits AI-based security considerations, and Jäkel et al. [36] analyzes AI and CSM in the construction industry but lacks a framework of formal governance for AI-CS deployment. Zhu et al. [35] recognizes the need for a holistic AI-CS-DT maturity model but does not provide a formal implementation strategy to guide organizations in its successful implementation. To develop a complete AI-CS-DT maturity model, organizations need a structured approach that acknowledges the dynamic interdependencies between AI adoption, CS vulnerabilities, and DT infrastructure, and without it, existing models are incomplete and fragmented, leaving gaps in risk management, compliance, and strategic decision-making.

D. INDUSTRY-SPECIFIC INSIGHTS

While there exist some industry-specific maturity models, most of them are still too generic to address sector-specific risks, regulation concerns, and operational intricacies, and industry-specific models give more concrete guidance but typically do not combine AI, CS, and DT in a systematic manner. Westerman et al. [28] provides real business cases in finance, healthcare, and retail, showing how companies implement DT strategies. But it does not address AI governance or CS risk management specifically, so it is less applicable to AI-based businesses, while Gölzer, and Fritzsche [30] provides a manufacturing-focused, data-driven operations model, integrating AI with industrial automation. But it lacks a formal CS framework, so AI-based security threats are not addressed. Lee et al. [32] investigates AI, CS, and DT in manufacturing environments, recognizing the role of CS in smart factories. However, it does not comprehensively discuss governance models that would enable organizations to embrace AI-CS-DT maturity in a practical manner. Furthermore, Jäkel et al. [36] assesses DT maturity in the construction sector, laying emphasis on industry-specific challenges without considering AI-based risk management or CS considerations in the context of smart construction ecosystems. Zhu et al. [35] presents a construction-specific maturity model incorporating AI and CS dimensions in DT programs, and while it gives a more specialized solution, it still lacks a complete AI-CS-DT

governance framework ready to be applied in practice. Finance, healthcare, and smart manufacturing sectors require tailored AI-CS-DT frameworks due to regulatory constraints, risk exposure, and automation complexity. However, existing maturity models often fail to provide sector-specific recommendations. To provide greater relevance to industries, future maturity models should be customized to specific industries, incorporating AI governance, CS risk, and regulatory compliance frameworks that address the unique requirements of each sector, as a one-size-fits-all approach to AI-CS-DT maturity fails to adequately address the specific challenges of DT in various industries, therefore necessitating more focused digital maturity assessments. Despite the fact that the constraints recognized in current maturity models underscore significant weaknesses in AI-CS-DT integration, their weaknesses must be addressed using a solid theoretical base. To create a comprehensive evaluative framework, we rely on three proven theoretical lenses offering systematic explanations of the processes through which organizations build digital competencies, reconcile technology with human factors, and react to external pressures: Dynamic Capabilities Theory (DCT), Socio-Technical Systems (STS) Theory, and the Technology-Organization-Environment (TOE) Framework [37], [38], [39], [40], [41], [42], [43].

One such significant view is the Dynamic Capabilities Theory (DCT) as put forward by Teece et al., which describes how organizations create, absorb, and reconfigure their internal and external capabilities to answer changing environments rapidly [37].

This theory is particularly relevant to AI-CS-DT maturity since the organisations must continuously adapt to emerging digital threats, evolving cyber threats, and AI-driven operational changes. Teece extended this theoretical foundation by highlighting mechanisms through which companies can establish competitive advantages by their dynamic capabilities for sensing, seizing, and transforming [38]. Building upon these foundations, Teece further emphasized the role of business models as dynamic capabilities themselves, illustrating how strategic adjustments in business models enable organizations to reconfigure their assets and operations in response to technological and market shifts [39]. Emerging research, such as Al-Moaid and Almarhdi, sheds light on the real-world implementation of dynamic capabilities in DT programs. Their paper underscores the significance of change management as a mediator for the successful execution of DT programs, specifically within the telecommunications industry [44].

This resonates with the DCT argument that companies have to update their strategic competences in light of technological shocks so as to adapt to such shocks successfully. Under this paradigm, an AI-CS-DT maturity model ought to reflect companies' capacity for upgrading their technology resilience, CS strategy, and AI embrace on a dynamic basis. A further key vantage point is the Socio-Technical Systems (STS) Theory, which highlights the dynamic relationship between technical and social aspects within companies. This paradigmatic theory guarantees that AI, CS, and DT maturity frameworks achieve a balance between technological innovation and workforce flexibility. Originally formulated by Trist and Bamforth [40], STS Theory examined the effects of technological change on human elements and thus laid the groundwork for existing AI regulation and CS frameworks. Extending this view, Bostrom and Heinen [41] focused on IT system deficiencies due to insufficient socio-technical integration. Successful AI-CS-DT models must incorporate STS principles to ensure AI-driven security, DT strategy, and employee engagement plans are harmonized for sustainable organizational resilience. Beyond organizational factors, the Technology-Organization-Environment (TOE) Framework provides a broader perspective for AI, CS, and DT adoption.

First proposed by Tornatzey and Fleischer [42], TOE describes technology readiness, organizational structure, and pressures from outside that influence the adoption of innovations.

Baker [43] extended this, using TOE to apply to information systems, with particular emphasis on regulation and competition. Maturity in AI-CS-DT is contingent upon internal IT capabilities, leadership, and regulatory environments externally. The application of TOE principles assists organizations in aligning AI governance, CS strategies, and DT for industry-specific, sustainable transformation.

Additionally, the Resource-Based View (RBV) theory offers a valuable complementary perspective, positing that organizational resources—such as AI and CS capabilities—are critical for achieving and sustaining competitive advantage. In the context of AI-CS-DT maturity, these digital competencies can be regarded as strategic assets that organizations must develop and leverage to drive successful transformation initiatives [5].

Drawing on these theoretical contributions, this study develops an integrated AI-CS-DT maturity assessment model that not only reflects cross-domain interrelationships but also includes empirical validation and industry-based guidelines. By addressing the shortcomings of current maturity models, this model offers a more systematic and holistic approach to measuring AI, CS, and DT maturity in diverse organizational settings.

III. PRELIMINARIES

Growing reliance on digital technologies renders it essential to gauge organizational maturity in AI, CS, and DT. Maturity models offer a structured way to measure readiness, adoption, and success. In this section, we formalize these constructs, developing a theoretical basis for investigating their interdependencies and impacts on organizational success.

A. AI MATURITY

AI has emerged as a disruptive technology that is impacting industries worldwide [2], [4], [7], [19], [21]. AIM refers to the degree to which organizations strategically take up and accept AI into their activities, processes, and decision-making [15]. Although there are a few organizations that are at the forefront

of leveraging AI for competitive advantage, the majority are in the early phases of adoption [3], [4], [23], [25]. The Gartner AIM Model is an often-quoted framework that outlines five phases of AIM: Awareness, Active, Operational, Systemic, and Transformational. The model emphasizes the importance of strategic alignment, data readiness, and organizational change management as key factors to achieve higher maturity levels [12]. Furthermore, Rogers' Innovation Diffusion Theory provides a conceptual framework that enables the understanding of the process of AI adoption in organizational settings. The theory highlights the significance of innovators, early adopters, and laggards in defining the shape of the adoption curve and affecting the maturation of organizations [1], [5], [41], [43]. Capability Maturity Models (CMMs) provide a formal method for determining an organization's readiness and ability regarding AI adoption. These frameworks focus on incremental improvement along people, process, technology, and data governance dimensions [4], [6], [23], [25], [26]. Recent directions in AIM include incorporation of ethical AI principles, XAI adoption, and edge AI technologies [7], [19], [20], [21], [25]. As AI systems become more complex, organizations will need to prioritize transparency, accountability, and inclusivity in AI endeavors [7], [19], [21], [23], [25].

AIM is a central aspect of organizational competitiveness in the era of digitalization [4], [21]. Organisations can indeed unlock the potential of AI through building their capabilities in data readiness, leadership, and ethical governance [1], [4], [7], [23], [25]. Maturity, however, requires surmounting significant challenges in the form of resistance to change and paucity of resources [1], [5], [6], [12], [21]. Strategic alignment, underpinned by a systemic and dynamic capabilities perspective, is increasingly critical for organizations aiming to embed AI technologies across their operations [1], [4], [5], [21], [37], [38], [39]. Understanding the maturity of AI requires a structured evaluation process that addresses different dimensions of an organization's AI capabilities.

B. CYBERSECURITY MATURITY (CSM)

CSM is the capacity of an organization to identify, protect, detect, respond to, and recover from cyber threats based on structured frameworks such as ISO 27001, the NIST Cybersecurity Framework (CSF), and CIS Controls [3], [8], [9], [24], [25]. More mature levels involve risk-informed security practices, automated threat detection capabilities, and continuous process improvement [3], [8], [9], [24], [25]. Numerous models exist to measure an organization's CS proficiency. For instance, the NIST CSF categorizes security functions into five groups: Identify, Protect, Detect, Respond, and Recover [8], [9], [25]. ISO/IEC 27001 focuses on risk-based security management and compliance [3], [24]. The US Department of Energy's C2M2 model assesses five levels of CSM [8], [9]. CSM is assessed by organizations with adherence to standards (ISO 27001, NIST 800-53, GDPR) [3], [8], [9], [24], [25]. Further, key performance indicators like threat detection time (TTD) and threat response time (TTR) are used to quantify security effectiveness. The increased use of AI-powered security products significantly improves the capacity to track and counter threats in real-time [5], [23].

C. DT MATURITY

Various maturity models have been developed to gauge the level of DT of an organization. The Deloitte Digital Maturity Model recognizes five stages of digital maturity: Initial – Isolated digital initiatives; Emerging – Cross-functional collaboration limited; Integrated – Digital strategy alignment across departments; Optimized – DT enterprise-wide; and Innovative – Continuous evolution through AI, automation, and data analytics [10]. Westerman et al. have developed the Digital Mastery Framework which classifies organizations into Beginners – Low digital intensity, traditional business models; Conservatives – Robust IT governance and low digital innovation; Fashionistas – High digital usage but low strategic alignment; and Digital Masters – Organizations that utilize technology efficiently to drive strategic impact [28]. MIT Sloan Digital Maturity Model is a widely adopted model categorizing firms based on their leadership's digital vision, digital capabilities, and operational transformation [11].

There are various factors that affect an organization's digital maturity. C-level commitment (CEO, CIO, CTO) and strategic investment are key to DT success. Digital leadership that is proactive fosters agility, allowing firms to adopt new technologies like AI, cloud computing, and automation [1], [5], [11], [21], [27]. Firms that are digital-first in their culture enjoy higher usage of digital technologies [5]. Organizations that are change-averse are confronted with legacy systems, silos internally, and competency gaps. DTM requires cloud computing, big data analytics, and automation based on AI. Companies that are successful in leveraging these technologies manage to overcome transformation barriers and emerge as competitive players in digital markets [1], [5], [11], [21], [27]. Organizations that are data-driven and possess real-time analytics capabilities are more responsive and competitive. Domains like finance, health, and defense are under strict regulatory requirements (e.g., GDPR, ISO 27001) that impact digital maturity [5], [24]. Highly regulated domains must reconcile innovation with CS and risk management.

IV. METHODOLOGY

This research uses a mixed-methods design to evaluate AIM, CSM, and DTM's organizational maturity. The study adopts various approaches to analysis, including:

- **Quantitative Survey Analysis** – Likert scale surveys were employed for measuring maturity levels [4], [6], [9], [22], [27].
- **Synthetic Data Generation** – The real responses were augmented with statistically generated data to enhance robustness. The technique is widely used in AI-driven analytics, CS modeling, and DTM assessment to enhance dataset reliability and generalizability.

Research highlights that synthetic data augmentation enhances privacy protection, reduces bias, and enriches predictive modeling in structured assessment [22].

- **Inferential Analysis** – Used to determine correlations, interdependencies, and cause-and-effect. The method is being extensively applied in research on DT, CS, and AI governance to reveal statistical interdependencies and forecast findings. Literature emphasizes that inferential methods such as regression analysis, ANOVA, structural equation modeling (SEM), and moderation and mediation analyses are essential to ascertain digital maturity frameworks and examine the consequences of strategic decision-making [1], [3], [5], [9], [22].
  - **SEM** – Used to estimate direct, indirect, and total effects of AIM, CSM, and DTM.
  - **Moderation and Mediation Analyses** – Conducted to examine the moderating roles of industry and location factors and whether CSM mediates the AI-DT relationship.
- **Thematic Qualitative Analysis** – Open-ended responses were analyzed thematically to capture qualitative patterns in organizational maturity perspectives, enriching the quantitative analysis.

A. RESEARCH HYPOTHESES

Based on theoretical foundations in AI adoption, CSM, and DT models, the following hypotheses are developed to structure the research model. The hypotheses capture direct influences, mediation mechanisms, and moderation effects among organizational maturity dimensions.

Direct Effects: First, we hypothesize direct relationships between AIM, CSM, and DTM:

- **H1**: AIM positively influences CSM, suggesting that advanced AI adoption enhances CS practices.
- **H2**: AIM positively influences DTM, indicating that AI capability development supports broader DT initiatives.
- **H3**: CSM positively influences DTM, reflecting that stronger CS frameworks facilitate secure DT.

Mediation Effect: Given CS's critical role as an enabler in digital ecosystems, we propose that CSM mediates the relationship between AIM and DTM:

- **H4**: CSM mediates the relationship between AIM and DTM, acting as a bridge that connects AI adoption efforts with successful DT.

Moderation Effects: Furthermore, recognizing that organizational context can shape maturity pathways, we hypothesize that industry and regional factors moderate key relationships:

- **H5**: The impact of AIM on DTM is moderated by industry sector, such that different sectors (e.g., technology vs. government) experience varying strengths in this relationship.
- **H6**: The impact of CSM on DTM is moderated by geographical region, acknowledging regional disparities in digital infrastructure and CS policies.

The conceptual research model is illustrated in Figure 1, and Table 2 lists the derived hypotheses. SEM was applied to test the direct effects, mediation pathways, and moderation influences hypothesized among organizational maturity dimensions.

TABLE 2. Research hypotheses.

H_N	Statement
H1	AIM positively influences CSM.
H2	AIM positively influences DTM.
H3	CSM positively influences DTM.
H4	CSM mediates the relationship between AIM and DTM.
H5	The impact of AIM on DTM is moderated by industry sector.
H6	The impact of CSM on DTM is moderated by geographical region.

B. SURVEY DEVELOPMENT AND DATA COLLECTION

The survey instrument was developed to quantify organizational maturity in AI, CS, and DT based on existing frameworks and industry benchmarks. The questions were formulated from scholarly research and globally accepted models to render a structured evaluation.

In addition to structured Likert-scale questions, participants were encouraged to provide open-ended responses describing their maturity experiences, allowing for qualitative thematic extraction during analysis.

The survey structure in Table 3 assesses AI maturity by combining proven models [4], [5], [7], [12], a multi-domain reference [21], known standards [23], and formal frameworks [25]. AI adoption requires strategic alignment with business objectives, as emphasized in DTM and AIM Models [5], [12]. AI effectiveness requires a good data management foundation, which is one of the key elements of AI Capability Maturity Models [4]. Likewise, infrastructure readiness determines if organizations possess appropriate technological foundations to support AI initiatives [5], [12]. The ability to attract and develop AI talent is another fundamental driver, explored in a multi-domain AI, CS, and DT framework [21]. Good governance policies offer control and accountability, drawing on the AI Ethics Maturity Model [7]. Organizations, meanwhile, must integrate ethical AI practices to ensure fairness and transparency, in line with risk management principles [25]. A mature AI organization also activates a wide range of AI applications, implementing AI in many business processes, as described in the AI Capability and Digital Maturity Models [4], [12]. Moreover, performance measurement is essential to assess the contribution of AI, complemented by structured risk management practices [25]. Lastly, adherence to AI standards, e.g., ISO/IEC 42001 [23], offers an internationally accepted basis for AI governance and risk management. By integrating these perspectives, organizations can systematically assess their AI maturity and facilitate successful, responsible AI adoption.

CSM, as presented in Table 4, evaluates the CSM of an organization based on well-known CSM frameworks [8], [9], [26], risk management standards [25], [27], international standards [24], and views on future security trends like AI,

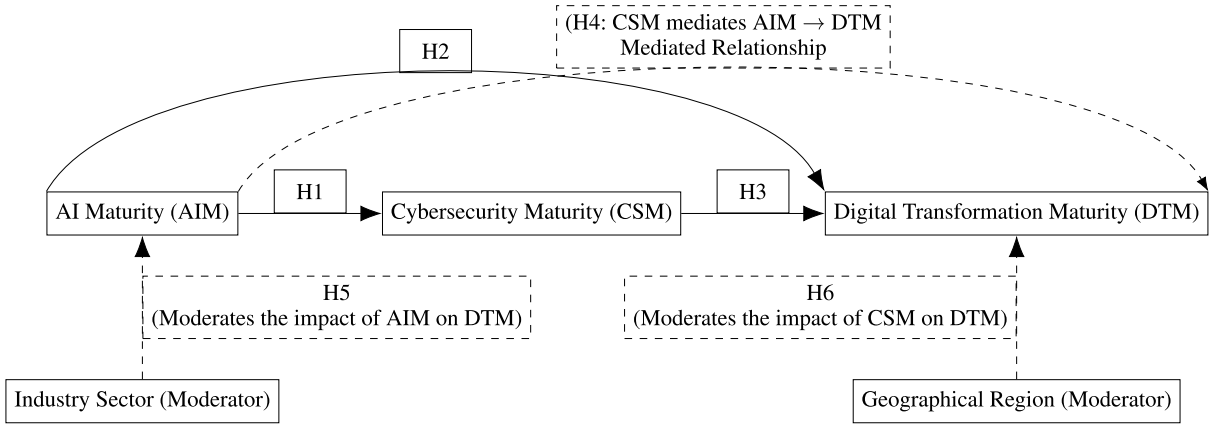

FIGURE 1. Conceptual model of hypotheses.

TABLE 3. AIM survey questions and research references.

Survey Question	References
Our organization has a documented AI strategy that aligns with overall business objectives.	[5], [12]
Our organization effectively manages and utilizes data for AI projects, ensuring data quality, accessibility, and governance.	[4]
Our organization has the necessary technology and infrastructure to support AI development and deployment.	[5], [12]
Our organization attracts, develops, and retains talent with AI expertise.	[21]
Our organization has governance policies in place to oversee AI development and deployment, including accountability and transparency measures.	[7]
Our organization is committed to implementing ethical guidelines and practices in AI development, ensuring fairness, transparency, and inclusivity.	[25]
Our organization has diverse and advanced AI use cases implemented across various functions.	[4], [12]
Our organization uses metrics and key performance indicators (KPIs) to measure the performance and impact of AI initiatives.	[25]
Our organization follows the ISO 42001 standard and its practices for managing AI systems.	[23]

Web 3.0, and quantum security [19], [20]. At the core of the notion of CSM lies the risk assessment and governance process, where structured methods borrowed from well-known maturity frameworks allow organizations to methodically detect, analyze, and mitigate cyber threats [8], [26]. These models align with international security standards, ensuring compliance and standardized security policies [24]. Effective asset management is another key pillar, as organizations must track, secure, and monitor IT infrastructure, incorporating best practices outlined in CS assessment frameworks [8], [9]. To defend against cyber threats, organizations implement multi-layered security measures such as multi-factor authentication (MFA), vulnerability scanning, and penetration testing with the aid of risk management standards that emphasize proactive defense mechanisms [27]. Sustaining cyber resilience with formal incident response (IR) and disaster recovery (DR) processes also complements organizational preparedness with assurance of least disruption of operations and alignment with best practices from models, standards, and risk management frameworks [8], [24], [25]. Given the interdependent nature of digital ecosystems, third-party risk management (TPRM) is of critical significance, as CS frameworks emphasize the imperatives of AI-powered monitoring to mitigate vulnerabilities across supply chains and external partnerships [8], [9]. Human factors persist as pronounced security challenges, thus making employee training and awareness programs indispensable in augmenting cyber resilience. These programs, supported by maturity models and risk frameworks, help organizations develop a security-first culture [8], [9], [27]. As threats evolve, organisations will have to adapt with the new technologies of Web 3.0 security and blockchain integration that call for more robust access controls and AI-driven threat detection [19], [20]. Finally, increasing quantum computing-based threats imply investments in quantum-resistant cryptography that is given priority in ongoing CS research [19], [20]. Through the combination of maturity model findings, frameworks, international standards, and current security paradigms, companies are able to systematically review and develop their CS resilience in the more complicated digital world.

DTM, as shown in Table 5, measures an organization's DTM based on existing models [1], [5], [10], [11], [12], frameworks [25], [27], and industry standards [24], [45], [46]. The formulation of a solid digital strategy is essential for aligning transformation activities with organizational goals and guaranteeing measurable outcomes, as highlighted by prominent digital maturity frameworks [1], [5], [10], [11], [12]. Organizations must invest in the development of a strong digital infrastructure that supports scalability, reliability, and the easy deployment of digital initiatives, a fact confirmed by digital maturity models and frameworks [5], [10], [12], [27]. Another key area is customer experience improvement using digital technologies, where personalization and engagement initiatives are guided by DT models [1], [5], [11]. For competitiveness, organizations should develop a culture of digital innovation with emerging technologies and pilot

TABLE 4. CSM survey questions and relevant references.

Survey Question	References
Our organization conducts regular risk assessments and has a dedicated CS governance framework in place.	[8], [24], [26]
Our organization effectively tracks and manages IT assets, including hardware, software, and configurations, to ensure security.	[8], [9]
Our organization employs multi-factor authentication (MFA) and regularly performs vulnerability scans and penetration tests.	[27]
Our organization has a documented and regularly tested incident response and disaster recovery plan to ensure resilience during disruptions.	[8], [24], [25]
Our organization assesses the CS practices of third-party vendors and supply chain partners to mitigate risks.	[8], [9]
Our organization regularly conducts CS training and awareness programs for employees at all levels.	[8], [9], [27]
Our organization is prepared for emerging technologies like Web 3.0, including decentralized systems and blockchain integration.	[19], [20]
Our organization is exploring or implementing quantum-resistant cryptographic solutions to prepare for the risks posed by quantum computing.	[19], [20]

TABLE 5. DTM survey questions and relevant references.

Survey Question	References
Our organization has a comprehensive digital strategy that aligns with its overall business objectives and drives measurable outcomes.	[1], [5], [10], [11], [12]
Our organization has robust digital infrastructure that supports scalability, reliability, and the implementation of digital initiatives.	[5], [10], [12], [27]
Our organization uses digital technologies to personalize customer experiences and enhance engagement throughout the customer journey.	[1], [5], [11]
Our organization fosters a culture of digital innovation and experimentation through investments in emerging technologies and pilot programs.	[1], [5], [10] [12], [27]
Our organization has automated critical business processes to improve efficiency, accuracy, and productivity.	[5], [10], [12], [27]
Our organization adheres to recognized industry standards, holds certifications, and attestation (e.g., ISO 27001, GDPR, SOC, CSA, SOX, HIPAA compliance).	[24], [25], [45], [46]
A digital-first culture is embedded across all levels of our organization, promoting innovation, collaboration, and agility.	[1], [5], [10], [11], [12]

projects as enablers of agility and experimentation, a recurring theme in digital maturity models, and frameworks [1], [5], [10], [12], [27]. The other pillar of transformation is the automation of business processes wherein disciplined methods give a boost to productivity, accuracy, and effectiveness and best practices of digital maturity models, and frameworks [5], [10], [12], [27]. Compliance with recognized industry standards and regulatory requirements, such as ISO 27001, SOC 2, and SOX, ensures data protection, preserving privacy, and improving governance in digital ecosystems [24], [25], [45], [46]. Finally, a digitally engaged culture that is pervasive within an organization promotes innovation, facilitates collaboration, and improves agility, drawing on learnings from recognized models of digital maturity [1], [5], [10], [11], [12]. By integrating model learnings, frameworks, and industry standards, organizations can benchmark and enhance objectively their DTM to remain successful in a rapidly evolving digital landscape.

Employing research-driven survey questions, as seen in Tables 3, 4, and 5, this research offers a broad, evidence-driven digital maturity evaluation. The formal evaluation enables organizations to measure their progress, recognize strengths and weaknesses, and create focused strategies for future digital development.

Data were collected using Google Forms with a 5-point Likert scale to capture structured feedback. The collected data were analyzed through descriptive statistics, ANOVA, t-tests, and correlation analysis to identify patterns and relationships among AIM, CSM, and DTM levels. Additionally, qualitative insights were obtained by conducting thematic analysis on the open-ended responses.

The initial dataset consisted of 26 validated responses from mid- to senior-level professionals, including Chief Information Officers (CIOs), Chief Technology Officers (CTOs), and Chief Security Officers (CSOs), who were actively engaged in CS, DT, and AI-related initiatives. Participants were recruited through targeted LinkedIn keyword searches, specialized professional forums, and academic technology networks to ensure strategic relevance. The sample covered a diverse range of sectors, including technology, finance, healthcare, education, and government. Participation was voluntary and anonymized, and respondents were selected based on their leadership roles in advancing digital innovation within their organizations. Both structured 5-point Likert scale responses and open-ended qualitative feedback were collected to support subsequent statistical modeling and thematic analysis of organizational maturity patterns.

Gaussian Mixture Models (GMM) were utilized to cluster and model distribution patterns [47]. Monte Carlo sampling techniques supplied statistical matching between real and synthetic responses [48]. To verify accuracy of the generated data, the Kolmogorov-Smirnov (KS) test was utilized to match real and synthetic distributions with no significant discrepancies [49], [50].

Table 6 presents the external indices utilized to normalize the synthetic dataset. These indices were selected to impart a robust and regionally calibrated measure of AIM, CSM, and DTM within different geopolitical and industrial contexts. The global distribution of AI Preparedness Index (AIPI) scores reflects regional variation in AI adoption, as depicted in Figure 2 [51] and Oxford Insights AI Readiness Index [52] offer national benchmarks to measure the levels of AI adoption, shaping the AI maturity scores of the dataset. The CSM is normalized with the National Cybersecurity Index (NCSI) [53] and ITU Global Cybersecurity Index (GCI) [54], which review national security readiness and governance structures. In normalizing DT, the OECD Digital Economy Outlook 2024 [55] and IMD World Digital Competitiveness

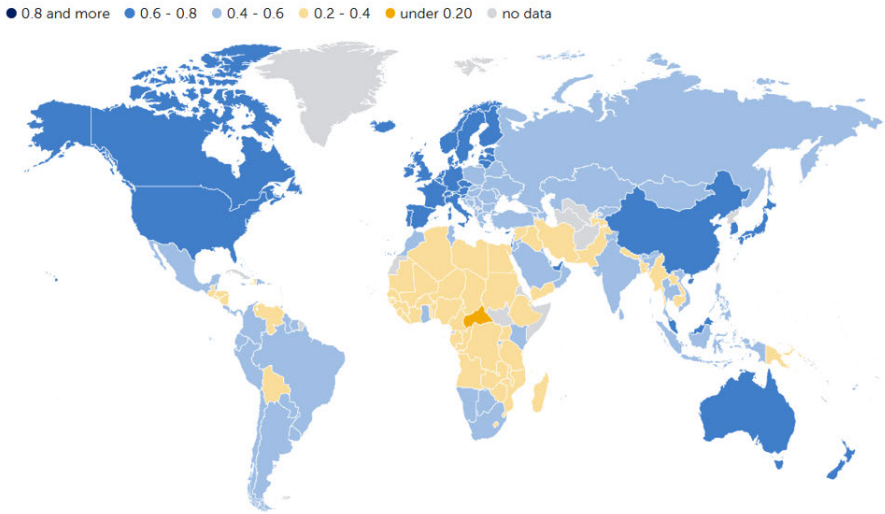

FIGURE 2. Global Distribution of AI Preparedness Index (AIPI) Scores (2024) [51]. Note:The index scores range from 0 to 1, with higher values indicating greater preparedness. Specifically, scores of 0.8 and above denote high AI preparedness, scores between 0.6 and 0.8 indicate moderate preparedness, and scores below 0.6 reflect low preparedness across AI infrastructure, skills, innovation, and regulatory dimensions.

TABLE 6. External indices used for synthetic data normalization.

Source	Impact on Dataset
IMF AI Preparedness Index (AIPI) [51]	Adjusts AI maturity based on government AI adoption levels per country.
Oxford Insights AI Readiness Index 2023 [52]	Weights AI adoption based on country-level readiness. Adjusts AI strategy, governance, and infrastructure maturity.
National Cybersecurity Index (NCSI) 2023 [53]	Adjusts CSM by national security preparedness. Calibrates risk management and governance scores.
ITU Global Cybersecurity Index (GCI) 2023 [54]	Adjusts CSM based on national security readiness. Standardizes CS governance.
OECD Digital Economy Outlook 2024 [55]	Normalizes DTM across regions. Reflects realistic digital adoption trends.
IMD World Digital Competitiveness Index [56]	Adjusts DTM based on each country's digital readiness. Aligns AI strategy and implementation with national digital capabilities.
Fortune 500 Industry Breakdown [57]	Aligns AI maturity with sectoral adoption trends. Ensures industries with higher AI adoption, such as finance and technology, exhibit greater maturity than lower-adoption sectors like agriculture and government.

Index 2024 [56] provide detailed overviews of trends in digital adoption at the sectoral and regional levels. These resources guarantee that variations in digital infrastructure and readiness at the country level are well accounted for in order to make precise adjustment to the dataset regarding DTM. Furthermore, the Fortune 500 Industry Breakdown [57] maps AI maturity levels onto sectoral adoption patterns. This provides assurance that sectors with traditionally high AI uptake, like finance and technology, are more mature than others with less uptake, like government and agriculture. By consolidating these varied indices, the dataset is more realistically and hierarchically calibrated, and it is appropriate for analytical and predictive modeling in AI, CS, and DT studies.

V. EMPIRICAL FINDINGS AND ANALYSIS

This chapter presents the key findings of the study, emphasizing the interrelationships between AIM, CSM, and DTM. The findings are described in several subsections, beginning with SEM analysis, examining direct, indirect, and mediating impacts between the variables. Then, descriptive statistics are provided, offering an overview of the levels of maturity for various dimensions. The industry and regional comparisons highlight digital maturity differences across and within industries and regions. The section concludes lastly by discussing strategic and pragmatic implications that provide essential insight to researchers, business leaders, and policymakers.

A. SEM ANALYSIS

SEM was run to analyze bidirectional relationships between AIM, CSM, and DTM. The analysis measured:

- Direct influence of AI on CS and DT.
- CS's influence on AI.
- CS's mediating role in the influence of AI on DT.

The findings confirm substantial interdependencies, CS being a foundation enabler of AI-led transformation. Moderation analysis examined whether Industry and Region influenced the AI-DT and CS-DT relationships. Results indicated that industry significantly affects it, with technology and

finance sectors showing a greater correlation, while regional differences were less pronounced. Mediation analysis found CSM to be a partial mediator of AI-DT ($\beta = 0.16, p < 0.01$), validating its significance in secure DT plans.

The study revealed that the finance and technology sectors show high levels of AIM and CSM compared to the education and government sectors. A strong correlation between CSM and DT initiatives suggests that strong infrastructure is a critical element in companies with high digital maturity.

Additionally, AIM differs significantly between developed and developing nations, with the latter adopting at lower levels due to infrastructure constraints and inadequate investment. These results provide a basis for strategic guidance and policy deliberations in AI, CS, and DT adoption. The results of this research indicate the essential interaction among AIM, CSM, and DTM. The results of the SEM analysis shown in Table 7 indicate that AIM has a significant impact on both CSM ($\beta = 0.49, p < 0.01$) and DTM ($\beta = 0.48, p < 0.01$), suggesting that companies investing in AI strategies are also likely to have more robust customer service systems and more developed DT programs.

TABLE 7. SEM results.

Hypothesis	Coefficient (β)	P-Value
H1: AIM → CSM	0.49	<0.01
H2: AIM → DTM	0.48	<0.01
H3: CSM → DTM	0.49	<0.01
H4: CSM (Mediates) AIM → DTM	0.16	<0.01

The results validate H1, with the implication that higher AIM leads to stronger CSM. AI-powered threat detection, anomaly detection, and automation significantly enhance CS strategies. Similarly, H2 is supported, showing that AIM accelerates DTM by enabling intelligent automation, predictive analytics, and digital workflows.

H3 suggests that CSM has a direct influence on DTM. The firms with strong CS positions experience faster and more secure digital adoption since security is a key enabler of digital trust and compliance. The mediation in H4 (visually depicted in Figure 3) indicates that CSM partially mediates the AIM-DTM relationship, confirming that secure AI environments facilitate broader DT initiatives.

This mediation effect further substantiates the Resource-Based View (RBV) theory by demonstrating that CS and AI capabilities act as critical strategic assets underpinning DT success.

B. QUALITATIVE INSIGHTS FROM OPEN-ENDED RESPONSES

To complement the structured survey analysis, we conducted a thematic review of the open-ended responses provided by participants. Three major themes emerged:

- **Leadership Commitment Challenges**: Several participants emphasized the difficulty of securing top-management support for integrated AI, CS, and DT initiatives.

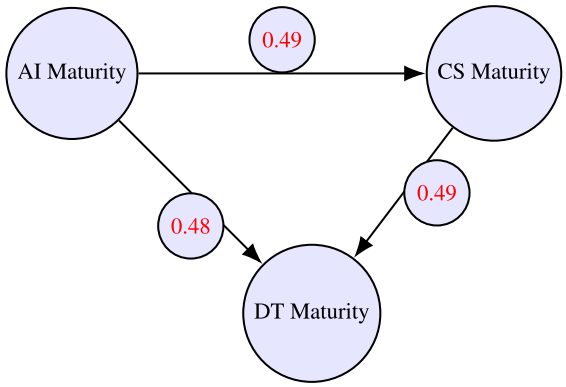

FIGURE 3. SEM path diagram showing relationships between AI, CS, and DTM.

- **Resource Constraints**: Respondents frequently mentioned limited budgets, skills shortages, and infrastructural gaps as key barriers to advancing maturity levels.
- **Ethical AI Concerns**: Ethical issues surrounding AI transparency, bias mitigation, and accountability were recurrent concerns raised by participants.

These qualitative insights align with the quantitative findings, underscoring the multifaceted challenges organizations face when striving to advance AIM, CSM, and DTM simultaneously.

C. DESCRIPTIVE STATISTICS INSIGHTS

The descriptive statistics validate the results of the structural equation modeling (SEM) analysis. As seen from Table 8, the average maturity scores indicate that CSM (Mean = 3.90) is slightly higher than AIM (Mean = 3.85) and DTM (Mean = 3.75), which suggests that companies prioritize security in their digitalization strategies.

TABLE 8. Descriptive statistics for maturity scores.

Variable	Mean	Standard Deviation	Q1	Median	Q3
AIM	3.85	0.75	3.25	3.90	4.50
CSM	3.90	0.80	3.30	4.00	4.60
DTM	3.75	0.78	3.20	3.80	4.40

D. INDUSTRY-WISE MATURITY COMPARISON

Table 9 shows Finance and Technology industries at the forefront of innovation when it comes to AI, CS, and DT. Government and Education sectors show lower maturity levels, mainly owing to regulatory challenges, budget limitations, and legacy systems.

TABLE 9. AIM, CSM, and DTM scores by industry.

Industry	AI	CS	DT
Technology	4.25	4.10	4.30
Finance	4.00	4.05	4.10
Healthcare	3.70	3.80	3.65
Government	3.20	3.40	3.15
Education	3.50	3.60	3.40

E. REGIONAL DISPARITIES IN MATURITY LEVELS

Table 10 shows regional variation, with the most mature being North America and Europe and the least mature being

South America and Africa. These are due to the extent of investment, digital infrastructure, and regulation.

TABLE 10. Maturity scores by region.

Region	AI	CS	DT
North America	4.10	4.05	4.20
Europe	4.00	4.00	4.05
Asia	3.85	3.90	3.95
South America	3.60	3.70	3.55
Africa	3.30	3.40	3.20

F. STRATEGIC AND PRACTICAL IMPLICATIONS

On the basis of these findings, the following strategic implications are concluded for business leaders, policymakers, and tech strategists:

- Balancing AI and CS Investments
  - Investing in AI firms must enhance CS protections to counter AI-based attacks.
  - AI deployment that is secure makes systems resistant to adversarial attacks and data exposure.
  - AI-enabled security controls (e.g., predictive risk assessment, anomaly detection) need to be integrated into CS plans.
  - AI governance frameworks investment, such as ISO 42001, can assist in AI risk management.
- Tailored Digital Maturity Strategies for Different Sectors
  - Maturity levels of DT are quite heterogeneous across industries and need to be addressed through tailored strategies.
  - Education and the government need special policies to help counter regulatory and budgetary issues.
  - Increased investment and incentives should underpin the secure adoption of AI in industries with robust regulatory demands.
  - The financial and technology private sector organizations must prioritize security-focused AI innovation.
- Regulatory and Security Standards as Maturity Drivers
  - Adherence to international standards of security and AI governance is important in the pursuit of enhancing maturity.
  - Adherence to standards like ISO 42001 and ISO 27001 facilitates systematic application of AI and CS.
  - Organizations must actively evolve to meet new regulatory needs for AI, CS, and data protection.
  - Industry-wide collaboration on AI ethics and security governance can enhance overall digital resilience.
- Bridging Regional Digital Divides and Policy Adjustments
  - Extensive regional variations in AIM, CSM, and DTM necessitate policy intervention and investment drives.
  - Underdeveloped regions need to be endowed with better digital infrastructure and investments in AI and CS capacities.
  - Government-sponsored schemes can drive faster adoption of AI and CS in underdeveloped markets.
  - International collaborations to close the digital divide can improve global CS resilience.

VI. CONCLUSION AND FUTURE RESEARCH

This study provides an extensive summary of the interplay between AIM, CSM, and DTM, shedding new light on their interdependencies. The findings solidify CS as a core enabler of AI-driven DT and underscore the need for organizations to align AI investments with cyber defense plans.

SEM results validate the two-way influence of AI and CS ($\beta = 0.49, p < 0.01$) and confirm the role of CSM on DT results as positive ($\beta = 0.49, p < 0.01$). Descriptive statistics also unveil that the Technology and Finance sectors are leading in digital maturity, while the Government and Education sectors lag due to regulatory and financial challenges.

A. THEORETICAL CONTRIBUTIONS

These findings contribute to the Strategic Alignment Model (SAM) and support the Resource Based View (RBV) theory, reiterating the role of AI and CS as complementary enablers of DT.

- The SAM demands that firms align IT strategies and business objectives. The findings show that AI-CS alignment plays a key role in achieving DT at an accelerated pace.
- The RBV conceptualizes AI and CS capabilities as strategic organizational resources facilitating competitive advantage. This study validates AI and CS as required assets to sustain DTM.

B. LIMITATIONS AND FUTURE RESEARCH

Despite its contributions, this study has several limitations that must be addressed by future research.

- Synthetic Data Limitations. While the synthetic data set was statistically verified, it is possible that it does not capture the full dynamic decision-making tendencies of organizations. Real-world cross-industry survey responses should be prioritized in future research for increased empirical strength.
- Sector-Specific and Regional Insights. The study provides an industry-level analysis but does not go much into sectoral CS policy or AI adoption strategies. Future research needs to tackle the issue of how regulatory climates influence AI-CS maturity across important sectors such as healthcare, finance, and public administration.
- Longitudinal Studies on AI-CS-DT Evolution. A longitudinal study would allow researchers to track how AI

and CS maturity evolve over time, showing more about their long-term impacts on DT success.

- Emerging Factors in AI-CS-DT Integration. Future research should examine emerging factors affecting AI and CS strategies, including:
  - Regulatory Dynamics: The ways in which evolving data protection laws (e.g., GDPR, AI Act) shape AI and CS convergence.
  - Workforce Adaptation: How organizations develop AI-savvy CS governance frameworks and retrain staff for AI-infused security environments.
  - Ethical AI Governance: Explainable AI, bias mitigation, and transparency as major facilitators for safe AI adoption.
  - Next-Generation Security Architectures: Zero Trust, Quantum-Resistant Cryptography, and AI-driven threat intelligence as future AI-CS convergence points.
  - Limited Quantitative Sample Size: Although the thematic insights are grounded in real survey responses, the relatively small number of quantitative observations (n=26) limits the statistical power and generalizability of the findings. While bootstrapping was employed to improve the robustness of the analysis, future research should validate these results using larger and more diverse quantitative datasets.

This research accentuates the need for an AI-CS-DT integrated approach, with an emphasis on real data collection as the next urgency in evolving maturity measurement models for companies working in the evolving digital landscape.

REFERENCES

[1] G. Vial, "Understanding digital transformation: A review and a research agenda," *J. Strategic Inf. Syst.*, vol. 28, no. 2, pp. 118–144, Feb. 2019, doi: 10.1016/j.jsis.2019.01.003.

[2] S. Ransbotham, D. Kiron, P. Gerbert, and M. Reeves, "Reshaping business with artificial intelligence: Closing the gap between ambition and action," *MIT Sloan Manage. Rev.*, vol. 59, no. 1, pp. 1–10, 2017. [Online]. Available: https://sloanreview.mit.edu/projects/reshaping-business-with-artificial-intelligence/

[3] T. R. McIntosh, T. Susnjak, T. Liu, P. Watters, D. Xu, D. Liu, R. Nowrozy, and M. N. Halgamuge, "From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models," *Comput. Secur.*, vol. 144, Sep. 2024, Art. no. 103964, doi: 10.1016/j.cose.2024.103964.

[4] H. F. Hansen, E. Lillesund, P. Mikalef, and N. Altwaijry, "Understanding artificial intelligence diffusion through an AI capability maturity model," *Inf. Manage.*, vol. 58, no. 6, pp. 103–124, 2021, doi: 10.1007/s10796-024-10528-4.

[5] P. C. Verhoef, T. Broekhuizen, Y. Bart, A. Bhattacharya, J. Qi Dong, N. Fabian, and M. Haenlein, "Digital transformation: A multidisciplinary reflection and research agenda," *J. Bus. Res.*, vol. 122, pp. 889–901, Jan. 2021, doi: 10.1016/j.jbusres.2019.09.022.

[6] A. M. Maier, J. Moultrie, and P. J. Clarkson, "Assessing organizational capabilities: Reviewing and guiding the development of maturity grids," *IEEE Trans. Eng. Manag.*, vol. 59, no. 1, pp. 138–159, Feb. 2012, doi: 10.1109/TEM.2010.2077289.

[7] J. Krijger, T. Thuis, M. De Ruiter, E. Ligthart, and I. Broekman, "The AI ethics maturity model: A holistic approach to advancing ethical data science in organizations," *AI Ethics*, vol. 4, no. 1, pp. 1–19, 2023, doi: 10.1007/s43681-022-00228-7.

[8] U.S. Dept. Energy, Washington, DC, USA. (2021). *Cybersecurity Capability Maturity Model (C2M2), Version 2.1*. [Online]. Available: https://c2m2.doe.gov/

[9] M. N. Y. Marican, S. A. Razak, A. Selamat, and S. H. Othman, "Cyber security maturity assessment framework for technology startups: A systematic literature review," *IEEE Access*, vol. 11, pp. 5442–5452, 2023, doi: 10.1109/ACCESS.2022.3229766.

[10] Deloitte Insights. (2020). *Deloitte Digital Maturity Model (DMM): Achieving Digital Transformation*. [Online]. Available: https://www2.deloitte.com

[11] G. C. Kane, D. Palmer, A. N. Phillips, D. Kiron, and N. Buckley, "Strategy, not technology, drives digital transformation: Becoming a digitally mature enterprise," *MIT Sloan Manage. Rev.*, vol. 57, no. 9, pp. 1–10, 2015. [Online]. Available: https://sloanreview.mit.edu/article/strategy-not-technology-drives-digital-transformation/

[12] Gartner Res. (2020). *Gartner Digital Maturity Model: Assessing Digital Bus. Readiness*. [Online]. Available: https://www.gartner.com

[13] Y. Zhu, H. Wan, C. Llopis-Albert, J. Ye, and S. Zeng, "Evaluating digital maturity in specialized enterprises: A multi-criteria decision-making approach," *Int. Entrepreneurship Manage. J.*, vol. 21, no. 1, pp. 1–22, 2025, doi: 10.1007/s11365-024-01051-8.

[14] A. Jamwal, R. Agrawal, and M. Sharma, "Developing a maturity model for industry 4.0 practices in manufacturing SMEs," *Oper. Manage. Res.*, vol. 18, no. 1, pp. 111–143, Mar. 2025, doi: 10.1007/s12063-025-00545-0.

[15] N. F. Zakiuddin, S. M. Anggara, and Suhardi, "Developing digital service transformation maturity model in public sector," *IEEE Access*, vol. 12, pp. 174491–174506, 2024, doi: 10.1109/ACCESS.2024.3468341.

[16] C. Matt, T. Hess, and A. Benlian, "Digital transformation strategies," *Bus. Inf. Syst. Eng.*, vol. 57, no. 5, pp. 339–343, Aug. 2015, doi: 10.1007/s12599-015-0401-5.

[17] N. Van Zeebroeck, T. Kretschmer, and J. Bughin, "Digital 'is' strategy: The role of digital technology adoption in strategy renewal," *IEEE Trans. Eng. Manag.*, vol. 70, no. 9, pp. 3183–3197, Sep. 2023.

[18] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data Inf. Manage.*, vol. 8, no. 2, Jun. 2024, Art. no. 100063. [Online]. Available: https://www.journals.elsevier.com/data-and-information-management

[19] P. Shetty, "AI and security, from an information security and risk manager standpoint," *IEEE Access*, vol. 12, pp. 77468–77474, 2024, doi: 10.1109/ACCESS.2024.3408144.

[20] Z. L. Teo, C. W. N. Quek, J. L. Y. Wong, and D. S. W. Ting, "Cybersecurity in the generative artificial intelligence era," *Asia–Pacific J. Ophthalmology*, vol. 13, no. 4, Jul. 2024, Art. no. 100091, doi: 10.1016/j.apjo.2024.100091.

[21] A. R. D. Rodrigues, F. A. F. Ferreira, F. J. C. S. N. Teixeira, and C. Zopounidis, "Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework," *Res. Int. Bus. Finance*, vol. 60, Apr. 2022, Art. no. 101616, doi: 10.1016/j.ribaf.2022.101616.

[22] J. W. Creswell and V. L. Plano Clark, *Designing and Conducting Mixed Methods Research*, 3rd ed., Thousand Oaks, CA, USA: Sage, 2018.

[23] *Artificial Intelligence—Management System—Requirements*, ISO/IEC Standard 42001:2023, Geneva, Switzerland, 2023. [Online]. Available: https://www.iso.org/standard/81220.html

[24] *Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, ISO/IEC Standard 27001:2022, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/27001.html

[25] NIST. (2023). *Artificial Intelligence Risk Management Framework*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[26] CMMI Inst., Pittsburgh, PA, USA. (2018). *Capability Maturity Model Integration (CMMI) Version 2.0*. [Online]. Available: https://www.cmmiinstitute.com

[27] Capgemini Res. Inst. (2020). *The Digital Maturity Model: Assessing Organizational Readiness for Digital Transformation*. [Online]. Available: https://www.capgemini.com

[28] G. Westerman, D. Bonnet, and A. McAfee, *Leading Digital: Turning Technology Into Bus. Transformation*. Boston, MA, USA: Harvard Univ. Press, 2014.

[29] A. Blondiau, T. Mettler, and R. Winter, "Designing and implementing maturity models in hospitals: An experience report from 5 years of research," *Health Inform. J.*, vol. 22, no. 3, pp.758–767, 2015, doi: 10.1177/1460458215590249.

[30] P. Gölzer and A. Fritzsche, "Data-driven operations management: Organisational implications of the digital transformation in industrial practice," *Prod. Planning Control*, vol. 28, no. 16, pp. 1332–1343, Dec. 2017, doi: 10.1080/09537287.2017.1375148.

[31] R. Teichert, "A model for assessing digital transformation maturity for service provider organizations," *Buildings*, vol. 14, no. 1, p. 91, 2024.

[32] K. Lee, Y. Song, M. Park, and B. Yoon, "Development of digital transformation maturity assessment model for collaborative factory involving multiple companies," *Sustainability*, vol. 16, no. 18, p. 8087, Sep. 2024, doi: 10.3390/su16188087.

[33] Z.-S. Chen, Z.-R. Wang, X.-J. Wang, M. J. Skibniewski, B. B. Gupta, and M. Deveci, "Leveraging probabilistic optimization for digital transformation maturity evaluation of construction enterprises," *IEEE Trans. Eng. Manag.*, vol. 71, pp. 8717–8746, 2024.

[34] A. Cammarano, V. Varriale, F. Michelino, and M. Caputo, "A framework for investigating the adoption of key technologies: Presentation of the methodology and explorative analysis of emerging practices," *IEEE Trans. Eng. Manag.*, vol. 71, pp. 3843–3866, 2023.

[35] H. Zhu, L. Wang, C. Li, S. P. Philbin, H. Li, H. Li, and M. Skitmore, "Building a digital transformation maturity evaluation model for construction enterprises based on the analytic hierarchy process and decision-making trial and evaluation laboratory method," *Buildings*, vol. 14, no. 1, p. 91, Dec. 2023, doi: 10.3390/buildings14010091.

[36] J.-I. Jäkel, F. Fischerkeller, T. Oberhoff, and K. Klemt-Albert, "Development of a maturity model for the digital transformation of companies in the context of construction Industry 4.0," *J. Inf. Technol. Construction*, vol. 29, pp. 778–809, Sep. 2024, doi: 10.36680/j.itcon.2024.034.

[37] D. J. Teece, G. P. Pisano, and A. Shuen, "Dynamic capabilities and strategic management," *Strategic Manage. J.*, vol. 18, no. 7, pp. 509–533, Aug. 1997, doi: 10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.

[38] D. J. Teece, "Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance," *Strategic Manage. J.*, vol. 28, no. 13, pp. 1319–1350, Dec. 2007, doi: 10.1002/smj.640.

[39] D. J. Teece, "Business models and dynamic capabilities," *Long Range Planning*, vol. 51, no. 1, pp. 40–49, Feb. 2018, doi: 10.1016/j.lrp.2017.06.007.

[40] E. L. Trist and K. W. Bamforth, "Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system," *Human Relations*, vol. 4, no. 1, pp. 3–38, Feb. 1951, doi: 10.1177/001872675100400101.

[41] R. P. Bostrom and J. S. Heinen, "MIS problems and failures: A socio-technical perspective," *MIS Quart.*, vol. 1, no. 3, pp. 17–32, 1977, doi: 10.2307/248710.

[42] L. G. Tornatzky and M. Fleischer, *The Processes of Technological Innovation*. Lexington, MA, USA: Lexington Books, 1990.

[43] J. Baker, "The technology–organization–environment framework," in *Information Systems Theory: Explaining and Predicting Our Digital Society*, Y. K. Dwivedi, M. R. Wade, and S. L. Schneberger, Eds., New York, NY, USA: Springer, 2012, pp. 231–245.

[44] N. A. A. Al-Moaid and S. G. Almarhdi, "Developing dynamic capabilities for successful digital transformation projects: The mediating role of change management," *J. Innov. Entrepreneurship*, vol. 13, no. 1, p. 85, Nov. 2024, doi: 10.1186/s13731-024-00446-9.

[45] AICPA. (2023). *SOC 2 Trust Services Criteria, American Institute of Certified Public Accountants (AICPA)*. [Online]. Available: https://www.aicpacima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

[46] *Sarbanes-Oxley Act 2002*, U.S. Dept. Labor, Washington, DC, USA, 2002.

[47] A. A. Mas'ud, A. Sundaram, J. A. Ardila-Rey, R. Schurch, F. Muhammad-Sukki, and N. A. Bani, "Application of the Gaussian mixture model to classify stages of electrical tree growth in epoxy resin," *Sensors*, vol. 21, no. 7, p. 2562, Apr. 2021, doi: 10.3390/s21072562.

[48] Y.-K. Tse, "Applications of Monte Carlo methods," in *Model Construction and Evaluation*. Cambridge, U.K.: Cambridge Univ. Press, Jun. 2012, doi: 10.1017/CBO9780511812156.015.

[49] D. J. Steinskog, D. B. Tjøstheim, and N. G. Kvamstø, "A cautionary note on the use of the Kolmogorov–Smirnov test for normality," *Monthly Weather Rev.*, vol. 135, no. 3, pp. 1151–1157, Mar. 2007, doi: 10.1175/mwr3326.1.

[50] C. Nguyen, J. B. Carlin, and K. J. Lee, "Diagnosing problems with imputation models using the Kolmogorov–Smirnov test: A simulation study," *BMC Med. Res. Methodology*, vol. 13, no. 1, p. 170, Nov. 2013, doi: 10.1186/1471-2288-13-144.

[51] Int. Monetary Fund (IMF). (2024). *AI Preparedness Index (AIPI)*. [Online]. Available: https://www.imf.org/external/datamapper/datasets/AIPI

[52] Oxford Insights. (2023). *Government AI Readiness Index 2023*. [Online]. Available: https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-1.pdf

[53] e-Governance Acad. (2023). *National Cyber Security Index (NCSI)*. [Online]. Available: https://ncsi.ega.ee/ncsi-index/

[54] Int. Telecommun. Union (ITU). (2024). *Global Cybersecurity Index (GCI)*. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[55] Organisation for Econ. Co-Operation Develop. (OECD). (2024). *OECD Digital Economy Outlook*. [Online]. Available: https://www.oecd.org/en/publications/oecd-digital-economy-outlook-2024_f0b5c251-en.html

[56] IMD World Competitiveness Center. (2024). *World Digital Competitiveness Ranking*. [Online]. Available: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/

[57] Fortune. (2024). *Fortune 500 Industry Breakdown*. [Online]. Available: https://fortune.com/ranking/fortune500/

BURAK KUBILAY received the B.S. degree in systems engineering from Turkish National Defense University, in 2010, the B.A. degree in international relations from Anadolu University, in 2019, and the M.B.A. degree from Istanbul Medeniyet University, in 2021. He is currently pursuing the M.S. degree in cybersecurity with Işik University. He is the Eastern Europe Regional Security Manager with Mastercard. His research interests include cybersecurity, artificial intelligence, and organizational maturity, with a particular interest in assessing digital transformation and security frameworks across industries.

BARIS CELIKTAS received the B.S. degree in systems engineering from National Defense University, in 2008, the M.S. degree in international relations from Karadeniz Technical University, in 2016, the M.S. degree in applied informatics from Istanbul Technical University, in 2018, and the Ph.D. degree in cybersecurity engineering and cryptography from the Institute of Informatics, Istanbul Technical University, in 2022. He is currently an Assistant Professor with the Computer Engineering Department and the Director of the Cybersecurity Graduate Program, Işik University. Besides, he is a Cybersecurity Consultant and an Architect, specializing in enterprise cybersecurity and cryptography solutions, cloud security, risk management, and governance. He holds numerous industry-recognized certifications, including CISSP, CCSP, CISM, CISA, CRISC, SSCP, CCNP, Sec+, CySA+, C|EH(M), and ISO 27001, 22301, 20000, 27701, and 42001, as a Lead Auditor and a Lead Implementer, along with GDPR DPO and NIST Cybersecurity Consultant. His research interests include cybersecurity, network security, cloud computing, cryptography, malware analysis, risk management, and security applications.