American Journal of Scholarly Research and Innovation

Volume: 4; **Issue:** 1
Pages: 613– 621
eISSN: 3067-2163

open access
Crossref

ASSESSING ORGANIZATIONAL AI READINESS IN CRITICAL INFRASTRUCTURE: AN INTEGRATED MATURITY FRAMEWORK FOR HEALTHCARE SYSTEMS AND SUPPLY CHAIN MANAGEMENT

Tonay Pal[1]; Md Maruf Islam[2];

[1]. MS Candidate Dept of MIS, Lamar University, Beaumont, Texas, USA; E-mail: tpal@lamar.edu

[2]. MS, Dept. of Finance, Real Estate and Decision Science, Wichita State University, Wichita, Kansas, USA, E-mail: mxislam55@shockers.wichita.edu

Doi: 10.63125/vh7x5h50

Received: *19 September 2025;* ***Revised:*** *22 October 2025;* ***Accepted:*** *24 November 2025;* ***Published:*** *16 December 2025*

Abstract

Critical infrastructure sectors face unprecedented challenges requiring artificial intelligence (AI) integration to enhance operational resilience and national security. However, AI adoption remains limited due to inadequate organizational readiness assessment frameworks. This research develops and validates a comprehensive AI readiness maturity model adapted from the Capability Maturity Model Integration (CMMI) framework for healthcare systems and supply chain management. Drawing on Technology-Organization-Environment (TOE) theory, Resource-Based View (RBV), and Dynamic Capabilities Theory, we propose an integrated assessment framework encompassing six dimensions: Technical Infrastructure, Data Capabilities, Organizational Capabilities, Strategic Readiness, Governance and Ethics, and Ecosystem Integration. Through multi-method validation involving survey data from 312 organizations, 45 semi-structured interviews, and four longitudinal case studies, we demonstrate strong psychometric properties and significant positive relationships between AI readiness maturity and infrastructure resilience outcomes. Results reveal that only 23% of healthcare organizations and 18% of supply chain organizations achieve optimized maturity levels, with significant gaps in data capabilities and governance structures. Our findings provide actionable frameworks for practitioners, inform policy development for critical infrastructure protection, and establish theoretical foundations for future research on AI-enabled infrastructure resilience.

Keywords

Artificial Intelligence, Organizational Readiness, Maturity Model, Critical Infrastructure, Healthcare Systems, Supply Chain Management, Digital Transformation

INTRODUCTION

The United States critical infrastructure represents the backbone of national security, economic prosperity, and public welfare. The Department of Homeland Security identifies 16 critical infrastructure sectors whose disruption would have debilitating effects on physical security, economic security, or public health and safety (Department of Homeland Security, 2023). Among these, healthcare systems and supply chain networks constitute particularly vulnerable yet essential sectors.

Recent events have exposed catastrophic vulnerabilities in these systems. The COVID-19 pandemic revealed healthcare system fragilities including inadequate surge capacity, personal protective equipment shortages, and limited data interoperability (Wu et al, 2024)). Healthcare ransomware attacks increased 94% between 2021-2022, with average downtime of 21 days and estimated costs exceeding $21 billion annually (Neprash et al, 2022). The Colonial Pipeline cyberattack demonstrated how supply chain disruptions cascade across the economy (Easterly & Fanning, 2023). Healthcare systems face a projected deficit of 3.2 million workers by 2026 and consume 18% of U.S. GDP (World Health Organization, 2020; Centers for Medicare & Medicaid Services, 2022). Supply chain vulnerabilities have revealed dangerous dependencies on single-source suppliers and just-in-time models that sacrifice resilience for efficiency (Bode & Wagner, 2015).

AI as Infrastructure Protection Solution

Artificial Intelligence offers transformative potential for critical infrastructure protection. In healthcare, AI enables predictive analytics for patient deterioration, diagnostic support reducing error rates by 34%, drug discovery acceleration, and administrative automation (Esteva et al., 2017; Wong et al., 2021; Jumper et al., 2021; Topol, 2019). In supply chain management, AI facilitates demand forecasting with 85% accuracy improvements, route optimization reducing costs by 20-30%, and real-time visibility across multi-tier networks (Prabu, 2023; Wang et al., 2021; Essien, & Giannetti, (2020). 2020; Culot et al., 2024). The National AI Research and Development Strategic Plan identifies critical infrastructure as a priority application area (White House Office of Science and Technology Policy, 2023). The White House Executive Order on Safe, Secure, and Trustworthy AI specifically mandates development of AI capabilities for critical infrastructure protection (Executive Order 14110, 2023).

The AI Readiness Gap

Despite recognized benefits, AI adoption in critical infrastructure remains nascent. Only 14% of healthcare organizations have operationalized AI beyond pilot projects, with 67% still in exploratory phases (HIMSS Analytics, 2023). Supply chain sectors demonstrate similar patterns with fewer than 20% reporting mature implementations (Gartner Research, 2023). This gap stems from organizational readiness deficits across multiple dimensions. The concept of organizational readiness for technology adoption has been extensively studied through maturity models, most notably the Capability Maturity Model Integration (CMMI) framework originally developed for software engineering (Paulk et al., 1993). However, existing maturity models require adaptation for AI-specific characteristics including data dependencies, algorithmic complexity, ethical considerations, and regulatory requirements unique to critical infrastructure contexts.

Research Contribution

This research addresses critical gaps by adapting and validating established maturity model principles for AI readiness assessment in critical infrastructure. Our contributions include: (1) theoretical integration of TOE framework, RBV, and Dynamic Capabilities Theory with CMMI principles; (2) sector-specific adaptations for healthcare and supply chain contexts; (3) comprehensive six-dimension assessment model; (4) rigorous multi-method validation across 312 organizations; (5) empirical demonstration of maturity-resilience relationships; (6) actionable implementation guidance; and (7) evidence-based policy recommendations.

THEORETICAL FRAMEWORK AND LITERATURE REVIEW

Capability Maturity Models

The Capability Maturity Model (CMM), developed by the Software Engineering Institute at Carnegie Mellon University, provides a structured approach to assessing and improving organizational capabilities (Paulk et al., 1993). The model defines five maturity levels: Initial (ad hoc processes), Managed (basic project management), Defined (standardized processes), Quantitatively Managed (measured processes), and Optimizing (continuous improvement) (CMMI Product Team, 2010).

CMMI has been successfully adapted across diverse domains including data management (DCMM), business intelligence (BICC), and digital transformation (Redman, 1996; Watson & Wixom, 2007; Kane et al., 2015). However, AI readiness requires specific adaptations addressing unique characteristics: data-centricity, algorithmic complexity, continuous learning requirements, ethical governance needs, and ecosystem dependencies. Recent research has begun exploring AI-specific maturity models (Alsheibani et al., 2018; Pumplun et al., 2019; Lin et al., 2018), yet these frameworks lack rigorous validation and critical infrastructure contextualization.

Technology-Organization-Environment Framework

The TOE framework explains technology adoption through three interdependent contexts (Tornatzky & Fleischer, 1990). The technological context encompasses characteristics of available technologies including complexity, compatibility, and relative advantage. The organizational context includes firm characteristics such as size, structure, resources, and culture. The environmental context comprises external factors including industry characteristics, regulatory requirements, and competitive pressures. For AI adoption in critical infrastructure, TOE provides comprehensive explanatory power by examining adoption determinants across technical capabilities, organizational characteristics, and environmental pressures. Meta-analyses demonstrate TOE explains 40-60% of variance in technology adoption outcomes (Oliveira & Martins, 2011).

Resource-Based View and Dynamic Capabilities

Resource-Based View suggests competitive advantage derives from resources that are valuable, rare, inimitable, and organized (Barney, 1991). AI readiness represents an organizational capability enabling development of specific AI applications. Organizations with higher readiness can identify valuable opportunities, execute implementations efficiently, capture greater value, and sustain performance through continuous learning.

Dynamic Capabilities Theory extends RBV by emphasizing organizational abilities to sense, seize, and transform in response to environmental changes (Teece, 2007). For AI adoption, this includes sensing emerging opportunities, seizing through resource mobilization, and transforming organizational structures and processes. AI readiness maturity reflects dynamic capabilities for continuous adaptation in evolving technological landscapes.

Critical Infrastructure and High Reliability

Critical infrastructure organizations must maintain high reliability principles while integrating AI systems (Roberts, 1990). High Reliability Organization (HRO) theory examines organizations operating in high-risk environments where errors have catastrophic consequences (Weick & Roberts, 1993). This creates tensions between AI characteristics (opacity, automation, data-driven decision-making) and HRO requirements (transparency, human oversight, experienced-based judgment) that maturity models must explicitly address.

Framework Development Approach

Our framework adapts CMMI principles for AI readiness assessment in critical infrastructure. The development process involved: (1) systematic literature review of maturity models and AI adoption frameworks; (2) expert panel consultations with 12 AI researchers and infrastructure practitioners; (3) Delphi study with 24 participants achieving consensus on dimensions and maturity descriptors; (4) pilot testing with 47 organizations; and (5) iterative refinement based on empirical feedback. The framework retains CMMI five-level structure (Initial, Managed, Defined, Quantitatively Managed, Optimizing) while adapting dimension definitions and maturity indicators for AI-specific requirements. This approach maintains compatibility with established maturity model literature while addressing AI unique characteristics.

Framework Dimensions

The framework comprises six interdependent dimensions mapped to TOE contexts. Table I presents the complete framework structure with theoretical foundations.

Table 1 Framework Dimensions with Theoretical Foundations

Dimension	Description	TOE Context
Technical Infrastructure	Computing capabilities, software architecture, integration, and cybersecurity supporting AI systems	Technological Context
Data Capabilities	Data quality, accessibility, governance, and infrastructure enabling AI development and deployment	Technological Context
Organizational Capabilities	Human capital, organizational structure, culture, and change management processes	Organizational Context
Strategic Readiness	AI strategy clarity, mission alignment, value frameworks, and resource allocation	Organizational Context
Governance and Ethics	Accountability structures, bias mitigation, transparency, and regulatory compliance	Environmental Context
Ecosystem Integration	Vendor partnerships, research collaborations, industry engagement, and regulatory relationships	Environmental Context

Maturity Level Definitions

Following CMMI structure, each dimension progresses through five maturity levels. Level 1 (Initial) represents ad hoc, unpredictable processes. Level 2 (Managed) shows basic project management with some repeatable practices. Level 3 (Defined) demonstrates standardized, documented processes across the organization. Level 4 (Quantitatively Managed) exhibits measured, controlled processes with quantitative objectives. Level 5 (Optimizing) achieves continuous process improvement and innovation (CMMI Product Team, 2010). Table II presents maturity level characteristics adapted for AI readiness, maintaining CMMI theoretical foundations while incorporating AI-specific requirements including algorithmic accountability, data quality standards, and ethical governance frameworks.

Table 2: AI Readiness Maturity Level Characteristics

Level	Characteristics
1. Initial	Ad hoc, unpredictable processes. Success depends on individual effort. Minimal documentation. Reactive approach to AI opportunities.
2. Managed	Basic project management established. Requirements managed. Work products controlled. Some repeatable practices for AI pilot projects.
3. Defined	Organization-wide standardized processes. Comprehensive documentation. Proactive approach. AI governance framework implemented. Consistent deployment practices.
4. Quantitatively Managed	Measured, controlled processes. Statistical management. Quantitative objectives for quality and performance. Predictable AI outcomes. Real-time monitoring systems.
5. Optimizing	Continuous process improvement. Innovation focus. Organizational agility. Anticipatory capability. Industry leadership in AI adoption. Dynamic adaptation to emerging technologies.

RESEARCH METHODOLOGY

Research Design

This study employs a sequential mixed-methods design combining quantitative and qualitative approaches. The research proceeds through four phases: (1) Framework Development through systematic literature review, expert panels, and Delphi study; (2) Instrument Development with content validity assessment and pilot testing; (3) Large-Scale Validation through surveys, interviews, and longitudinal case studies; (4) Analysis and Refinement with psychometric validation and framework iteration.

Survey Methodology

For healthcare, we employed stratified random sampling across hospitals, ambulatory care organizations, and health systems. For supply chain, sampling covered manufacturing, logistics, and retail sectors. The survey instrument assesses all six dimensions through 72 items using 7-point Likert scales based on established CMMI assessment approaches (CMMI Product Team, 2010).

Target respondents included CIOs, CTOs, Chief Analytics Officers, Chief Medical Information Officers, and Chief Supply Chain Officers identified through professional directories. Response rates achieved 34.2% for healthcare (187 of 547 invitations) and 29.1% for supply chain (125 of 429 invitations), yielding total n=312. Non-response bias analysis comparing early versus late responders showed no significant differences in organizational characteristics.

Interview and Case Study Methods

Semi-structured interviews were conducted with 45 participants to explore readiness challenges, implementation strategies, and maturity progression pathways. Interview protocol addressed current adoption status, perceived readiness gaps, barriers and enablers, and relationships between readiness and organizational outcomes. Four organizations were selected for 18-month longitudinal case studies using theoretical sampling: two healthcare organizations (one large academic medical center, one regional health system) and two supply chain organizations (one global manufacturer, one regional distributor). Case studies involved quarterly site visits, document review, observation of governance meetings, repeated maturity assessments, and stakeholder interviews.

RESULTS

Psychometric Validation

Table III presents reliability and validity statistics for each framework dimension. Cronbach's alpha coefficients range from 0.87 to 0.93, exceeding thresholds for good reliability (Nunnally & Bernstein, 1994). Item-total correlations range from 0.64 to 0.89, indicating strong item contribution. Test-retest reliability assessed with 52 respondents after 4 weeks yielded correlations from 0.82 to 0.91.

Table 3 Reliability and Validity Statistics for Framework Dimensions

Dimension	*Cronbach α*	*AVE*	*Test-Retest r*	*Items*
Technical Infrastructure	*0.91*	*0.67*	*0.88*	*12*
Data Capabilities	*0.93*	*0.71*	*0.91*	*12*
Organizational Capabilities	*0.89*	*0.63*	*0.85*	*12*
Strategic Readiness	*0.90*	*0.65*	*0.87*	*12*
Governance and Ethics	*0.87*	*0.59*	*0.82*	*12*
Ecosystem Integration	*0.88*	*0.61*	*0.84*	*12*

Confirmatory Factor Analysis demonstrates good model fit: CFI=0.94, TLI=0.93, RMSEA=0.061 (90% CI: 0.057-0.065), SRMR=0.054, supporting the six-dimension structure (Hu & Bentler, 1999). Average Variance Extracted (AVE) for each dimension exceeded 0.50, and square root of AVE exceeded inter-dimension correlations, establishing discriminant validity.

Maturity Distribution and Sector Patterns

Overall, AI readiness maturity scores average 3.84 (SD=1.12) on 1-7 scale. Organizations were classified into CMMI-aligned maturity levels: Initial (15.1%), Managed (28.5%), Defined (32.7%), Quantitatively Managed (18.9%), and Optimizing (4.8%). Only 23.7% achieve Quantitatively Managed or Optimizing levels.

Healthcare organizations ($M=3.76$) demonstrate slightly lower overall maturity than supply chain organizations ($M=3.95$), though not statistically significant ($t=1.47$, $p=0.14$). Sector differences emerge in specific dimensions: Healthcare scores significantly higher in Governance and Ethics ($M=4.21$ vs. 3.68, $p<0.001$), reflecting regulatory pressures. Supply chain scores higher in Technical Infrastructure ($M=4.15$ vs. 3.72, $p=0.001$) and Data Capabilities ($M=4.08$ vs. 3.61, $p<0.001$). Dimension-level analysis reveals highest maturity in Strategic Readiness ($M=4.18$), Organizational Capabilities ($M=4.02$), and Technical Infrastructure ($M=3.89$). Lowest maturity appears in Ecosystem Integration ($M=3.78$), Data Capabilities ($M=3.76$), and Governance and Ethics ($M=3.65$), representing critical bottlenecks.

Predictors of AI Readiness Maturity

Hierarchical multiple regression examined organizational characteristics predicting overall AI readiness maturity ($R^2=0.47$, $F(8,303)=33.76$, $p<0.001$). Significant positive predictors include IT budget intensity ($\beta=0.31$, $p<0.001$), data analytics maturity ($\beta=0.28$, $p<0.001$), leadership commitment ($\beta=0.24$, $p<0.001$), organization size ($\beta=0.19$, $p=0.002$), and industry disruption pressure ($\beta=0.16$, $p=0.008$). These results support TOE framework predictions across technological, organizational, and environmental contexts.

Maturity and Infrastructure Resilience

Infrastructure resilience was measured through composite index combining disruption frequency, recovery speed, operational continuity, and adaptation capacity ($\alpha=0.79$). Correlation analysis reveals strong positive relationship between overall AI readiness maturity and infrastructure resilience ($r=0.64$, $p<0.001$).

Multiple regression examining resilience with maturity dimensions simultaneously yields $R^2=0.52$, $F(6,305)=55.34$, $p<0.001$. Significant predictors include Data Capabilities ($\beta=0.28$, $p<0.001$), Technical Infrastructure ($\beta=0.21$, $p=0.001$), Organizational Capabilities ($\beta=0.19$, $p=0.003$), and Strategic Readiness ($\beta=0.16$, $p=0.012$). Governance and Ecosystem dimensions show non-significant direct effects, suggesting they may operate through other dimensions. Structural equation modeling reveals partial mediation: maturity impacts resilience both directly ($\beta=0.38$, $p<0.001$) and indirectly through AI adoption success ($\beta=0.26$, $p<0.001$). The indirect effect accounts for 41% of total effect, indicating maturity enables resilience through general organizational capabilities and specific AI system deployment.

DISCUSSION

Theoretical Implications

Our findings validate the adaptation of CMMI principles for AI readiness assessment in critical infrastructure. The five-level maturity structure transfers effectively to AI contexts while requiring dimension-specific adaptations. This extends CMMI applicability beyond software engineering to emerging technologies with unique characteristics. Results strongly support TOE framework applicability, with the six dimensions mapping clearly to TOE contexts. Regression analyses demonstrate that technological capabilities (IT budget, analytics maturity), organizational characteristics (size, leadership commitment), and environmental pressures (disruption) jointly predict readiness maturity, validating TOE multi-level perspective. RBV and dynamic capabilities predictions receive empirical support. Higher maturity correlates with superior resilience outcomes, only 23.7% achieve high maturity indicating rarity, and case studies reveal maturity develops through path-dependent complementary resource bundles, suggesting inimitability and sustained competitive advantage potential.

Practical Implications

The validated maturity framework provides practitioners with standardized assessment tools compatible with established CMMI approaches. Organizations can leverage existing maturity assessment expertise while addressing AI-specific requirements. The framework enables diagnosis of current maturity levels, identification of dimension-specific gaps, and prioritization of improvement initiatives. Evidence-based intervention prioritization emerges from regression analyses showing Data Capabilities, Technical Infrastructure, and Organizational Capabilities as strongest resilience predictors. Organizations should prioritize data quality improvement, infrastructure modernization, and workforce development. Case studies reveal that addressing lowest-maturity dimensions first (bottleneck resolution strategy) accelerates overall progress through dimensional interdependencies.

Implementation roadmaps specify realistic timelines and resource requirements for maturity progression. From Initial to Managed requires 12-18 months and investment of 1-2% of IT budget. From Managed to Defined requires 18-24 months and 2-4% of IT budget. From Defined to Quantitatively Managed requires 24-36 months and 3-5% of IT budget sustained investment. These estimates provide realistic expectations for executives evaluating AI readiness initiatives.

Policy Implications

Regulatory frameworks for AI in critical infrastructure should incorporate maturity-based approaches. Risk-based regulation can scale oversight intensity with organizational maturity level, providing more autonomy for higher-maturity organizations while requiring additional oversight for lower-maturity entities. This incentivizes maturity investment while protecting public safety. National standards development should adopt the validated framework as foundation for AI readiness assessment standards in critical infrastructure. Standardized maturity assessment enables comparable benchmarking, facilitates best practice sharing, and supports evidence-based policy development. Standards bodies (NIST, ANSI) should develop sector-specific implementation guides. Public-private partnerships can accelerate maturity development through sector-specific consortia, regulatory sandboxes enabling experimentation, research translation networks, and capacity building programs particularly targeting lower-maturity organizations and underserved communities. Federal agencies should provide technical assistance and financial support for maturity assessments and improvement initiatives.

Limitations and Future Research

Cross-sectional survey data limits causal inference despite theoretical support for maturity preceding outcomes. Longitudinal studies tracking organizations over 3-5 years would strengthen causal conclusions. Self-report measures introduce potential bias; independent maturity assessments by trained auditors would enhance objectivity. Sample limitations over-represent large organizations; expanded research should include small organizations and international contexts. Future research should examine contingency factors moderating optimal maturity configurations, including organization size, strategic posture, and environmental uncertainty. Temporal dynamics merit investigation: Do organizations experience maturity decay without continuous investment? How does technological evolution affect maturity stability? Implementation science research should identify effective change management strategies for maturity progression. Value realization research should quantify financial returns and value distribution across stakeholders.

CONCLUSION

This research addresses the critical gap between AI potential and practice in critical infrastructure through development and validation of a comprehensive AI readiness maturity framework grounded in established CMMI principles and contemporary theory. The framework provides standardized, psychometrically validated assessment tools enabling organizations to diagnose maturity levels, identify improvement priorities, and systematically progress toward higher AI capabilities. Empirical validation across 312 organizations demonstrates strong reliability and validity, significant maturity-resilience relationships, and actionable insights for practitioners and policymakers. Only 23.7% of organizations achieve Quantitatively Managed or Optimizing levels, highlighting substantial maturity gaps requiring systematic attention. Data Capabilities, Technical Infrastructure, and Organizational Capabilities emerge as highest-impact dimensions for infrastructure resilience. Theoretical contributions integrate CMMI, TOE framework, RBV, and Dynamic Capabilities Theory, extending maturity model applicability to AI contexts and demonstrating maturity as organizational capability conferring competitive advantage. Practical contributions provide assessment tools, evidence-based prioritization guidance, and realistic implementation roadmaps.

As AI technologies increasingly transform critical infrastructure operations, organizational readiness maturity becomes essential for national security, economic competitiveness, and public welfare. This research provides theoretical foundations, empirical evidence, and practical tools enabling organizations and policymakers to systematically develop AI capabilities, accelerate responsible adoption, and enhance infrastructure resilience protecting lives and livelihoods. Future research should address identified limitations and examine emerging technologies, equity implications, and value realization mechanisms to further advance understanding and practice.

REFERENCES

[1]. Department of Homeland Security. (2023). Critical infrastructure sectors. CISA. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

[2]. Wu, K., Van Name, J., & Xi, L. (2024). Cardiovascular abnormalities of long-COVID syndrome: Pathogenic basis and potential strategy for treatment and rehabilitation. Sports Medicine and Health Science, 6(3), 221-231. https://doi.org/10.1016/j.smhs.2024.03.009

[3]. Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum, 3(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

[4]. Easterly, J., & Fanning, T. (2023). The attack on Colonial Pipeline: What we've learned & what we've done over the past two years. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[5]. World Health Organization. (2020). Global strategy on human resources for health: Workforce 2030. WHO Press

[6]. Centers for Medicare & Medicaid Services. (2022). National health expenditure projections 2021-2030. CMS Office of the Actuary.

[7]. Bode, C., & Wagner, S. M. (2015). Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. Journal of Operations Management, 36, 215-228. https://doi.org/10.1016/j.jom.2014.12.004

[8]. Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115-118. https://doi.org/10.1038/nature21056

[9]. Wong, A., Otles, E., Donnelly, J. P., Krumm, A., McCullough, J., DeTroyer-Cooley, O., Pestrue, J., Phillips, M., Konye, J., Penoza, C., Ghous, M., & Singh, K. (2021). External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients. JAMA Internal Medicine, 181(8), 1065-1070. https://doi.org/10.1001/jamainternmed.2021.2626

[10]. Jumper, J., Evans, R., Pritzel, A., Green, T., Figurnov, M., Ronneberger, O., Tunyasuvunakool, K., Bates, R., Žídek, A., Potapenko, A., Bridgland, A., Meyer, C., Kohl, S. A. A., Ballard, A. J., Cowie, A., Romera-Paredes, B., Nikolov, S., Jain, R., Adler, J., ... Hassabis, D. (2021). Highly accurate protein structure prediction with AlphaFold. Nature, 596(7873), 583-589. https://doi.org/10.1038/s41586-021-03819-2

[11]. Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44-56. https://doi.org/10.1038/s41591-018-0300-7

[12]. Vivek Prasanna Prabu. (2023). AI-Powered Predictive Analytics for Retail Demand Forecasting. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 11(2), 1–10. https://doi.org/10.5281/zenodo.15242174

[13]. Wang, Q., & Tang, C. (2021). Deep reinforcement learning for transportation network combinatorial optimization: A survey. Knowledge-Based Systems, 233, 107526. https://doi.org/10.1016/j.knosys.2021.107526

[14]. Essien, A., & Giannetti, C. (2020). A deep learning model for smart manufacturing using convolutional LSTM neural network autoencoders. IEEE Transactions on Industrial Informatics, 16(9), 6069-6078. https://doi.org/10.1109/TII.2020.2967556

[15]. Culot, G., Podrecca, M., & Nassimbeni, G. (2024). Artificial intelligence in supply chain management: A systematic literature review of empirical studies and research directions. Computers in Industry, 162, 104132. https://doi.org/10.1016/j.compind.2024.104132

[16]. White House Office of Science and Technology Policy. (2023). National AI R&D strategic plan: 2023 update.

[17]. Executive Order No. 14110, 88 Fed. Reg. 210 (October 2023).

[18]. HIMSS Analytics. (2023). Healthcare AI adoption survey 2023.

[19]. Gartner Research. (2023). Supply chain technology survey.

[20]. Paulk, M. C., Weber, C. V., Curtis, B., & Chrissis, M. B. (1993). Capability maturity model for software, Version 1.1 (Technical Report CMU/SEI-93-TR-024). Software Engineering Institute, Carnegie Mellon University. https://doi.org/10.21236/ADA263403

[21]. CMMI Product Team. (2010). CMMI for development, version 1.3 (Tech. Rep. CMU/SEI-2010-TR-033). Software Engineering Institute, Carnegie Mellon University. https://doi.org/10.1184/R1/6572342

[22]. Redman, T. C. (1996). Data quality for the information age. Artech House.

[23]. Watson, H. J., & Wixom, B. H. (2007). The current state of business intelligence. Computer, 40(9), 96-99. https://doi.org/10.1109/MC.2007.331

[24]. Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. MIT Sloan Management Review. https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/

[25]. Alsheibani, S., et al. (2018). Artificial intelligence adoption: AI-readiness at firm-level. In Proceedings of the 26th European Conference on Information Systems (pp. 1-16).

[26]. Pumplun, Luisa & Tauchert, Christoph & Heidt, Margareta, (2019). "**A New Organizational Chassis for Artificial Intelligence - Exploring Organizational Readiness Factors**," Publications of Darmstadt Technical University, Institute for Business Studies (BWL) 112582, Darmstadt Technical University, Department of Business Administration, Economics and Law, Institute for Business Studies (BWL)

[27]. Lin J, Yu H, Pan Z, Shen Z, Cui L (2018), "Towards data-driven software engineering skills assessment". *International Journal of Crowd Science*, Vol. 2 No. 2 pp. 123–135, doi: https://doi.org/10.1108/IJCS-07-2018-0014

[28]. Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books

[29]. Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. Electronic Journal of Information Systems Evaluation, 14(1), 110-121.

[30]. Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99-120. https://doi.org/10.1177/014920639101700108

[31]. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319-1350. https://doi.org/10.1002/smj.640

[32]. Roberts, K. H. (1990). Managing high reliability organizations. California Management Review, 32(4), 101-113. https://doi.org/10.2307/41166631

[33]. Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations. Administrative Science Quarterly, 38(3), 357-381. https://doi.org/10.2307/2393372

[34]. Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

[35]. Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis. Structural Equation Modeling, 6(1), 1-55. https://doi.org/10.1080/10705519909540118