



Review Article

Advancing IT Competency for Digital Transformation and Learning Ecosystem Expansion: An Integrative Review and Practical Framework

Mohammed Jahed Sarwar* 

York College, City University of New York (CUNY), New York, The United States

Abstract

Digital transformation has shifted from a technology modernization agenda to a capability agenda—one that depends on how effectively organizations develop, govern, and sustain IT competencies across cloud platforms, cybersecurity, data and AI, and digitally mediated learning and service ecosystems. This integrative review synthesizes peer-reviewed research and authoritative standards (2018-2025) to identify core competency domains and organizational enablers required to transcend incremental, legacy-bound models. *Findings converge on five domains—(1) cloud and platform engineering, (2) cybersecurity and digital trust, (3) data, AI and automation (including generative AI governance), (4) experience engineering and service design, and (5) learning ecosystem engineering—supported by cross-cutting mechanisms in architecture, risk management, talent pathways, and change leadership.* Building on this synthesis, the paper proposes an actionable competency-based framework and a phased implementation roadmap that organizations can use to assess readiness, prioritize investments, and operationalize continuous upskilling. The central contribution is practical and policy-relevant: it positions IT competency as the enterprise control point that converts technology investments into resilience, inclusion, and measurable operational performance in the information age.

Keywords

Digital Transformation, IT Competency, Cloud Computing, Cybersecurity, Artificial Intelligence, Generative AI, Learning Ecosystems, Organizational Resilience

1. Introduction

Across sectors, digital transformation (DT) is increasingly characterized by platform architectures, data-centric operating models, and rapidly evolving cyber and regulatory risk. Contemporary research frames DT as a socio-technical change process that reshapes strategy, structures, and value creation rather than a one-time IT upgrade [1-6]. This perspective helps explain why many transformations stall: technology acquisition outpaces the development of competencies, governance,

and operating routines that make new capabilities durable [7-9].

The post-pandemic period further intensified the need for digitally resilient learning and service delivery. Large-scale education disruption accelerated the use of online platforms and spotlighted disparities in connectivity, skills, and accessibility [22]. At the same time, workforce evidence continues to show material cybersecurity and cloud skills gaps—an issue

*Correspondence: Mohammed Jahed Sarwar (msarwar1@york.cuny.edu)

Received: 15 December 2025; Accepted: 24 December 2025; Published: 21 February 2026



Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

that raises transformation risk and increases the cost of sustaining secure digital operations [15-17, 20].

This paper synthesizes recent evidence on the IT competencies that underpin successful DT and learning ecosystem expansion and translates the synthesis into a practical framework and implementation roadmap. The aim is to provide a publishable, editor-friendly contribution that connects theory to actionable governance, architecture, and talent development decisions.

2. Methods: Integrative Review Design

An integrative review approach was used to bridge empirical research, conceptual scholarship, and practitioner-relevant standards. Sources were identified through iterative searches of major scholarly databases and discipline repositories, complemented by citation chasing from highly cited DT reviews and capability papers. Inclusion prioritized (a) peer-reviewed journal articles and systematic reviews published between 2018 and 2025, and (b) authoritative standards and guidance documents relevant to cybersecurity, AI governance, and digital inclusion. Sources lacking methodological transparency or credibility were excluded.

2.1. Search Strategy and Selection Criteria

To strengthen methodological transparency, we documented the search strategy and screening criteria used in this integrative review. Searches were conducted across major scholarly databases and practitioner repositories (e.g., Scopus, Web of Science, IEEE Xplore/ACM Digital Library, ERIC, and Google Scholar), complemented by backward/forward citation chasing from highly cited digital transformation reviews. Keyword combinations were built around (a) digital transformation, (b) IT competency/capability, and (c) learning ecosystem/workforce development, including terms such as “digital transformation” AND “IT competency” OR “IT capability,” “cloud,” “cybersecurity,” “data/AI,” “governance,” and “learning.” We prioritized peer-reviewed publications and authoritative practitioner standards published primarily between 2015 and 2025, with older foundational works retained when repeatedly cited. Sources were included if they (1) defined or operationalized IT competencies for digital transformation, (2) reported empirical findings or validated frameworks, or (3) articulated governance, security, or platform practices with clear organizational relevance. Sources lacking sufficient methodological clarity, unverifiable claims, or unclear provenance were excluded. The final synthesis drew on 35 sources (see References), which were coded and integrated into the competency framework (Figure 1) and implementation roadmap (Table 2).

2.2. Data Extraction and Synthesis Procedures

Data extraction and synthesis were conducted thematically. First-cycle coding mapped recurring competency statements to capability domains; second-cycle coding identified organizational enablers (e.g., governance, architecture, change management) and outcome mechanisms (e.g., resilience, service quality, inclusion). The synthesis was then translated into (a) a competency-based framework (Figure 1) and (b) a phased implementation roadmap (Table 2).

3. Results: A Competency-based Framework for Digital Transformation

Across the reviewed literature, DT success is consistently associated with coherent capability building organizations align strategy, architecture, people, and governance to realize technology value [1-5, 8]. The synthesis yielded five IT competency domains supported by cross-cutting enablers (Table 1). Figure 1 summarizes the proposed framework, positioning competency development as the mechanism connecting strategic drivers to operational and learning outcomes. Figure 1 summarizes the synthesized competency domains and their linkages to drivers, enabling mechanisms, and measurable outcomes.

Cloud competency extends beyond vendor certification to include platform engineering, automation, and disciplined cost and reliability management. Capability indicators include infrastructure-as-code (IaC), standardized continuous integration/continuous delivery (CI/CD) pipelines, Site Reliability Engineering (SRE) practices (e.g., service level objectives/service level indicators [SLOs/SLIs]), identity-centric access control, and integration patterns for hybrid environments. From a DT perspective, cloud capabilities function as a dynamic capability: they increase strategic agility and enable continuous renewal of business and operating models [8].

DT expands the attack surface through cloud services, third-party integrations, and AI-enabled workflows, making security-by-design a baseline competency. National Institute of Standards and Technology (NIST) Zero Trust Architecture provides an established reference for identity-centric controls, segmentation, and continuous verification [15]. ISO/IEC 27001 and ISO/IEC 27002 provide requirements and control guidance for information security management systems (ISMS) and operational controls [16, 17]. Competency also includes identity and access management (IAM), incident response, and third-party risk management. Workforce research continues to document material skills gaps, increasingly including cloud security and AI security competencies, underscoring the need for structured talent pathways and continuous training [20].

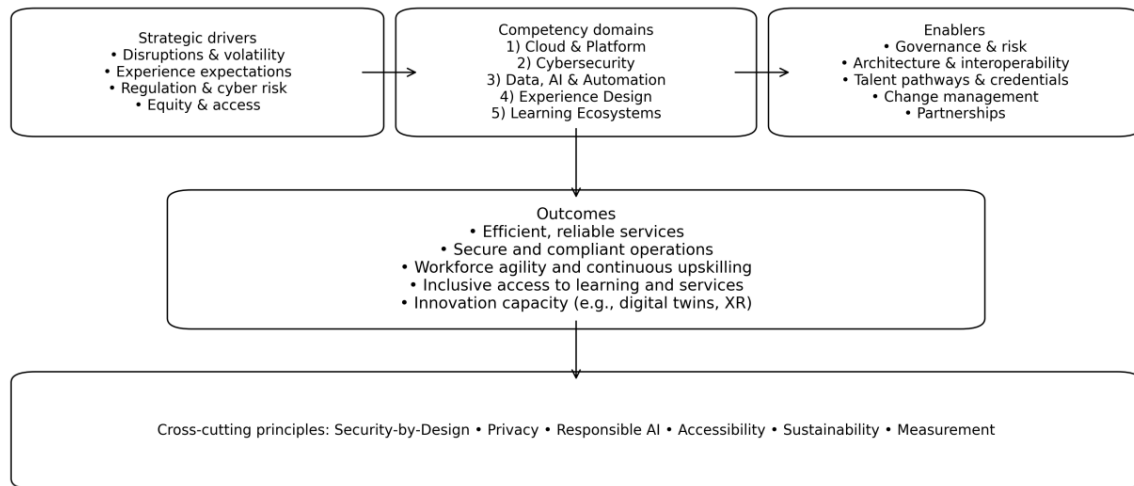


Figure 1. Competency-Based Framework Linking Strategic Drivers, IT Competency Domains, Enabling Mechanisms, and Measurable Outcomes.

Data, AI, and Automation (Including Generative AI)

AI has become integral to digital operating models, affecting decision workflows, customer and employee interaction, and IT service management. Organizations therefore require competencies in data stewardship, model lifecycle management (MLOps), evaluation and monitoring, and responsible AI practices. A validated DT skills framework emphasizes the interdependence of technical skills (data/AI, architecture) and socio-organizational skills (collaboration, change capability) [10].

Generative AI amplifies both value potential and risk (e.g., hallucinations, data leakage, model misuse). The NIST AI Risk Management Framework (AI RMF 1.0) and the Generative AI Profile provide practical guidance for mapping and treating risks across the AI lifecycle and operationalizing trustworthiness controls such as transparency, privacy, and accountability [18, 19]. Organizational AI governance reviews similarly converge on the need for role clarity, risk taxonomy, and oversight mechanisms to align AI use with legal and ethical obligations [12, 13].

While industry narratives often frame DT as technology-led, scholarly research emphasizes customer and employee value creation through integrated experience, process, and data redesign [1-3, 11]. Experience engineering competencies include service design, user experience (UX) and accessibility, analytics-enabled personalization, and change adoption. These competencies also support the transition from digitization to deeper transformation stages by aligning front-stage experiences with back-stage operating routines and performance metrics [2].

Learning ecosystem expansion requires interoperable educational technology (EdTech) platforms (e.g., learning management systems [LMS], collaboration suites, and identity

services), sustainable support models, and the capability to serve diverse learners and staff. DT research underscores that capability building is inseparable from organizational learning and innovation—mechanisms that also underpin resilient learning ecosystems [7].

Digital inclusion is not only a social priority but also a performance constraint. Global reporting shows that connectivity and affordability gaps persist, limiting participation in digital learning and services [21, 22]. In practice, learning ecosystem engineering includes mobile-first design, low-bandwidth options, accessible content, and locally supported digital literacy initiatives.

As summarized in Table 1, the literature converges on a core set of IT competency domains and representative indicators that can be operationalized for assessment and workforce development.

Framework generalizability and context. Although the competency domains are intentionally cross-sectoral, their implementation is context-sensitive. In higher-education environments, governance and learning ecosystem design typically emphasize instructional continuity, student digital equity, accessibility, and shared services—often under constrained budgets and complex stakeholder structures. In enterprise settings, the same competencies may be optimized toward customer experience, product/platform scalability, and regulatory/commercial risk exposure. Accordingly, we recommend that users treat Figure 1 as a modular reference architecture: organizations should calibrate domain emphasis, indicators, and maturity targets to their operating model, risk profile, and mission. This contextualization preserves comparability while supporting pedagogically transformative and operationally relevant adoption.

Table 1. Synthesized IT Competency Domains and Representative Indicators.

Domain	Core Competencies	Example Operational Indicators	Representative Sources
Cloud & Platform Engineering	Cloud architecture; platform engineering; automation; reliability; cost governance	IaC and CI/CD standards; SRE practices; hybrid integration patterns; policy-as-code guardrails	[8, 10]
Cybersecurity & Digital Trust	Zero trust; IAM; incident response; security governance; privacy	Continuous monitoring; segmentation; third-party risk controls; ISMS controls	[15-17, 20]
Data, AI & Automation	Data stewardship; MLOps; evaluation and monitoring; responsible AI; generative AI workflow design	Model registry and monitoring; secure data pipelines; AI risk controls; human-in-the-loop escalation	[10, 12, 13, 18, 19]
Experience Engineering	Service design; UX and accessibility; analytics-driven personalization; change adoption	Journey mapping; accessibility audits; experience KPIs; integrated front/back-stage architecture	[1-3, 11]
Learning Ecosystem Engineering	EdTech architecture; identity integration; learning analytics governance; digital literacy enablement	Interoperability; accessible/multi-modal delivery; support capacity; measurement of learning outcomes	[7, 21, 22]

4. Discussion: Cross-sector Implications

The synthesis indicates that DT should be governed as an enterprise capability program. Dynamic capability research emphasizes that DT is an ongoing process of strategic renewal driven by agility and learning mechanisms rather than a single technology project [8]. Similarly, DT research notes that value realization depends on aligning operating routines, organizational structure, and performance measurement with digitally enabled business models [2, 3, 11, 14].

Across contexts, common failure modes include (a) skills treated as ad-hoc training rather than a talent system; (b) procurement without architectural coherence; and (c) insufficient attention to experience, accessibility, and change adoption. The proposed framework addresses these issues by coupling domain competencies with enabling mechanisms and measurable outcomes, enabling leaders to prioritize investments and controls with greater precision.

5. Recommendations: A Phased Implementation Roadmap

Emerging evidence suggests that immersive modalities—extended reality (XR), including virtual and mixed reality—can strengthen workforce training and higher-education learning ecosystems when paired with learning analytics and accessibility-by-design practices [23-27]. Digital twins are likewise increasingly used to model complex socio-technical systems and evaluate operational scenarios, making them promising for training, simulation, and continuous improvement in digitally mediated environments [28, 29]. Workforce trend reporting underscores that reskilling pressure and digital skill shifts remain structural features of the labor market, reinforcing the need for institutionalized learning pathways and micro-credentials [30]. Finally, systems dynamics approaches can complement roadmap execution by modeling feedback loops between capability investment, adoption behavior, and performance outcomes [31].

Table 2. Practical Roadmap for Advancing IT Competency and Transformation Readiness.

Phase	Primary Actions	Outputs / Evidence of Progress
0-90 days (Stabilize & Govern)	Establish DT governance; define competency domains and skill inventory; adopt baseline cybersecurity controls and a zero trust roadmap; set AI usage policy aligned to AI RMF; identify priority learning services and accessibility requirements.	Governance charter; skills baseline; risk register; minimum security and AI guardrails; prioritized service/learning backlog.

Phase	Primary Actions	Outputs / Evidence of Progress
3-12 months (Build & Enable)	Stand up platform engineering (IaC, CI/CD, reliability practices); implement identity-centric controls; deploy data governance and MLOps foundations; create role-based learning pathways and micro-credentials; modernize learning platform integration and analytics governance.	Reusable platform templates; reliability KPIs; operational ISMS controls; model monitoring; proficiency evidence; integrated learning services.
12-24 months (Scale & Optimize)	Scale automation and AI with human oversight; expand digital twin and extended reality (XR) pilots [23-29] for training and operations; institutionalize cost governance; measure experience and learning outcomes; refine controls based on audits and incidents; sustain communities of practice.	Reduced cycle time and incidents; validated pilots with return on investment (ROI); improved access and satisfaction metrics; continuous improvement cadence; repeatable audit outcomes.

6. Limitations

This integrative review prioritizes cross-sector relevance; it does not claim the exhaustive coverage of a full systematic review across all databases and languages. Additionally, outcome claims in the literature can be context-dependent and influenced by measurement differences. Future work should operationalize the framework into validated survey instruments and longitudinal studies linking competency investments to measurable performance and equity outcomes.

7. Conclusion

DT success depends on deliberate IT competency development treated as an enterprise capability. Evidence converges on five competency domains supported by governance, architecture, and change leadership. The proposed framework and roadmap provide a practical structure to assess readiness, prioritize investments, and implement continuous upskilling while maintaining cybersecurity and responsible AI controls. For leaders, the implication is clear: competency is the leverage point that converts technology spending into resilient operations and inclusive, scalable learning ecosystems.

Abbreviations

AI	Artificial Intelligence
CI/CD	Continuous Integration/Continuous Delivery
DT	Digital Transformation
EdTech	Educational Technology
IaC	Infrastructure-as-code
IAM	Identity and Access Management
ISMS	Information Security Management System
KPI	Key Performance Indicator
LMS	Learning Management System
MLOps	Machine Learning Operations

NIST	National Institute of Standards and Technology
ROI	Return on Investment
SLI	Service Level Indicator
SLO	Service Level Objective
SRE	Site Reliability Engineering
UX	User Experience
XR	Extended Reality

Author Contributions

Mohammed Jahed Sarwar is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

References

- [1] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 28(2), 118-144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- [2] Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889-901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- [3] Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies*, 58(5), 1159-1197. <https://doi.org/10.1111/joms.12639>
- [4] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471-482. <https://doi.org/10.25300/MISQ/2013/37.2.3>

- [5] Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & Information Systems Engineering*, 57, 339-343. <https://doi.org/10.1007/s12599-015-0401-5>
- [6] Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation*, 102, 102217. <https://doi.org/10.1016/j.technovation.2020.102217>
- [7] Trener, B., Chng, S., Wang, Y., Lu, H., & Abukhait, R. (2021). Preparing workplaces for digital transformation: An integrative review and framework of multi-level factors. *Frontiers in Psychology*, 12, 620241. <https://doi.org/10.3389/fpsyg.2021.620241>
- [8] Warner, K. S., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52(3), 326-349. <https://doi.org/10.1016/j.lrp.2018.12.001>
- [9] Vogelsang, K., Liere-Netheler, K., Packmohr, S., & Hoppe, U. (2019). Success factors for fostering a digital transformation in manufacturing companies. *Journal of Enterprise Transformation*, 8(1-2), 121-142. <https://doi.org/10.1080/19488289.2019.1578839>
- [10] Bouwmans, A., de Leeuw, A., & van der Heijden, B. (2024). The digital transformation skills framework: A new tool to support organizational transformation. *PLOS ONE*, 19(1), e0296374. <https://doi.org/10.1371/journal.pone.0296374>
- [11] Kretschmer, T., & Khashabi, P. (2020). Digital transformation and organization design: An integrated approach. *California Management Review*, 62(4), 86-104. <https://doi.org/10.1177/0008125620940292>
- [12] Batool, A., Sefat, M., & Mahmoud, Q. (2025). AI governance in organizations: A systematic literature review. *International Journal of Information Management*, 74, 102695. <https://doi.org/10.1016/j.ijinfomgt.2024.102695>
- [13] Mallinson, R. (2025). A unified approach to AI governance: Bridging theory and practice. *AI and Ethics*, 5, 1-15. <https://doi.org/10.1007/s43681-024-00550-0>
- [14] Volberda, H. W., Khanagha, S., Baden-Fuller, C., Mihalache, O. R., & Birkinshaw, J. (2021). Strategizing in a digital world: Overcoming cognitive barriers, reconfiguring routines and introducing new organizational forms. *Long Range Planning*, 54(5), 102110. <https://doi.org/10.1016/j.lrp.2021.102110>
- [15] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
- [16] ISO/IEC. (2022). ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.
- [17] ISO/IEC. (2022). ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization.
- [18] National Institute of Standards and Technology. (2023). AI Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology.
- [19] Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.600-1>
- [20] ISC2. (2024). ISC2 cybersecurity workforce study 2024. ISC2. <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study>
- [21] International Telecommunication Union. (2024). Measuring Digital Development: Facts and Figures 2024. ITU Publications.
- [22] United Nations Sustainable Development Group. (2020). Policy Brief: Education during COVID-19 and beyond. United Nations.
- [23] Burke, D., Crompton, H., & Nickel, C. (2025). The Use of Extended Reality (XR) in Higher Education: A Systematic Review. *TechTrends*, 69, 998-1011. <https://doi.org/10.1007/s11528-025-01092-y>
- [24] Bödding, R., Schriek, S. A., & Maier, G. W. (2025). A systematic review and meta-analysis of mixed reality in vocational education and training. *Virtual Reality*, 29, 44. <https://doi.org/10.1007/s10055-025-01118-z>
- [25] Steen, C. W., Söderström, K., Stensrud, B., et al. (2024). Virtual reality-based mental health training: A systematic review. *BMC Medical Education*, 24, 587. <https://doi.org/10.1186/s12909-024-05613-w>
- [26] Moulaei, K., Sharifi, H., Bahaadinbeigy, K., et al. (2024). Virtual reality for cognitive disorders and dementia: A systematic review and meta-analysis. *BMC Psychiatry*, 24, 678. <https://doi.org/10.1186/s12888-024-05989-7>
- [27] Al-Emran, M., et al. (2024). Virtual, augmented reality and learning analytics impact on learners and educators: A systematic review. *Education and Information Technologies*, 29, 19913-19962. <https://doi.org/10.1007/s10639-024-12602-5>
- [28] Pellegrino, G., Gervasi, M., Angelelli, M., & Corallo, A. (2025). Digital twins to increase sustainability throughout the system life cycle: A systematic literature review. *Information Systems Frontiers*, 27, 7-32. <https://doi.org/10.1007/s10796-024-10536-4>
- [29] Isaza Domínguez, L. G. (2024). Digital twins for Industry 5.0: A systematic literature review. *Engineering Proceedings*, 82(1), 5. <https://doi.org/10.3390/engproc2024082005>
- [30] World Economic Forum. (2023). The Future of Jobs Report 2023. World Economic Forum.
- [31] Viswanathan, R., & Telukdarie, A. (2021). A systems dynamics approach to SME digitalization. *Procedia Computer Science*, 180, 816-824. <https://doi.org/10.1016/j.procs.2021.01.331>

Biography

Mohammed Jahed Sarwar is a Senior Systems Administrator and doctoral candidate (Doctor of Business Administration, Information Systems Management). His work focuses on digital transformation governance, secure cloud and cybersecurity operating models, and the expansion of inclusive learning ecosystems through resilient IT architectures and responsible AI practices.

Research Field

Mohammed Jahed Sarwar: Digital Transformation; IT Service Management; Cloud Platforms; Cybersecurity Governance; Responsible AI; Digital Learning Ecosystems.