

A Literature Review on Digital Transformation Challenges: Saudi Vision 2030

Heba Ahmed Allathy^{1*}, Ali Nasser Al-Tahitah²

Faculty of Leadership & Management, Universiti Sains Islam Malaysia, Nilai, Malaysia

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.101800008>

Received: 06 March 2026; Accepted: 16 March 2026; Published: 20 April 2026

ABSTRACT

Digital transformation has progressed from an aspirational theme to a system-wide mandate in Saudi Arabia's Vision 2030, where it supports economic diversification, innovation and sustainable development. This literature review combines up-to-date research and policy sources to analyze the principal challenges that govern digital transformation in the Kingdom. The review uncovers structural and organizational barriers, including institutional resistance to change, capability and skills gaps, cybersecurity risk, interoperability and data governance complexity, procurement constraints and uneven infrastructure readiness level across regions. It then looks at the implications of these challenges in terms of sectoral priorities by the Government, the health care sector, the educational sector, the tourism sector, SMEs and small enterprises in particular - some of the progress, some of the bottlenecks. Finally, it sets out evidence-informed recommendations for policymakers and leaders to mitigate risks while ensuring the implementation of all this in line with the outcomes of Vision 2030 through coherent governance, secure adoption of the cloud, human-centered talent pipelines, and human-centered service design. By compiling information from credible sources since 2018, the paper provides an integrated map of barriers and levers that may be used to strengthen the digital ecosystem in Saudi Arabia for the next phase of Vision 2030.

Keywords: digital transformation, sustainable development, innovation, organizational change, Saudi Arabia, Vision 2030.

INTRODUCTION

Saudi Arabia's Vision 2030 positions digitalization as the driver of national change, directly linked to diversification of non-oil GDP, strengthening competitiveness at a global level and improving public services. National plans to have the Kingdom as one of the best digitized governments by 2030 and expand the contribution of the digital economy to GDP, scale sectoral delivery of data- and AI-enabled services and strengthen the resilient national cyberspace for citizens and businesses (Digital Government Authority 2024; National Cybersecurity Authority 2022). These documents situate digital transformation, not as a discrete improvement of the technology but as a whole-of-government transformation that requires synchronization of regulation, common platforms, and capacity building. They also speak to user-centric design and design with security as requisites for trust, indicating that widespread adoption needs to be a step in parity with privacy, security and ethical guarantees built into delivery pipelines (Digital Government Authority, 2024; National Cybersecurity Authority, 2022).

Recently, however, there have been some concrete gains. Saudi Arabia has risen in the E-government ecosystem of the United Nations and ranked amongst world leaders by sub-indices like digital services and e-participation in 2024 and topped the region in ESCWA's Government Electronic and Mobile Services Maturity Index (Digital Government Authority, 2024; United Nations Department of Economic and Social Affairs, 2022). These achievements validate the trajectory and bring the bar higher for a resilient execution at scale. As digital services

become more integrated and proactive, their common service component of reliable uptime, openness in access within underserved communities, and transparency in their governance of the data becomes stronger. International guidance emphasizes the importance of keeping momentum by fostering inclusivity and building trust through design up to and including operation, rather than as afterthoughts or compliance exercises (Digital Government Authority, 2024; OECD, 2023; UN DESA, 2022).

But it is digitalization that remains Poire's centrepiece for diversification, aided by macroeconomic signals. Non-oil activities prompted a miracle of development in recent times, the domestic ICT market has surpassed SAR 180 billion in 2024 and official statements show that the output of digital economy exceeds the line of 15 percent of GDP, reflecting the appetite for infrastructure, platforms and skills (Communications, Space and Technology Commission, 2025; Ministry of Communications and Information Technology, 2025; Reuters, 2025). Yet it is the speed at which changes are being made that creates operational headwinds. As legacy systems are developed to be cloud-based and new services are launched, there must also be a transition to appropriate modern data governance, building on secure digital public infrastructure scaled to address the needs of these organizations, and the development of a skilled workforce to provide and support the new services. These activities are challenging to undertake at any time, but they are especially challenging in the context of rapid policy change and multi-sector reform agendas. Global and national analyses reveal bottlenecks in terms of interoperability, change management, cybersecurity readiness, and the implementation of privacy and data sharing rules in practice, so that it can still support innovation without removing rights (Digital Government Authority, 2024; Saudi Data and AI Authority, 2023; World Bank, 2023).

Digital transformation under Vision 2030 can be interpreted through two complementary lenses that clarify why adoption patterns differ across sectors. The Technology–Organization–Environment framework explains adoption as the joint outcome of technological characteristics, organizational capabilities and external pressures. In the Saudi context, this means cloud maturity, data quality, skills, budgeting practices and vendor ecosystems interact with regulatory requirements and national targets to shape choices by ministries, hospitals, universities and firms (Tornatzky & Fleischer, 1990). Where technology is modular and standards are clear, agencies move faster. Where organizational skills and governance are weak, the same technology produces uneven results. Institutional Theory helps explain convergence and inertia that appear once policies, audits and rankings begin to bite. Formal rules and normative pressures create isomorphic practices across ministries and sectors. The upside is coherence in standards and controls. The downside is compliance-first behavior that can slow user research and iterative delivery if incentives and procurement models do not reward learning and outcomes (DiMaggio & Powell, 1983). Taken together, TOE and Institutional Theory suggest that sectors with strong mandates and shared platforms can convert strategy into services quickly yet must guard against over-engineering for compliance, while sectors with lighter mandates can innovate rapidly but risk fragmentation without common data and consent standards.

Against this context, the current paper summarizes the literature to highlight critical issues from both the academic and policy perspectives and determine their implications for the realization of Vision 2030. Secondly, the paper synthesizes the various academic papers, government strategies and multilateral organization analyses to chart the major roadblocks to digital transformation in the Kingdom. The methodology section describes the design of the review, which includes criteria for sources of information and the criteria for selection, with an emphasis on recentness and credibility. Findings and discussion provide an interpretation of patterns across priority sectors, making links between organizational, technical and regulatory themes. The conclusion is a translation of insights gained into what policies can do in the long run, while also providing guidelines for any further research that can help keep the momentum going and enhance inclusion, resiliency, and trust (Digital Government Authority, 2024; World Bank, 2023).

LITERATURE REVIEW

Conceptualizing digital transformation under Vision 2030

Digital transformation in Saudi Arabia cannot best be described as a limited technology rollout but is measured by an institutional redesign. The guidance offered by the Organization for Economic Cooperation and

Development positions digital government as a human-centered reconfiguration of the public sector based on the alignment of policy, data stewardship, workforce capability and service design to deliver consistent value at scale (OECD, 2023; OECD, 2025). This approach moves from systems per se to explore what created the systems: the operating model, which should pay more attention to the outcome measures, is very iterative, and also the participation of the users throughout the service life cycle. Saudi policy has internally adopted this system's interpretation by developing a governing culture that is able to unify transformation across ministries and regions. The creation of the Digital Government Authority created a regulator and orchestrator for standards, compliance and platform choices that allow for common reference architectures and maturity models, leading to less fragmentation and reuse of standards (Digital Government Authority, 2024; Digital Government Authority, 2025). The DGA defines the framework of policies that guide agencies in how to integrate cloud services, build interoperable digital experiences life cycle, and model service quality to lead efforts to transition the state from project-based digitalization to platform-based, portfolio-based digitalization.

The second basic pillar is data and AI governance. The Saudi Data and AI Authority has developed and advanced a layered regime, consisting of the Personal Data Protection Law, implementing regulations, a national data management framework, and updated guidance on cross-border transfers. These instruments aim to balance innovation and privacy by establishing legal grounds for processing data, creating transparency on consent and limitation of purposes, as well as introducing risk-based measures for international data flows vital for cloud and AI ecosystems (Saudi Data and AI Authority, 2023; Saudi Data and AI Authority, 2024). Cybersecurity can fill out the triad of enablers: The national strategy and the sectoral controls defined by the National Cybersecurity Authority to specify the baseline obligations for public bodies and operators of essential service providers produce a common language for risk management, incident reporting and assurance in a complex, supplier landscape (National Cybersecurity Authority, 2022; National Cybersecurity Authority, 2024). Together, these institutions can bring the policy coherence and trust infrastructure that the OECD defines as preconditions for human-centered digital government, which links technical choices back to public value, respect for human rights and skills building for institutional scaling.

Table 1: Summary of Digital Transformation Challenges in Saudi Arabia

Category	Key Challenges	Sector Impact
Organisational	Resistance to change, skills gaps	Education, SMEs
Technological	Legacy systems, interoperability	Healthcare, Government
Regulatory	Data governance, compliance complexity	All sectors
Socio-economic	Digital divide, affordability	Rural areas, SMEs

Indicators of progress and remaining gaps

Ranking high in the United Nations E-government platform in 2022 and improving greatly in 2024, including the world's fourth digital service, and high regional ranking, the country's investments in platforms and license integration to unite services resulted in a high evaluation in all four technical aspects of digital government (UN DESA, 2022; DGA, 2024; Arab News, 2024). The World Bank's 2022 GovTech Maturity Index ranked the Kingdom as one of the most advanced governments regarding the core systems, service delivery and enablers, although ongoing citizen engagement across the government, and capacity within the ecosystem, remain highlighted focus areas (World Bank, 2022; SPA, 2022). The result of this shows momentum as well as friction in those local industries. In providing healthcare, the Seha Virtual Hospital is an example of scaled telemedicine and virtual care; however, on the path to providing these services, integration, equity, and data security must be kept up for continuous improvement as services grow (Financial Times, 2025; Suleiman, 2025). From the literature of studies of education, it was reported that adoption in ministries and universities depends on leadership, management, and the capabilities of its administrative staff, and that the opponent's resistance, isolated systems, and procurement regulations emerge as obstacles (Alojail, 2023; Alsulami et al., 2024). For SMEs, readiness and awareness is correlated with performance; however, the constraints around skills, financing, cybersecurity, and the digital divide can increase inequalities if not addressed (Tripathi et al., 2024; Muhammad et al., 2025). In tourism, digitized visas, marketing and smart destination services are working to

support Vision 2030 goals, although keeping the data governance and quality of service under control and consistent across regions is a priority (Almakaty, 2025).

Core challenge themes in the literature

Public organizations and institutions of higher education in Saudi Arabia are dealing with a constant execution gap between ambitious digital strategies and daily realities. Misaligned steady state: multifaceted bureaucracy, multiple approvals, and risk-averse cultures act as speed breakers in the culture, reducing the incentives to experiment and, in effect, making user research, rapid prototyping and continuous iteration necessary for delivering services of the 21st century (Alojail, 2023; OECD, 2023). When design choices are put through hierarchical committees instead of multidisciplinary product teams, user needs fall to the wayside, overshadowed by checklists for compliance and waterfall plans, in service of the dream of human-centered service. There is worldwide recognition that real change requires a user-centered approach and outcome-based measures embedded within governance and funding frameworks that allow teams to safely iterate while not reducing accountability (OECD, 2025). At the same time, the skills required to carry out this shift are uneven. Lack of cloud engineering prowess, cybersecurity, data science, product management, and service design capabilities is a hurdle to the replatforming of core systems and scaling data-driven services. Bodies of knowledge from multi-lateral reviews and sector-specific studies all indicate a need for continuous, large-scale upskilling, greater flexibility in hiring, and competency models (aligning job functions to agile delivery practices) in public line-of-business success (Suleiman, 2025; World Bank, 2023).

Acceleration gives rise to increased cyber risk exposure. The National Cybersecurity Strategy, together with its accompanying sectoral controls, creates a deep policy backbone, while capacity-building programs aimed at raising the level of defensive posture across government and critical sectors (NCA, 2022). Nevertheless, the literature points to practical challenges to synchronize governance, budgets and specialist talent across different entities, including small and medium-sized suppliers that constitute essential links in public service value chains (Saudipedia, 2024). Data protection is another level of organizational maturity. The Personal Data Protection Law and sectoral data standards will be the next milestone, but to be successful in gathering the required consents, limiting purposes and cross-border data transfers, and controlling the lifecycle of data to maintain its analytic utility at the expense of rights (Clyde & Co., 2024; SDAIA, 2023), acceptance mechanisms are needed. Technology decisions transcend these limits. Whole-of-government platforms and Cloud First approach are a potential promise to avoid interoperability and reuse; however, migration speeds will differ due to stiff procurement, multistate integration of legacy estates and risk management requirements in sensitive sectors such as health and justice (Alkhasawneh, 2025; CST, 2023-2025; DGA, 2024; European Scientific Journal, 2025). Finally, connectivity initiatives that combine both terrestrial and non-terrestrial networks are narrowing the geographical gaps, but affordability and skills divide abound. Implementing complementary social policies, currently low broadband subscription rates, and community-level support will be required in order to make the benefits of digital government enjoyable for all regions and social demographics (ITU WSIS Country Report, 2025; World Bank, 2023).

Across health, education, tourism and SMEs, the literature shows common enablers and distinct frictions. Governance clarity is strongest in health because national programs and shared platforms anchor decisions, while universities and school systems report slower approval cycles that hinder iterative delivery and product-team ways of working (Alojail, 2023). Data governance pressure is highest in health and tourism due to sensitive health information and cross-border marketing data, whereas many SMEs are still building basic data management maturity and rely on external providers for security and analytics (Almakaty, 2025; Tripathi et al., 2024). Cybersecurity exposure increases with digital scale. Virtual care, remote monitoring and fintech expand the attack surface, while a significant subset of SMEs operates with minimal third-party risk management and incident response (Suleiman et al., 2025). Interoperability hurdles appear where legacy estates are deepest, notably in education registers and hospital EHRs, which require API-first refactoring and data standards to unlock reuse. Tourism applications align faster with cloud-native patterns but need consistent consent flows and analytics governance across operators to maintain trust at scale (Digital Government Authority, 2024; Al-Anezi, 2025). Human capital gaps are transversal. Product management, service design and secure cloud engineering are scarce across sectors, with SMEs additionally constrained by financing for upgrades and leadership capacity

to manage change (World Bank, 2023; Tripathi et al., 2024). In synthesis, sectors with clear program governance and reusable platforms move faster yet face sharper requirements for privacy-by-design and cyber resilience, while lighter-legacy sectors adopt quicker but require standardized data and consent practices to avoid fragmentation.

CONCEPTUAL FRAMEWORK

The Technology Organization environment (TOE) theory coupled with Institutional Theory are the drivers of this study. TOE framework describes the digital transformation in terms of three dimensions:

- Infrastructure, cloud computing and cybersecurity are technological factors.
- Organizational variables such as leadership and skills, and the organizational culture.
- Regulations, policies, and initiatives of the Vision 2030 on the environment.

This is supplemented by Institutional Theory which explains how governance structures and regulatory pressures affect organizational behavior and frequently contribute to compliance generated strategies. This integrated framework gives an organized perspective to examine and evaluate the issue of digital transformation in the various domains in Saudi Arabia.

RESEARCH METHODOLOGY

This review takes an integrative approach to conducting a literature review of peer-reviewed articles, multilateral reports, official strategies, and regulatory documents from 2018 onwards. Credibility and recency were the order of the search, with the search focusing on sources from the OECD, the United Nations, the World Bank, Saudi public authorities and reputable academic publishers. The search strategy included database searches and targeted web searches for sectoral studies in the healthcare, education, tourism and SMEs. Inclusion criteria: articles have been included if they were substantive, discussed digital transformation in Saudi Arabia, related to Vision 2030 and explicitly focused on barriers, risks or implementation challenges. Non-Saudi contexts, advertising, and sources that were older than seven years, if they did not provide the necessary context, were excluded. Where more than one source reported on the same indicator, the researchers preferred official sources or multilateral sources. The synthesis technique of thematic analysis was used to group results into organizational, technical, regulatory and socio-economic categories and sector evidence was cross-checked against the national context. This approach enables triangulation between policy and practice, recognition that fast-changing reform regulatory developments can move beyond the space of the literature.

This paper follows a systematic integrative literature review method to consider the issues of digital transformation in Saudi Arabia within the framework of the Vision 2030. Sources were drawn from Scopus and Web of Science for academic evidence, from OECD, UN DESA and World Bank repositories for multilateral assessments, and from official Saudi portals for policy and regulatory texts, including the Digital Government Authority, the Saudi Data and AI Authority, the National Cybersecurity Authority and the Communications, Space and Technology Commission. Targeted web searches captured sectoral analyses in health, education, tourism and SMEs. Search strings combined subject, setting and outcome terms. Examples included “Saudi Arabia” AND “digital transformation” AND “Vision 2030,” “GovTech” AND “Saudi,” “personal data protection” AND “Saudi,” “telemedicine” AND “Saudi,” and “SMEs” AND “digital readiness” AND “Saudi.” Inclusion criteria required that sources analyse digital transformation in Saudi Arabia, discuss barriers, risks or implementation challenges, and be dated 2018 or later. Older seminal frameworks were retained only when needed for theory or constructs. Exclusion criteria removed non-Saudi contexts, promotional content and items lacking methodological transparency

The thematic analysis method was used to summarize the results into four major categories, including organizational, technological, regulatory, and socio-economic challenges.

Such systematic approach enhances transparency, reliability and reproducibility of the study.

FINDINGS AND DISCUSSION

Governance, coordination, and institutional change

The creation of the Digital Government Authority and the issuance of intergovernmental policies in Saudi Arabia were steps towards improving the orchestration of digital activities and ensuring compliance standards. Policies have been introduced for service maturity, cloud usage, data sharing, and open government, and they all provide a shared language for agencies and suppliers (DGA, 2024; DGA, 2025). Nevertheless, qualitative research in the education sector and research into government transformation highlights the role of structural hierarchies, legacy approval cycles, and risk management practices in acting as barriers to decisions and discouraging experimentation. Leadership buy-in is present, but mid-level management incentives and procurement policy and procedures need to be harmonized to maintain delivery speed (Alojail, 2023; OECD, 2023). In practice, this translates to long lead times to get shared platforms up and running to re-engineer the end-to-end services around the user journey instead of the agency silos, etc. A system-level implication is that improvements in governance have to be accompanied by operational tooling and metrics that incentivize including, delivering, and iterating, service reliability, and user satisfaction. The guidance of the Organization for Economic Cooperation and Development (OECD) on digital government focuses on outcome-oriented governance and human-centered design to reduce the gap between institutional policies and service experience (OECD, 2025). The UN and World Bank indicators provide much evidence of capability yet also contain a constant of citizen engagement and inclusion, particularly as the provision of services moves to proactive, data-driven models (UN DESA, 2022; World Bank, 2022).

Cybersecurity and resilience

As digital services scale, cybersecurity has a foundational role to play in building public trust and continuity of essential services. The National Cybersecurity Strategy provides a vision for secure and trusted cyberspace with sectoral and operational controls. Industry analyses and national portals feature supporting initiatives to localize cybersecurity talent and technologies (NCA, 2022; Saudipedia, 2024). Yet there exists in the literature mixed capacity and cost limitations among organizations, even more so, with small and certain types of non-health-based public providers. This unevenness runs the risk of creating weak links in the supply chain and ecosystem partnerships. Strengthening third-party risk management, incident reporting, and red team exercises in government and regulated sectors would mitigate this risk. The acceleration of virtual care and remote monitoring in the health sector and novel financial technologies increases the attack surface, and privacy-by-design and secure DevSecOps practices become essential, according to the Financial Times. 2025 Suleiman.

Data governance, privacy, and cross-border flows

The coming into force of the Personal Data Protection Law in September 2023, with the full enforceability due date being after the one-year transition, is indeed a pivotal step. Putting in place regulations, increased transfer rules and common contractual clauses, organizations can be given a mechanism to process data lawfully and keep international operations running (SDAIA, 2023; Clyde & Co., 2024; Morgan Lewis, 2024). At the same time, conventions being developed by the National Data Management Office, the SDAIA NDMO, are being applied to institutionalize data lifecycle practices and metadata management governance (Office of the National Data Management Officer 2020s). The challenge is to do it on a large scale. Many agencies and private ones have to retrofit systems for consent, purpose limitation, breach notification, and data subject rights, as well as enable analytics for public value. Interoperability tensions, e.g. between data localization requirements and cross-border service models can be present in the case of cloud and AI services. Ambiguous rules regarding cross-border mobility and rights-based filtering can make the life safer. However, as noted in World Bank's digital development progress reports, data governance as much as infrastructure is required for the sustainable development of inclusive digital economies (World Bank, 2023).

Cloud adoption, interoperability, and platformization

Cloud computing is one of the pillars of agile public services. The Kingdom's policies are supportive of cloud migration and "whole-of-government" platforms to re-use capabilities such as identity, payments, messaging

and case management. Government publications outline the potential cost and reliability benefits of cloud, and guidance in the education sector offers strategies for secure transformation (DGA, 2024; DGA, 2025). At the same time, empirical and conceptual studies show that there are hurdles such as rigid procurement models, data classification and residency questions, and integration with legacy systems not designed for API-first (European Scientific Journal, 2025; CST Cloud Outlook, 2023). One way to do this is to deploy a combination of a strong policy backbone with common technical patterns - reference architectures, NCA controls-based security baselines, and market models that permit vetted providers to deliver microservices on national platforms. This decreases fragmentation and improves interoperability between ministries. The World Bank (2022) and OECD (2023) report that there are evidence-based models that can be leveraged for an accelerated, safer journey to transformation (GovTech and OECD frameworks).

Human capital and change management

Digital transformation is successful when people and processes change at the same time as technology. Challenges over staff preparations, training, and motivation are documented in studies of ministries and universities. Interviews in the education sector identify critical success factors such as leadership sponsorship, governance clarity, and targeted professional development as key issues without which resistance to change and a lack of skills slow down the implementation process (Alojail, 2023; Alsulami et al., 2024). The national initiative to bring in AI curricula at scale and scaling up VET programs implies a strategic reaction; it would be a question of scale and impact of the curricula and work-based learning pathways, which will be crucial in terms of the long-term legacy (Times of India, 2025; World Bank, 2025). In reality, successful change management in public entities in Saudi Arabia will require multi-year capability programs that balance human resource policies against agile delivery roles, incentives for innovation, and communities of practice for sharing lessons across agencies. Empirical evidence shows that such socio-technical investments are on par with infrastructure investments in determining medium-term sustainability (OECD, 2025).

Inclusive access, connectivity, and the digital divide

A key component of legitimate and effective transformation in Saudi Arabia should be to make digital services accessible and usable for all. According to the ITU WSIS Country Report 2025, it can be concluded that terrestrial connectivity build-outs are increasingly linked with non-terrestrial solutions such as low-EOC satellites and HAPS to get coverage to sparsely populated or geographically challenging areas to directly support Vision 2030 inclusion objectives provided by National Connectivity initiatives led by CSTC. Coverage, though, is just the beginning. Inclusion is multidimensional and includes elements of affordability and access to devices, digital skills, and culturally and linguistically appropriate service design. Telemedicine interfaces, e-booking, and developing remote monitoring systems must treat universal device ownership, good bandwidth, high digital skills, and a background that is able to have the tendency to widen differences between older adults, low-income people and remote living elements, which is indicated by the health sector (Suleiman, 2025).

Closing these gaps involves a coordinated policy mix that contains correspondence between infrastructures and human support and rights-based design. Being assisted by information and communications with another person, in municipal offices, in hospitals, and in community centers, in finishing online transactions: Content, navigation and authentication requirements for accessibility presume low-level literacy and disability. Standard of accommodation in ITU WSIS Country Report, 2025. Localized pro bono and non-profit institutional experiences can adapt training and gain trust in community needs, and specialized subsidized data packages and devices with programmatic features can solve for cost platforms where coverage is not adequate (Suleiman, 2025). To ensure equity remains at the heart of platforms as they change, governments and providers must track outcomes using disaggregated indicators across geography, gender, age, disability, and income, horizontally linking to decisions regarding how to modify services and where to allocate resources so that the modernization process enhances, not impedes access for vulnerable groups (ITU WSIS Country Report, 2025; Suleiman, 2025).

Sectoral perspectives

Saudi Arabia's leaps in UN and World Bank indicators are a result of the success of national platforms and service integration. ESCWA's Global Education and Network Systems (GEMS) and DGA remain robust and

regularly positioned with regional leadership (DGA, 2023 - 2024). The challenge that now remains is getting to the point where you can maintain your reliability and user satisfaction while moving trends towards a proactive and life event-based service that relies on safe data sharing and automation around eligibility checks. This necessitates the use of privacy-enhancing technologies, strong consent management and ongoing user research, which have to become part of a delivery pipeline in procurement templates (SDAIA, 2023; OECD, 2025).

The health transformation program uses digital tools for accessibility and quality. Seha Virtual Hospital shows that the operational scalability, digitalization of the healthcare system, integration of electronic health records, interoperability and cybersecurity are great areas for work to do, considering the data volumes and AI use cases will increase in the near future (Financial Times, 2025; Al-Anezi, 2025). Furthermore, telemedicine and remote monitoring services should be developed to ensure clinical safety, algorithmic transparency and equitable access. Registration alignment of compliance to PDPL obligation with health data standards requires a Ministry-level activity, demonstrating increased digital adoption, while unequal capability and cultural resistance are common themes when looking at the university endeavors. The leadership, governance clarity and professional development (Alojail, 2023) are discovered in qualitative research as make-or-break factors for adoption. The trend of including AI as a part of primary education can help instill the digital talent pipeline if spearheaded with teacher training, industry partnership, and experiential learning (Times of India, 2025).

Vision 2030 makes tourism a diversification engine. Research and preprints include various aspects of what e-visas, tourism apps and digital marketing could do to both improve their discovery and experience, while also setting the bar to have data protection for this use across public and private operators. There is a need for consistent standards of consent, analytics, and cross-border marketing technologies in order to prevent risk of defacing trust as the sector is scaled (Almakaty, 2025). SMEs are at the core of job creation and innovation. Evidence available suggests that awareness and preparedness correlate with performance, but the barriers include access to finance to upgrade digitally, cybersecurity preparedness and managerial skills. Without targeted support, the same technologies that help achieve scale can be used to widen divides between firms that have the digital readiness and those that are digital laggards (Tripathi et al., 2024; Muhammad et al., 2025). Policy leavers - global and local - include streamlined compliance for SMEs, shared cybersecurity services, or a digital voucher for cloud and SaaS adoption.

Macroeconomic and ecosystem signals

The recent growth in the non-oil sectors of the economy in Saudi Arabia and constant inflows of foreign direct investment is indicative of rising investor confidence and better growth prospects in the services, manufacturing, logistics, and tourism sectors. These macro signals are reinforced by the Kingdom's participation in frontier initiatives such as cross-border central bank digital currency pilot, entrusting Saudi institutions in the rule-making of experiments of interoperability on the shaping of next-generation financial rails (Reuters, 2024; Reuters, 2025). In practical terms, these projects have the power to reduce frictions on international settlements, decrease the cost for exporters and SMEs and catalyze the building of ancillary fintech services that ride off the programmable money and the real-time data exchange. As these networks wind up, they're poised to lift the U.S. monetary association with top business partners and increase the need for Cybersecurity, Privacy, and speed (and academic consistencies) in both public and private players contributing to installments and cleansing (Reuters, 2024; Reuters, 2025). Parallel movement can be seen in the domestic ICT market that has exceeded SAR 180 billion in 2024 and is still accelerating in the following quarters based on cloud adoption, platform integration, and AI-enabled services that generate demand for system integrator/vendor, cybersecurity, and software startups (Communications, Space and Technology Commission, 2025). Yet the accelerated growth in the market raises policy issues. In order to avoid vendor lock-in and maintain long-term public value, procurement regimes, as well as technical and architectural standards, should prioritize open APIs, portability and outcome-based contracting that favors reliability of services and user satisfaction, instead of hardware volume (Digital Government Authority, 2024). A strong competition policy that ensures monitoring of concentration in markets for cloud and platforms can ensure that there is healthy entry of local innovators, while harmonized skills programs in cybersecurity, data engineering, and product management will ensure that firms are capturing value rather than outsourcing it (Digital Policy Alert, 2024; DGA, 2024; CST, 2025). Together, those measures can turn macro-level confidence into new-layer digital ecosystems that promote Vision 2030 diversification goals.

CONCLUSION

Saudi Arabia's digital transformation since the launch of Vision 2030 shows some remarkable progress in global indices, market growth, and flagship services. The country has been able to develop a solid policy and institutional ground for language acquisition, Sign Languages for Education and Audition, and an investment in platforms, connectivity, and sectoral reforms. The literature reviewed here converge on a set of persistent challenges that need to be overcome for the progress to persist, such as institutional resistance and process inertia, uneven digital skills and change management capacity, cybersecurity expose and risks of third-party engagement, complex data governance and cross-border flow of data, integration and interoperability challenges associated with migrating to the cloud, and inclusion gaps that could increase and further fragment divides. These issues cannot be addressed by incoordinately focusing on technology procurement but must be tackled with a synchronized approach focusing on governance, capabilities, and user-centered delivery.

Directions for Future Research

First, the researchers should assess the PDPLs' compliance with innovation outcomes, including how privacy-enhancing technologies and risk-based transfer mechanisms affect analytics and AI adoption, as well as international trade. Second, longitudinal studies that monitor the impact of whole-of-government platforms on service reliability, costs, and user satisfaction across the ministry should be conducted, in order to better understand the conditions under which shared platforms accelerate service delivery or slow it down. Third, health and education need to be evaluated in detail in terms of digital equity, in terms of differential access, outcomes, and trust by region and demographics. Fourth, SME-focused research can be used to test the efficacy of vouchers, managed cybersecurity services and digital sandboxes in increasing adoption without imposing disproportionate burdens. Finally, comparative analyses within the GCC and within the OECD can help shed light on the role that procurement models, capability pipelines and ecosystem governance play in how quickly and how resilient transformation unfolds. By basing policy experimentation on rigorous evaluation and open data, the Kingdom will be able to continue to align digital transformation with Vision 2030's goals of prosperity, inclusion, and sustainability.

REFERENCES

1. Al-Anezi, F. M. (2025). Challenges of Healthcare Systems in Saudi Arabia to Delivering Vision 2030: An Empirical Study From Healthcare Workers Perspectives. *Journal of Healthcare Leadership*, 173-187. <https://www.tandfonline.com/doi/abs/10.2147/JHL.S516159>
2. Almakaty, S. (2025). Tourism development and management in Saudi Arabia [Preprint]. Preprints.org. <https://doi.org/10.20944/preprints202501.1464.v1>
3. Alojail, M. (2023). Critical success factors and challenges in adopting digital transformation at the Ministry of Education in Saudi Arabia. *Sustainability*, 15(21), 15492. <https://doi.org/10.3390/su152115492>
4. Clyde & Co. (2024, September). Saudi Arabia's Personal Data Protection Law becomes enforceable: Next steps for compliance. <https://www.clydeco.com/en/insights/2024/09/saudi-arabia-s-personal-data-protection-law-become>
5. Communications, Space and Technology Commission. (2025, May 12). CST: 180B SAR is the size of the communications and technology market during 2024. <https://www.cst.gov.sa/en/media-center/news/N2025051201>
6. Digital Government Authority. (2024). Digital Government Policies, V2.0. <https://dga.gov.sa/sites/default/files/2024-03/Digital%20Government%20Policies%20-%20V2.0.pdf>
7. Digital Government Authority. (2024, July). Saudi Arabia ranks fourth in digital services and first regionally, UN EGDI 2024. <https://dga.gov.sa/en/news/Saudi-arabia-ranks-4th-in-digital-services>
8. Digital Government Authority. (2024, October). Digital Transformation Strategies Across Saudi Arabia (V1.0). <https://dga.gov.sa/sites/default/files/2024-10/Digital%20Transformation%20Strategies%20Across%20Saudi%20Arabia-%20V1.0.pdf>
9. Digital Government Authority. (2025, April). Effective integration of cloud computing in digital transformation of the education sector (V1.0). <https://dga.gov.sa/sites/default/files/2025->

- 04/Effective%20Integration%20of%20Cloud%20Computing%20in%20Digital%20Transformation%20of%20the%20Education%20Sector-V1.0.pdf
10. Financial Times. (2025, March 5). ‘Virtual hospitals’ deliver home treatment to remote patients. <https://www.ft.com/content/104151c3-f808-4c2d-a20a-b1394846772c>
 11. Morgan Lewis. (2024, September). Saudi Arabia Personal Data Protection Law: Transition period ends September 14. <https://www.morganlewis.com/pubs/2024/09/saudi-arabia-personal-data-protection-law-transition-period-ends-september-14>
 12. National Cybersecurity Authority. (2022). National Cybersecurity Strategy. https://nca.gov.sa/national_cybersecurity_strategy-en.pdf
 13. OECD. (2023). 2023 OECD Digital Government Index: Main findings. https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html
 14. OECD. (2025). Government at a Glance 2025: Digital Government Index. https://www.oecd.org/en/publications/2025/06/government-at-a-glance-2025_70e14c6c/full-report/digital-government-index_1edec44e.html
 15. Saudi Data and AI Authority. (2023). Implementing Regulations of the Personal Data Protection Law. <https://sdaia.gov.sa/en/SDAIA/about/Documents/ImplementingRegulation.pdf>
 16. Saudi Data and AI Authority. (2023, April). Personal Data Protection Law (English v2). <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>
 17. Saudipedia. (2024). Cybersecurity in Saudi Arabia. <https://saudipedia.com/en/article/196/economy-and-business/data-and-ai/cybersecurity-in-saudi-arabia>
 18. Suleiman, A. K., et al. (2025). Transforming healthcare: Saudi Arabia’s Vision 2030. *Journal of Medicine and Life*, 18(2), 110–120. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11753010/>
 19. Times of India. (2025, August 25). Saudi Arabia introduces AI curriculum for over six million students. <https://timesofindia.indiatimes.com/world/middle-east/saudi-arabia-introduces-ai-curriculum-for-over-six-million-students-as-part-of-vision-2030-goals/articleshow/123499532.cms>
 20. Tripathi, A., et al. (2024). SMEs’ awareness and preparation for digital transformation in Saudi Arabia’s Ha’il region. *Sustainability*, 16(9), 3831. <https://doi.org/10.3390/su16093831>
 21. United Nations DESA. (2022). UN E-Government Survey 2022: The future of digital government. <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/149-Saudi-Arabia/dataYear/2022>
 22. World Bank. (2022). 2022 GovTech Maturity Index update. <https://www.worldbank.org/en/programs/govtech/2022-gtmi>
 23. World Bank. (2023). Digital progress and trends report 2023. <https://openknowledge.worldbank.org/server/api/core/bitstreams/95fe55e9-f110-4ba8-933f-e65572e05395/content>
 24. World Bank. (2025, January 30). Saudi GDP grew 1.3 percent in 2024, lifted by non-oil sector [via Reuters]. <https://www.reuters.com/world/middle-east/saudi-arabia-gdp-grew-13-2024-govt-estimate-shows-2025-01-30/>