**ESI Preprints** **Not Peer-reviewed**

# Advancing Cloud Adoption in the Saudi Public Sector: Challenges, Global Insights, and Strategic Policy Recommendations

***Abdal Hafeth Alaraj***
International American University, USA

Doi: 10.19044/esipreprint.5.2025.p627

Approved: 28 May 2025
Posted: 30 May 2025



*Cite As:*
Alaraj A.H. (2025). *Advancing Cloud Adoption in the Saudi Public Sector: Challenges, Global Insights, and Strategic Policy Recommendations*. ESI Preprints.
https://doi.org/10.19044/esipreprint.5.2025.p627

## Abstract

Cloud computing has become a cornerstone of digital transformation strategies in the public sector, offering government entities scalable infrastructure, cost efficiency, and enhanced service delivery. In Saudi Arabia, adopting cloud technologies is a national priority aligned with Vision 2030, aiming to modernize government operations and increase digital agility. However, the transition to cloud environments within government institutions faces several challenges. This paper examines the key barriers to cloud computing adoption in Saudi Arabia's governmental sector. These include data governance concerns, cybersecurity requirements, organizational readiness gaps, and rigid procurement models. Through a comprehensive analysis of national frameworks and sector-specific studies, the paper highlights the root causes of slow adoption and identifies opportunities for improvement. The study also draws comparative insights from global practices, offering lessons that can inform local strategies. Based on the findings, practical recommendations are proposed to support more effective cloud adoption in the Kingdom's public sector. These focus on governance enhancement, capacity building, policy alignment, and fostering a cloud-positive culture within institutions.

**Keywords:** Cloud Computing, Government Sector, Public Sector Transformation, Saudi Arabia, Cloud First Policy, Data Sovereignty, Digital

Government, Cloud Adoption Challenges, Cybersecurity in Cloud, Vision 2030

## Introduction

Cloud computing is transforming how governments operate and deliver services. It provides public institutions with scalable, on-demand infrastructure, offering the potential to reduce costs, enhance flexibility, and modernize service delivery. Globally, cloud technologies have become essential components of government digital strategies as agencies move away from traditional systems in favor of more secure and efficient environments.

In Saudi Arabia, cloud adoption supports the goals of Vision 2030, which seeks to expand the digital economy, improve government efficiency, and foster innovation. The Cloud First Policy advances this agenda by urging ministries and agencies to prioritize cloud-based solutions in all new technology initiatives. Supporting this policy is a regulatory ecosystem that includes data governance rules, cybersecurity standards, and standardized service models.

Despite this strategic direction, implementation remains uneven across government entities. Many organizations face structural and operational challenges that slow progress. These issues include legacy procurement systems, internal resistance, limited technical capacity, and complex compliance requirements. As noted in one national report, "government agencies face challenges in cloud adoption due to fragmented internal processes and varying digital capabilities" (NCA, 2022). These gaps show the importance of focused actions to turn national policy into practical steps at the institutional level.

This paper explores the current landscape of cloud computing adoption in Saudi Arabia's government sector. It analyzes institutional, regulatory, and technical barriers, reviews relevant literature and policy frameworks, and offers strategic recommendations tailored to the national context.

## Literature Review

Cloud computing is regarded as a foundational element in modernizing government services worldwide. Its ability to streamline infrastructure, improve agility, and reduce costs makes it an attractive option for public sector transformation. Nevertheless, adoption is frequently hindered by various internal and external factors. The literature identifies issues related to data security, regulatory uncertainty, technical complexity, and organizational readiness.

Among the most persistent concerns are data privacy and security. Government institutions often handle sensitive citizen information, making them particularly cautious about migrating services to the cloud. One study found that "security, privacy, and loss of governance are still the main obstacles for adopting cloud computing technology" (Majid Al-Ruithe, 2018). These concerns are especially prominent in environments with strict national data regulations, such as Saudi Arabia.

Institutional capacity also plays a critical role. A government report noted that "adoption efforts remain uneven due to varying levels of maturity, leadership support, and internal technical readiness" (CITC, 2023). This inconsistency suggests that policy mandates alone are insufficient to ensure widespread adoption; organizations must possess the skills, tools, and change-readiness to act on those policies.

Other studies echo the challenge of limited internal expertise. For instance, a lack of cloud awareness and IT proficiency in higher education institutions has hindered implementation. A sector-specific review reported that a "lack of awareness and technical knowledge" significantly delayed cloud projects in Saudi universities (Fatani, 2021).

Several countries have addressed these barriers internationally through coordinated national strategies. The United Kingdom, for example, launched a G-Cloud framework to simplify procurement and ensure secure access to pre-approved vendors. Singapore's GovTech model and the UAE's cloud zones similarly prioritize standardization and security compliance.

Furthermore, technological infrastructure is a determining factor in effective cloud deployment. According to a strategic outlook report, "the increasing enterprise adoption of cloud-based solutions necessitates high-performance, secure, and scalable connectivity" (Khan, 2025). These requirements pressure national networks and data centers to evolve alongside digital government initiatives.

Overall, the literature suggests that cloud adoption in the public sector depends on regulatory guidance and institutional capacity, trust frameworks, and technological readiness. In Saudi Arabia, these findings highlight the need to match policy goals with the ability to carry them out effectively on the ground.

**Saudi Arabia Context**

Saudi Arabia's public sector is undergoing a strategic digital transformation as part of its Vision 2030 agenda. A key element of this transformation is the broad use of cloud computing technologies to enhance government efficiency, improve service delivery, and support data-driven decision-making. To operate this shift, the government introduced the Cloud

First Policy in 2020, which serves as the primary directive for cloud adoption among government entities.

The policy requires that public institutions adopt a tiered approach to cloud service deployment. Specifically, "government entities must always prioritize Cloud solutions in the following sequence: first Software as a Service (SaaS), then Platform as a Service (PaaS), and lastly Infrastructure as a Service (IaaS)" (KSA Cloud First Policy, 2020). This structure is intended to reduce complexity, optimize performance, and minimize the cost and time of implementation.

Regulatory and operational oversight of the Cloud First Policy is distributed among several national bodies. The Digital Government Authority (DGA) is responsible for policy guidance and digital maturity assessment. The National Cybersecurity Authority (NCA) enforces cybersecurity compliance through instruments such as Cloud Cybersecurity Controls (CCC). The National Data Management Office (NDMO) ensures proper data classification and information governance, while the Communications, Space & Technology Commission (CST) regulates cloud service providers and enforces licensing and operational standards.

Regulatory and operational oversight of the Cloud First Policy is distributed among several national bodies. The Digital Government Authority (DGA) provides policy guidance and digital maturity assessment. The National Cybersecurity Authority (NCA) enforces cybersecurity compliance through Cloud Cybersecurity Controls (CCC) instruments. The National Data Management Office (NDMO) ensures proper data classification and information governance. At the same time, the Communications, Space & Technology Commission (CST) regulates cloud service providers and enforces licensing and operational standards.

Another barrier is the variation in digital readiness among different agencies. Some ministries have successfully initiated migration strategies, while others rely on legacy infrastructure. This inconsistency was acknowledged in a national digital guideline, which emphasized that "agencies must evaluate cloud readiness across technical, security, and data classification dimensions before initiating migration" (DGA, 2023). In practice, many agencies lack the internal capacity or governance models to perform such evaluations effectively.

A study on national digital architecture further explained that "digital transformation programs must address differences in institutional capacity and establish a common governance baseline to ensure consistent outcomes" (SDAIA, 2024). Without this consistency, cloud migration efforts risk being fragmented, delayed, or mismatched with national strategies.

While Saudi Arabia has made significant progress in developing policy frameworks and infrastructure, the operationalization of cloud

adoption remains uneven. Bridging this gap will require more substantial alignment between national strategy and agency-level execution, supported by tailored governance models, shared platforms, and capacity-building initiatives.

**Key Challenges in Saudi Government Cloud Adoption**

In Saudi Arabia's public sector, cloud computing adoption faces several interrelated challenges that limit the widespread and consistent implementation of national cloud strategies. These barriers are technical but also institutional, regulatory, and cultural. This section outlines six primary challenges identified through policy reviews and empirical studies.

**Data Sovereignty and Loss of Governance**

Data sovereignty is one of the most cited concerns in Saudi government cloud adoption. Agencies are restricted in where and how they store sensitive data, especially those categorized under high-security classifications. As mandated by policy, "data classified in level 1 (top secure) or level 2 (secure) must be hosted in the Government cloud (NIC)" (KSA Cloud First Policy, 2020). This requirement supports national security but restricts broader cloud ecosystems' flexibility and scalability. Inter-agency coordination and clarity in governance responsibilities also remain inconsistent. For example, one report notes that "government agencies are required to coordinate with multiple stakeholders to ensure proper data governance, but the fragmentation between cloud providers and institutional policies creates risk" (Yesser, 2023).

**Security and Privacy Concerns**

Government agencies are particularly cautious about data security due to the sensitivity of the information they manage. Concerns about unauthorized access, breaches, and insufficient control over external environments persist. A foundational study found that "privacy issues," "security issues," and "loss of governance" were the most significant concerns expressed by public sector employees regarding cloud computing (Majid Al-Ruithe, 2018). These worries are exacerbated by limited awareness of existing cybersecurity frameworks. Another review confirmed that "security and privacy challenges continue to discourage organizations from moving sensitive workloads to public cloud environments" (Amin, 2021).

**Organizational Readiness and Skills Gap**

While policy frameworks exist, many government agencies lack the skilled personnel to execute cloud migration plans. A national review in the

education sector found that a "lack of awareness and lack of technical knowledge" delayed or derailed cloud initiatives (Fatani, 2021). Similarly, a gap in practical skills has been identified as a key barrier in government settings. One study concluded that "the shortage of experienced IT personnel is a major concern for government institutions planning to migrate to cloud platforms" (Khanfar, 2020).

**Resistance to Change and Digital Culture**

Adopting cloud solutions often requires structural changes in workflows and governance. These shifts can meet internal resistance, particularly in risk-averse and hierarchical organizational cultures. According to one research paper, "resistance to organizational change remains a challenge in digital transformation, especially where roles, control, and data access are restructured by cloud platforms" (Alshehri, 2021). Effective change management and leadership engagement are essential to mitigate this challenge.

**Procurement Limitations and Vendor Lock-In**

The cloud services procurement process often conflicts with the traditional procurement models used in the public sector. These legacy systems were designed for hardware and long-term software contracts, not for the pay-as-you-go, service-based model typical of cloud computing. One study revealed that "vendor lock-in" remains a pressing concern, particularly when agencies lack exit strategies or contract flexibility (Majid Al-Ruithe, 2018). Another report explained that "the rigidity of current procurement models in the public sector reduces the ability to engage flexibly with cloud service providers or to diversify across vendors" (Mansour, 2020).

**Technical Infrastructure and Connectivity Barriers**

Despite national investments in ICT, disparities in infrastructure remain across Saudi government agencies. Some entities lack access to the high-performance connectivity required for secure, uninterrupted cloud services. This can deter or delay migration efforts. A recent analysis observed that "the growing complexity of cloud infrastructure necessitates more advanced connectivity solutions, particularly for mission-critical applications" (Alotaibi, 2022). Without such infrastructure, cloud transformation will continue to face operational bottlenecks.

**Comparative Insights from Global Practices**

Governments worldwide have developed various strategies to overcome the challenges of cloud computing adoption. The approaches taken by the United Kingdom, the United Arab Emirates (UAE), and Singapore are

particularly noteworthy. Their models offer valuable insights that Saudi Arabia can adapt to strengthen its cloud transformation journey.

**United Kingdom: G-Cloud and Centralized Procurement**

The United Kingdom has implemented a highly structured and centralized approach to cloud adoption through its G-Cloud framework. This digital marketplace enables public agencies to procure cloud services from pre-approved vendors quickly and efficiently. The framework also reduces the administrative burden of procurement while ensuring compliance with national cybersecurity and data protection standards. As observed in one comparative study, "countries like the UK and Singapore established national cloud platforms that served to standardize procurement, enhance cybersecurity, and centralize compliance" (El-Haddadeh, 2020).

**United Arab Emirates: Executive-Driven Transformation and Data Localization**

The UAE's government has promoted cloud computing through strong top-down leadership and public-private partnerships with major global cloud providers. Executive sponsorship has played a pivotal role in accelerating cloud adoption, supported by national cloud zones that align with local data residency and security requirements. These zones have helped address concerns about data sovereignty while providing scalable and compliant cloud infrastructure. This approach illustrates the effectiveness of aligning political will with technological deployment.

**Singapore: Trust Frameworks and Technical Enablement**

Singapore has advanced cloud adoption through a balanced model that combines governance, technology, and workforce development. Its Government on Commercial Cloud (GCC) program provides agencies with secure cloud access supported by centralized compliance controls, pre-certified service providers, and technical templates. One analyst noted that "the integration of centralized compliance frameworks and technical enablement tools increases institutional trust in cloud platforms and encourages adoption" (Mujtaba, 2021).

**Relevance to the Saudi Context**

The experiences of the UK, UAE, and Singapore provide Saudi Arabia with actionable models for institutional alignment and technical acceleration. Standardizing procurement, investing in executive-level advocacy, and establishing technical toolkits for government agencies are all proven enablers of cloud success. These international examples suggest that

centralized governance, regulatory clarity, and digital skill-building are essential to translating policy intent into operational impact.

**Strategic Recommendations**

To advance cloud adoption in Saudi Arabia's public sector, a set of integrated strategic measures is required. These recommendations are derived from the challenges explored earlier and shaped by global practices that have yielded positive outcomes. Each recommendation reinforces alignment between national policy and organizational action while promoting trust, capability, and performance across institutions.

**Establish Cloud Governance Units in Each Government Entity**

While national frameworks exist, institutional-level governance is inconsistent. Government entities should create dedicated cloud governance teams to oversee adoption strategies, ensure regulatory compliance, and align with national digital priorities. One guideline emphasizes that "agencies must evaluate cloud readiness across technical, security, and data classification dimensions before initiating migration" (DGA, 2023). These internal structures are essential for translating strategic intent into operational results.

**Build a National Public Sector Cloud Skills Program**

A structured training program should be introduced to address skill gaps to enhance cloud literacy, cybersecurity awareness, and vendor management capabilities across ministries. This initiative could include tiered certification, on-the-job learning, and career advancement incentives. A national study confirms that "the shortage of experienced IT personnel is a major concern for government institutions planning to migrate to cloud platforms" (Khanfar, 2020).

**Modernize Public Sector Procurement for Cloud Services**

Procurement reform is needed to enable flexible engagement with cloud service providers. This includes implementing pre-approved vendor lists, standardized contract templates, and consumption-based billing options. As highlighted in comparative research, "standardized procurement frameworks can enhance cybersecurity and reduce institutional delays" (El-Haddadeh, 2020). These models can significantly reduce onboarding time and support multi-vendor ecosystems.

**Introducing a Cloud Acceleration Fund for Priority Agencies**

Targeted financial support should be directed toward under-resourced government entities that demonstrate high cloud impact potential. A cloud acceleration fund can finance pilots, shared services, and fast-track cloud

transformation in ministries with cross-cutting public service functions. This can stimulate sector-wide adoption and generate proven templates for replication.

**Implement National Change Management Frameworks**

Adoption success depends on stakeholder buy-in and cultural alignment. Ministries should be supported with national toolkits that guide leadership alignment, staff engagement, and workflow redesign. As one study affirms, "resistance to organizational change remains a challenge in digital transformation, especially where roles, control, and data access are restructured by cloud platforms" (Alshehri, 2021). A national change management framework will help mitigate these internal barriers and normalize adoption practices across the public sector.

## Conclusion

Cloud computing has become a vital enabler of digital transformation in the Saudi public sector. The government has taken commendable steps through the Cloud First Policy and regulatory frameworks, but implementation remains inconsistent across ministries. This paper identified key adoption challenges, including data residency requirements, cybersecurity concerns, procurement inflexibility, and skills shortages.

The study analyzed local barriers and examined global benchmarks from the United Kingdom, United Arab Emirates, and Singapore. It emphasized the need for a whole-of-government approach. Saudi Arabia can benefit from international practices prioritizing centralized procurement, capacity building, and institutional alignment.

The recommendations proposed in this paper range from governance structures and procurement reforms to skills development and change management, offering a path forward. As highlighted in the literature, "resistance to organizational change remains a challenge in digital transformation" (Alshehri, 2021), underscoring the importance of leadership, communication, and workforce readiness.

With continued investment in policy execution and organizational capability, Saudi Arabia is well-positioned to lead in developing secure, scalable, and citizen-centric government cloud services.

**Conflict of Interest:** The author reported no conflict of interest.

**Data Availability:** All data are included in the content of the paper.

**Funding Statement:** The author did not obtain any funding for this research.

**References:**


1. Alkhater, W. (2022). Benefits and challenges of the adoption of cloud computing in telecommunications companies in Saudi Arabia. Journal of Computer and Communications, 10(1), 10–23.
2. Alotaibi, F. (2022). Connectivity and cloud infrastructure constraints in Saudi Arabia. Journal of Digital Infrastructure, 6(2), 112–124.
3. Alsabaan, R. (2023). Cloud computing and its role in accelerating digital transformation and its sustainable impact in the government sector. Riyadh: SDAIA Publications.
4. Alshehri, A. (2021). Key issues in public sector cloud transformation projects: A qualitative review. Saudi Journal of Information Systems, 5(1), 44–55.
5. Amin, N. (2021). Information security and privacy challenges of cloud computing for government adoption: A systematic review. Journal of Cybersecurity Policy, 8(3), 31–42.
6. CITC. (2023). Cloud computing and regulatory overview – CITC report (KSA). Communications, Space & Technology Commission.
7. DGA. (2023). Guideline for cloud computing adoption by government agencies – V1.0. Digital Government Authority. https://www.dga.gov.sa
8. El-Haddadeh, R. (2020). Digital innovation dynamics influence on organizational adoption: The case of cloud computing services. Information Systems Frontiers, 22(4), 985–999.
9. Fatani, N. (2021). Factors affecting the adoption of cloud computing in Saudi Arabian universities. International Journal of Advanced Computer Science and Applications, 12(3), 112–119.
10. Khan, W. U. (2025). Saudi Arabia's cloud broadband landscape: Opportunities and challenges in the era of Vision 2030. Journal of Business and Management Studies, 7(1), 259–262. https://doi.org/10.32996/jbms.2025.7.1.20
11. Khanfar, K. (2020). Factors influencing cloud computing adoption in Saudi Arabia: A governmental perspective. Arabian Journal of e-Government, 4(2), 88–97.
12. KSA Cloud First Policy. (2020). Cloud First Policy. Ministry of Communications and Information Technology, Saudi Arabia.
13. Majid Al-Ruithe. (2018). Key issues for embracing the cloud computing to adopt a digital transformation: A study of Saudi public sector. Procedia Computer Science, 130, 1037–1043. https://doi.org/10.1016/j.procs.2018.04.145
14. Mansour, M. (2020). Barriers to IT procurement reform in the Saudi public sector. Public Administration and ICT Policy Journal, 9(4), 215–229.

15. Mujtaba, R. (2021). An overview on the global governmental efforts on fostering the use of cloud computing. Journal of Emerging Technology and Public Management, 3(1), 77–85.
16. SDAIA. (2024). Guideline for National Overall Reference Architecture (NORA) – V1.0. Saudi Data and Artificial Intelligence Authority.
17. Yesser. (2023). Guideline for cloud architecture governance in public sector projects (Arabic). e-Government Program (Yesser), Saudi Arabia.