Access Partnership

Software Growth in the Kingdom of Saudi Arabia

Market Opportunities, Entry Pathways, and Compliance Considerations for Independent Software Vendors



accesspartnership.com

Our firm

We make innovation work for the world

We work with businesses, governments, and multilateral institutions to unlock new markets, drive commercial success, and create solutions that advance humanity.

Our multidisciplinary team includes geopolitical analysts, regulatory specialists, and communications strategists, as well as economists, engineers, physicians, and scientists.

We combine on-the-ground expertise across every region with deep specialism, letting us go beyond conventional consulting to design and execute bold, end-to-end strategies that help you scale sustainably and deliver meaningful impact for society.

We help ambitious organisations turn ideas into real-world outcomes quickly and decisively. Whether you're expanding into new markets, launching new solutions, or tackling global challenges, we combine commercial insight, public-policy and regulatory analysis, and deep networks to help you move with confidence and clarity.

Find out more here: accesspartnership.com

Commissioned by aws

Copyright © 2026. The information contained herein is the property of AA Access Partnership Limited and is provided on condition that it will not be reproduced, copied, lent, or disclosed, directly or indirectly, nor used for any purpose other than that for which it was specifically furnished.

AA Access Partnership Pte Ltd

Disclaimer:
This document is provided for informational purposes only and does not constitute legal, regulatory, or compliance advice. The information contained herein is current as of October 2026 and is subject to change. Organizations should consult with qualified legal counsel regarding their specific compliance obligations in Saudi Arabia. AWS makes no representations or warranties regarding the accuracy or completeness of regulatory interpretations presented in this document.

Contents

Executive Summary 01

01. Understanding the Business Environment 03

1.1 General Business Environment

1.2 Regulatory Requirements Applicable to Software Providers

02. Saudi Arabia: The Next Growth Frontier for Software 08

2.1 Trends in the Software Industry

2.2 Current Market Value and Potential

03. Overview of Saudi Arabia's Digital Transformation Journey 11

3.1 Key trends driving growth in Saudi Arabia's digital sector

3.2 Overview of software industry landscape: Stakeholders, sub-sectors, key customer segments

04. Endnotes 15

Executive Summary

Saudi Arabia is moving from oil-led prosperity to a data-driven economy. Backed by Vision 2030, the Kingdom is deploying world-class cloud regions, national 5G coverage, AI "giga-projects," and record-level public-sector IT spending. For international independent software vendors (ISVs), the message is clear: now is the moment to embed, localize, and scale in one of the fastest-growing software markets worldwide, while also planning early for market access requirements such as the Kingdom's Regional Headquarters (RHQ) rules for government and state-linked contracting. This Guide provides general market and public information to help international independent software vendors (ISVs) evaluate and plan for entry and growth in Saudi Arabia. Specifically, it offers:

1. **Regulatory guidance on market entry**
2. **An overview of key stakeholders and frameworks**
3. **Market context and growth opportunities**



Market context and growth opportunities

- **Size & trajectory.** Saudi Arabia's software market was estimated at USD 4.3 billion in 2024[1] and is projected to more than double to USD 9.3 billion by 2030, based on Access Partnership estimates using regional software growth forecasts as a proxy.
- **Demand engines.** Four mutually reinforcing trends are driving uptake:

1. **Government-first digitization:** 98% of government services are now available online, and Saudi Arabia's Cloud First Policy has been in place since 2019.
2. **Cloud capacity boom:** Multiple hyperscale and regional cloud providers operate in-country data centers. AWS announced that its first Saudi Arabia Cloud Infrastructure Region is on track to launch in December 2026, while its expanded collaboration with HUMAIN is expected to make up to 50 MW available in Saudi Arabia's first AI Zone by 2028.
3. **AI, IoT & 5G adoption:** Saudi giga-projects are creating demand for sector-specific software in areas such as mobility, sustainability, energy management, and environmental monitoring. NEOM's Technology & Digital strategy identifies 5G+ connectivity, digital twins, AI, and advanced robotics as focus areas, while Red Sea Global has described its use of environmental sensors and data-led monitoring to support regenerative tourism and conservation.
4. **SME digital leapfrogging:** According to the Saudi Ministry of Commerce, the Kingdom had 1.7 million active commercial records, with registrations continuing to rise. This expanding SME base commonly starts with SaaS tools, while tech SMEs accounted for 34% of an estimated SAR 32 billion (USD 8.5 billion) in total government demand for digital solutions in 2023 – approximately SAR 10.9 billion (USD 2.9 billion) in SME-supplied demand.

Overview of key stakeholders

- **Regulators & enablers.** Government entities include, but are not limited to: Ministry of Information and Communications Technologies (MCIT); Saudi Data & AI Authority (SDAIA); the Communications, Space and Technology Commission (CST); National Cybersecurity Authority (NCA); Saudi Central Bank (SAMA); Ministry of Finance (MOF) & Digital Government Authority (DGA).
- **Cloud & infrastructure anchors** in the Kingdom include multiple global hyperscalers and regional cloud providers, supported by expanding in-country data center and cloud-region capacity.
- **Local digital champions** include but are not limited to: STC Group (USD 20 billion revenue in 2024), HUMAIN (PIF-backed AI firm building up to 500 MW AI data center capacity), Aramco Digital (planning USD 0.5 billion in digital investments over three years; major tech partnerships), and SITE (PIF-owned cybersecurity & digital integrator with IPO preparations underway for 2026).
- **High-value customer clusters** include government ministries, banks & fintechs, hospitals, education providers, retail & e-commerce, SMEs, and the fast-rising e-sports sector.

Why early compliance matters

In Saudi Arabia, aligning early with its modern regulatory stack, including the Personal Data Protection Law (PDPL), the Cloud Computing Services Provisioning Regulations (CCSPR), and the NCA/SAMA cyber controls, helps ISVs reduce risk, build credibility, and avoid operational delays. Although the laws do not explicitly reward early adopters, regulatory expectations make compliance a prerequisite for government contracts and tenders. This report highlights the principal entity incorporation, licensing, data, cloud, cybersecurity, Saudization, tax, and reporting considerations that ISVs should assess with qualified Saudi counsel and relevant regulators before market entry.

Key takeaways for ISVs

Key opportunities

- Access to one of the region's fastest-growing software markets
- Planned AWS Saudi Region, with launch targeted for December 2026
- A pipeline of smart city, fintech, and healthcare projects

Key considerations

- Choosing the right legal vehicle
- Aligning with relevant local laws and controls
- Leveraging Saudi cloud regions
- Mapping sector-specific procurement rules
- Investing in Saudization quotas

Bottom line: Saudi Arabia combines sizeable spend, decisive policy backing, and cloud capacity. ISVs leveraging cloud infrastructure that meets local regulatory requirements may be better positioned to serve the growing Saudi demand. AWS provides tools and resources to help ISVs navigate compliance and localization requirements.

01

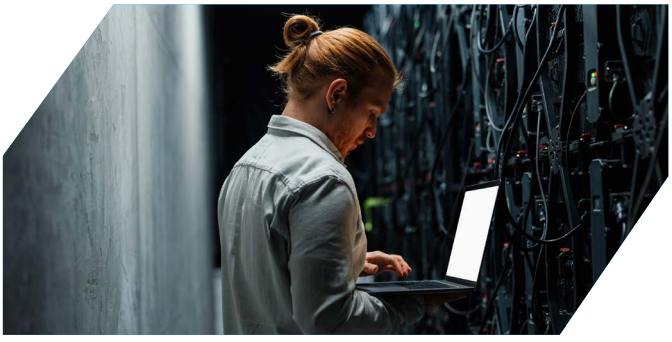
Understanding the Business Environment

1.1 General Business Environment

Saudi Arabia has simplified foreign investment through regulatory reforms, allowing up to 100% foreign ownership, while streamlining the investment license process under the Ministry of Investment (MISA).[2] Approved licenses are coupled with a relatively swift company registration process via the Ministry of Commerce (MOC)'s Commercial Registration (CR) system, enabling the reservation of trade names and corporate setup within weeks.

For companies targeting government or state-linked contracts, Saudi Arabia's Regional Headquarters (RHQ) rules remain a key market-access consideration: non-RHQ multinationals are generally restricted from such contracts, although newly formalized exemption pathways allow government entities to contract with non-RHQ suppliers in defined cases, including technical uniqueness, specialized expertise, significant price advantage, or small contracts below SAR 1 million (approximately USD 267,000).[3]

Registered entities must also undertake routine compliance measures such as VAT registration via Zakat, Tax and Customs Authority (ZATCA), labor and social insurance via the General Organization for Social Insurance (GOSI), Saudization quotas, corporate banking setup, and annual financial audits. Commercial Register (CR) holders must confirm their registered information electronically each year; annual CR renewal and expiry dates have been abolished. Separate business licence, audit and Saudization obligations may still apply.



1.2 Regulatory Requirements Applicable to Software Providers[4]

1. **Data Protection (PDPL) – controller vs processor duties**

Saudi Arabia's Personal Data Protection Law (PDPL), fully enforceable from September 2024, distinguishes between the roles involved in SaaS delivery to ensure clear accountability across the processing chain:[5]

- The customer is typically the **data controller** because it determines the purpose and means of processing (what data is collected, for what business purposes, and how long it is retained).
- The ISV operating the SaaS application acts as the **data processor**, because it processes personal data for the benefit and on behalf of the controller and does not independently determine the purposes of processing.
- Where an ISV relies on an infrastructure provider to host or manage the environment, the cloud provider functions as a **sub-processor** engaged by the ISV to support delivery of the service.

This distinction matters because PDPL assigns different legal responsibilities depending on who decides why or how data is processed. Controllers are ultimately accountable and must ensure the processors they appoint comply with PDPL requirements, including appropriate safeguards and oversight through contracts and governance. Processors must process only within the controller's instructions and support the controllers' compliance, such as security measures and operational support, while flowing relevant obligations down to any sub-processors through contractual controls. In practice, this role clarity enables traceable responsibility, enforceable contractual allocation, and consistent protection of personal data end-to-end in a SaaS supply chain.

As the PDPL implementing framework continues to evolve, SDAIA periodically updates its guidance, regulations, and compliance requirements.

Organizations should refer to SDAIA's official PDPL portal for the most current and authoritative information on controller/processor obligations, cross-border transfer requirements, and related compliance measures.[6]

Practical tip: *ISVs should (i) agree a PDPL-compliant data processing agreement with the customer and use SDAIA's Standard Contractual Clauses where required for cross-border transfers; (ii) set a contractual internal breach-escalation target (e.g., within 24 hours) to help the customer meet any applicable statutory notification deadline; and (iii) verify the chosen cloud deployment against applicable CST, NCA, and PDPL requirements.*

2. Cloud Computing Services Provisioning Regulation (CCSPR)

Under CST, the Cloud Computing Services Provisioning Regulations (CCSPR) govern how cloud services are provided in Saudi Arabia and apply to both Cloud Service Providers (CSPs) and to customer/tenants that use those services, such as ISVs.[7] Key elements include CSP registration with CST, service classification (Qualification A/B/C), and data localization rules (e.g., public sector/government data may not be transferred outside Saudi Arabia unless permitted by law).

CCSPR is directly relevant to ISVs in two common scenarios:

- Where an ISV operates its SaaS platform on a CST-registered cloud (the ISV is a tenant)
- Where an ISV sells to Saudi customers whose workloads are subject to CCSPR-driven hosting or classification requirements, its architecture, deployment options, and contracts must support the customer's compliance.

While CSPs must provide infrastructure capable of meeting localization and security requirements, the responsibility for ensuring that deployed workloads and the data they contain comply with localization restrictions lies with the customer. ISVs therefore need to design and operate their SaaS deployments in a way that enables customers to meet these requirements through region selection, data residency controls, and contractual flow-downs.

2.1 Guide for Cloud Computing Service Providers

ISVs acting solely as customers/tenants of cloud providers generally do not require CSP registration; ISVs providing regulated cloud services themselves should assess whether CST registration applies to their delivery model. The CST Guide for Cloud Computing Service Providers clarifies the CSP registration and baseline requirements, including the information CSPs must file, which ISVs can use to vet hosting partners and evidence compliance to Saudi customers.[8]

2.2 Registration Guide in the Qualifying Category for Provision of Cloud Computing Services

The CST Qualifying Category registration guide sets out a transitional path for entities that want to provide cloud services in Saudi Arabia through a Saudi data center but do not yet meet the full CST A/B/C registration requirements. Registration under the qualifying track is time-limited (one year from approval) and comes with constraints on what services/segments the provider can support while it works toward full classification.[9]

In practice, the guide is a useful screening tool for ISVs and Saudi customers to assess a hosting provider's regulatory status and suitability for specific workload types. It is particularly relevant in two cases:

- where an ISV self-hosts and effectively provides cloud services (for instance, if it operates infrastructure for multiple customers), which may trigger CSP-like compliance considerations.
- where an ISV is selecting a hosting partner and needs to confirm whether the provider is fully registered (A/B/C) or only operating under the qualifying pathway.

3. Cybersecurity (ECC & CCC)

Cybersecurity framework	Who it covers	What an ISV must do
NCA Essential Cybersecurity Controls (ECC 2-2024)[10]	• Government entities. • Any private organization that owns, operates, or hosts Critical National Infrastructure (CNI).	• If your SaaS is hosted **for a ministry/CNI operator,** map your platform to the ECC baseline. • Provide the customer with evidence for annual ECC attestation or audit.
NCA Cloud Cybersecurity Controls (CCC 2-2024)[11]	• **CSPs** running the underlying IaaS/PaaS/SaaS stack. • **Cloud Service Tenants** – any customer (including an ISV) deploying workloads on that cloud.	• **Scenario A – ISV provides cloud services itself** → Assess whether CST cloud service registration is required, implement the NCA CCC controls applicable to the provider's role and in-scope customers, and meet any applicable assessment or audit requirements. • **Scenario B – ISV uses a CST-registered in-Kingdom cloud provider** → Verify the provider's CST registration and applicable NCA cloud-control status, then flow relevant CCC obligations into customer contracts.

In February 2026, the National Cybersecurity Authority (NCA) launched a public consultation on a **draft Regulatory Framework for Licensing Cybersecurity Services, Products, and Solutions;**[12] the consultation closed on 26 March 2026. As of October 2026, the NCA's public materials reviewed for this update did not identify a final published version of that broader framework, so ISVs should continue to monitor the NCA and the Haseen licensing service before offering cybersecurity services, products, or solutions in the Kingdom. Separately, the NCA's Non-CNI Private Sector Entities Cybersecurity Controls (NCNICC-1:2025) establish minimum cybersecurity controls for in-scope private sector entities that do not operate critical national infrastructure. ISVs should therefore assess whether NCNICC, as well as sector-specific and contractual controls, applies to the customer or deployment.

Sector-Specific Procurement Compliance Requirements

Navigating Saudi Arabia's regulatory landscape requires more than just meeting general business requirements. Sector-specific compliance is the key that unlocks the Kingdom's most valuable contracts, especially in high-growth areas like healthcare, finance, and government. For ISVs, aligning with these specialized frameworks is not just a legal obligation, but a critical strategic move. It demonstrates a company's commitment to the highest standards of data security and governance, builds trust with potential customers, and establishes a reputation as a mature, reliable partner. Aligning with applicable sector-specific requirements can support procurement eligibility, customer due diligence, and readiness to respond to Saudi tenders, positioning ISVs for long-term growth as key enablers of Saudi Arabia's digital future.[13]

Sector	Key Regulatory & Procurement Requirements	Principal Authority
Healthcare	• **Health Insurance Transactions Interoperability (through National Platform for Health and Insurance Exchange Services – NPHIES):** ISVs connecting healthcare providers and payers to NPHIES must implement standardized APIs based on HL7's Fast Healthcare Interoperability Resources (FHIR) Release 4 specification, in addition to the NPHIES Implementation Guide, to support workflows such as eligibility, authorization, and claims exchange.[14] • **MOH e-Health & EMR compliance:** Where a healthcare software solution is subject to applicable MOH/Saudi Health Council interoperability, testing or certification requirements, the ISV should provide the technical specifications, testing evidence, and documentation required by the healthcare customer. Requirements depend on the system and procurement context.[15] • **Health Data Hosting Regulations:** Health/medical data storage should be hosted within Saudi Arabia's geographical boundaries. ISVs should use a CST-registered cloud service provider or suitable locally hosted/on-premises infrastructure.[16] Any cross-border transfer of personal data (including health data where it qualifies as sensitive data) should follow SDAIA'S PDPL cross-border transfer framework, including a required risk assessment.[17] • **Patient Data Protection & PDPL Alignment:** ISVs should support healthcare customers in meeting applicable consent, data minimization, and breach notification requirements, including the 72-hour notification deadline where the statutory conditions are met.[18]	MOH/Saudi Health Council (SHC/NHIC)/ SDAIA
Financial Services Industry	• **SAMA Outsourcing & Cloud Computing Framework:** For any critical outsourcing, the SAMA-regulated customer must obtain SAMA's prior approval and flow the Framework's audit, data location, exit, and subcontractor clauses into its contract; the ISV must therefore cooperate and provide the evidence needed for the customer's compliance.[19] • **SAMA Cybersecurity Framework:** The SAMA Cybersecurity Framework establishes four cybersecurity control domains: Leadership & Governance; Risk Management & Compliance; Operations & Technology; and Third-Party Security. The framework applies to SAMA-regulated organizations. When an ISV provides core-banking SaaS or hosts customer data, the SAMA-regulated customer must flow down the relevant Framework controls (e.g., secure SDLC, encryption, incident response, third-party oversight) through its contract.[20] • **Open Banking Licensing:** ISVs providing open banking infrastructure, API connectivity, consent management tools, data-sharing solutions, or fintech integration services may need to support SAMA-regulated customers or licensed fintechs in meeting SAMA's open banking requirements. This includes demonstrating secure API design, customer consent management, data protection controls, operational resilience, and third-party risk management.[21]	SAMA/MCIT
Government	• **MOF Government Tenders & Procurement Law:** Bidders (including foreign ISVs) must be aware of certain obligations in undertaking the bidding process, including: (i) registration of supplier profile on Etimad portal and payment of an annual fee, (ii) submission of separate technical and financial offers, and (iii) submission of bid bonds in certain cases.[22] • **CST CCSPR:** No cross-border transfers of government data unless allowed by law; use a CSP class appropriate to data classification (Class C for high-classified).[23] • **NCA Essential & Cloud Cybersecurity Controls:** Demonstrate compliance with the applicable NCA Essential/Cloud Cybersecurity Controls and any audit, attestation, or evidence requirements specified by the government customer or tender.[24] • **DGA Guideline for Cloud Computing Adoption by Government Agencies:** The guideline outlines the cloud adoption process for government agencies and provides guidance on data classification, security, and migration.[25]	MOF/CST/NCA/ DGA

Sector	Key Regulatory & Procurement Requirements	Principal Authority
Education	• **Children & Incompetents' Data-Protection Policy:** Any platform that collects or stores data on children must obtain guardian consent, collect only the "minimum data necessary," notify affected individuals and the National Data Management Office (NDMO) in the case of a breach, and delete the data upon the child's request. Direct marketing to minors by data controllers is prohibited. ISVs must build these safeguards into their LMS or analytics stack so schools can provide evidence of compliance during MOE procurements.[26] • **Learning Management System (LMS) Integration Standards:** ISVs integrating their solutions with the national Madrasati platform should comply with applicable API and integration requirements.[27] • **E-Content Classification:** ISVs should assess applicable Gmedia age-classification requirements for digital materials.[28]	SDAIA/MOE/Gmedia
Retail & E-Commerce	• **E-Commerce Law (2019):** Any service provider that sells goods or SaaS to Saudi consumers (including an overseas ISV) must protect personal data and electronic communications and may not keep them longer than the transaction period unless the user gives explicit consent. Breaches can incur administrative fines (up to SAR 1 million/USD 267,000).[29] • **ZATCA E-Invoicing (Fatoorah) Regulation:** Taxpayers in the Integration Phase must integrate their e-invoicing solutions with the Fatoora Platform, issue e-invoices in the prescribed format, and include the required additional fields. ZATCA states that taxpayers may use any solution provider whose solution complies with the requirements; inclusion in ZATCA's indicative provider list is not mandatory. By July 2026, ZATCA had announced Wave 25, covering taxpayers whose VAT-subject revenues exceeded SAR 187,500 in 2022, 2023, 2024, or 2025, with integration required by 1 February 2027. Applicability and deadlines should be checked against the latest ZATCA wave notice.[30] • **Anti-Fraud & Secure Payments:** Payment gateway ISVs should assess applicable SAMA mada requirements and Payment Card Industry Data Security Standard (PCI DSS) obligations.[31] • **Customs & Consumer Protection Guidelines:** ISVs offering cross-border digital goods or SaaS subscriptions should assess applicable customs and consumer protection requirements.[32]	MOC/ZATCA/SAMA
E-Sports & Gaming	• **Gmedia Licensing for Digital Games & E-Sports Platforms:** Applicable Gmedia licensing requirements may include content classification and age-rating for digital games and e-sports platforms.[33] • **Local Hosting for Multiplayer Servers:** Tiered data sovereignty requirements under CST's CCSPR according to data sensitivity categorization, with a preference for local hosting to reduce latency and improve user experience.[34] • **Data & Parental Controls:** Minors' online safety provisions such as SDAIA's Children and Incompetents' Data Protection Policy and Gmedia's Age Classification Guidelines.[35]	Gmedia/SAFEIS/ CST/ SDAIA

02

Saudi Arabia: The Next Growth Frontier for Software

2.1 Trends in the Software Industry

Saudi Arabia's software and SaaS industry is undergoing rapid transformation, driven by visionary government leadership, increasing digital adoption among businesses, and major investments by global technology players. The latest baseline used in this report recorded 58 data centers, 21 service providers, and 28 cloud computing service providers in 2024.[36] For more current market context, CST reported that the Saudi technology market reached SAR 115 billion in 2025 and launched a Cloud Computing Market Maturity Index in September 2026. There are three major trends currently shaping the industry:

1. Government leadership to drive digital transformation

At the center of this transformation is Vision 2030, the Kingdom's strategic blueprint for economic diversification and digital modernization. Vision 2030 has positioned digital transformation as a core instrument of economic diversification, embedding software demand directly into national development priorities. Flagship "giga-projects" such as Diriyah, Qiddiya, and the Red Sea Project are being developed as digitally native environments, requiring advanced software solutions across urban planning, mobility, logistics, energy management, healthcare delivery, and citizen services. Unlike conventional infrastructure projects, these initiatives generate sustained, multi-year demand for complex, interoperable software systems, creating opportunities for vertical and enterprise-grade SaaS providers.

This role of the state is reinforced by direct public sector investment in digital infrastructure and services. Public ICT contract values reached SAR 38 billion (USD 10.13 billion) in 2024 – an 18.75% increase over the previous year.[37]

Saudi Arabia's strong performance in digital government delivery, as evidenced by its global ranking (6th globally in the 2024 United Nations E-Government Development Index[38]) and the near-universal digitalization of public services (more than



5,300 or 98% of government services are provided digitally[39]) further signal a mature public sector customer capable of procuring, deploying, and scaling software solutions. Its investments in state-owned technology firms like HUMAIN create further potential for the Saudi government to continue leading in digital transformation.

2. Rapid enterprise digital adoption and strong return on investment

Enterprise demand for software in Saudi Arabia is both broad-based and commercially grounded. Across sectors, including healthcare, logistics, retail, and financial services, firms are increasingly adopting software as core operational systems. This shift reflects a transition from pilot-led digitalization to enterprise-wide deployment, supported by clear evidence of return on investment. Survey data from 2024 indicates that Saudi enterprises report that 80% of digital leaders in Saudi Arabia are actively driving innovation through digital transformation (well above the global average of 65%) and more than 80% reported profitability gains from increased use of software solutions.[40]

This combination of proven ROI and senior leadership buy-in reduces uncertainty around value realization to SaaS adoption in the Kingdom.

3. Strong digital foundations lower execution risks for software providers

The Kingdom has invested heavily in cloud infrastructure, data centers, and digital payments systems, creating an environment in which software solutions can be deployed at scale with relatively limited localization or infrastructure constraints. Rapid growth in electronic payments and transaction volumes[41] illustrates the depth of digital integration across the economy, enabling downstream software use cases in areas such as fintech, retail technology, data analytics, and customer engagement platforms. For software firms, this translates into shorter deployment cycles and a clearer pathway from adoption to scale.

Taken together, these structural characteristics differentiate Saudi Arabia from other fast-growing digital markets - the Kingdom combines state-anchored demand, enterprise readiness, and robust digital infrastructure.

As a result, global technology companies are deepening their presence in the Kingdom, further strengthening the foundation for the growth of the software and SaaS market. During LEAP 2025, the Kingdom announced USD 14.9 billion in private sector investments, including a USD 5 billion investment by DataVolt, in collaboration with NEOM, to establish a net-zero AI cloud center; a USD 1.4 billion investment by AIFanar to develop four data centers; and a USD 75 million investment by Zoom to serve clients in the MENA region.[42] In August 2026, AWS confirmed that its first Saudi Arabia Cloud Infrastructure Region, representing more than USD 5.3 billion in planned investment, is on track to launch in December 2026. AWS and HUMAIN also announced an expanded collaboration expected to provide up to 50 MW of AI Zone capacity by 2028.[43]

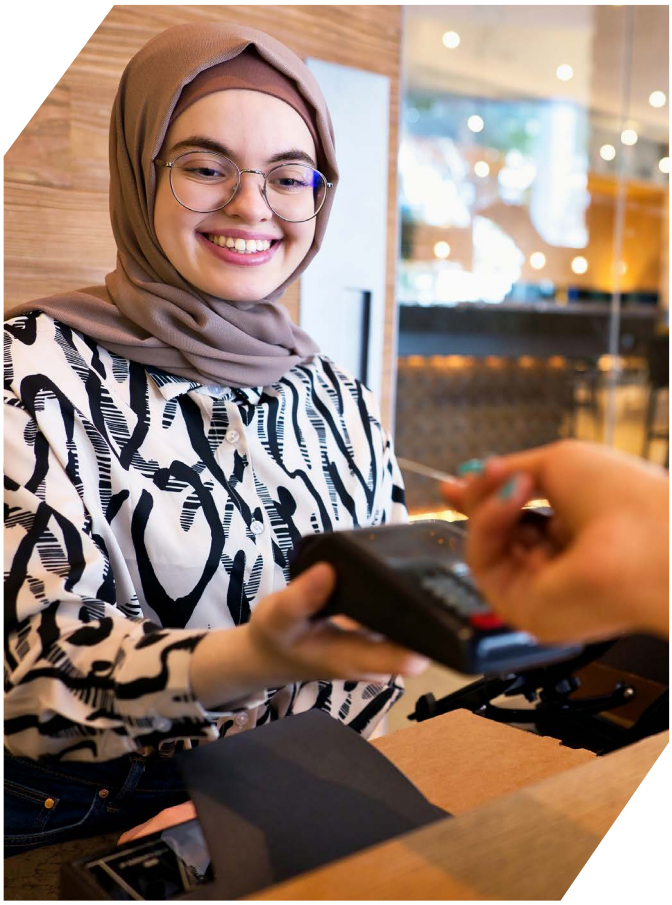
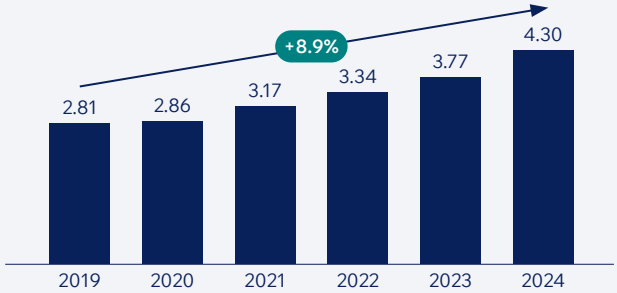


Figure 1

Market value of Saudi Arabia's software industry, 2019-2024

Total expenditure on software, USD billion



Source: Access Partnership analysis based on data from Gartner and the World Bank.

2.2 Current Market Value and Potential

Saudi Arabia's software market has outpaced the broader ICT sector, reaching an estimated USD 4.3 billion in 2024 (Figure 1).[44] Between 2019 and 2024, the Kingdom's software market recorded a CAGR of 8.9%, exceeding the ICT sector's 7.5% growth rate.[45] This ongoing expansion is creating a vibrant ecosystem that draws in new market participants and accelerates innovation across sectors.

In Access Partnership's indicative 2024 sector breakdown – estimated by applying the distribution of Saudi cloud expenditure as a proxy for software expenditure – the public sector represented 36.1% of software spending, followed by ICT services (17.1%) and education (9.5%).[46]

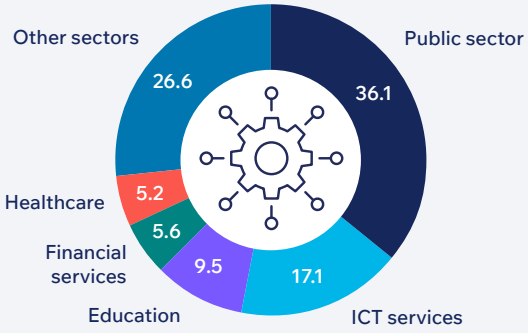
The impact of this growth is also increasingly visible through initiatives such as the annual LEAP technology conference in Riyadh, which has more than doubled the investments announced from 2022 to 2025.

Looking ahead, Saudi Arabia is expected to sustain this growth trajectory. Between 2025 and 2030, the Kingdom's software industry is estimated to grow by a CAGR of 13.9%, reaching USD 9.34 billion by 2030 (Figure 3).[47]

Figure 2

Breakdown of Saudi Arabia's software expenditure by sector, 2024

Share of total expenditure on software, %



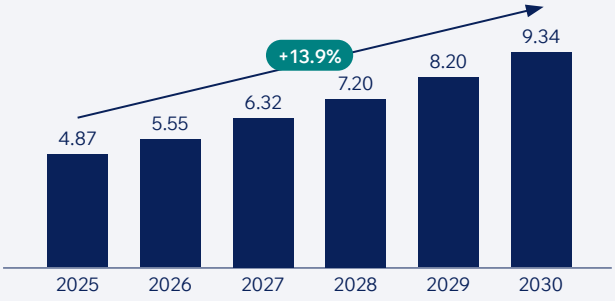
Notes: Other sectors include: Agriculture; Manufacturing; Utilities and Energy; Wholesale and Retail Trade; Restaurant and Hotels; Transport, Storage and Communication; Real Estate; Business Services; and Arts, Entertainment and Recreation.

Source: General Authority for Statistics, Access Partnership analysis.

Figure 3

Projected market value of Saudi Arabia's software industry, 2025-2030

Total expenditure on software, USD billion



Source: Access Partnership analysis, Gartner.

03

Overview of Saudi Arabia's Digital Transformation Journey

This Chapter first outlines the growth trends shaping demand, then maps the stakeholders, the software subsectors, and the customer segments you will encounter when deploying in Saudi Arabia.

3.1 Key trends driving growth in Saudi Arabia's digital sector

Saudi Arabia is undergoing a profound digital transformation, propelled by its Vision 2030 agenda and ambitious national programs. The 2020 Digital Economy Policy sets out the Kingdom's strategy to become one of the top 15 economies in the world by 2030. It outlines Saudi Arabia's approach to policymaking in the digital sector, with the aim of expanding digital infrastructure, developing national human capital, and driving technology adoption, use, and innovation to reach this target.[48] From 2023-2024, the technology and telecommunications sectors in the Kingdom recorded an average growth rate of 8.5%, with the former reaching a value of USD 26.9 billion and the latter exceeding USD 21 billion.[49] Saudi Arabia ranked first globally in the 2025 International Telecommunication Union (ITU) ICT Development Index.[50]

Between 2025 and 2030, Saudi Arabia's digital transformation market is projected to grow from approximately USD 55 billion to more than USD 90 billion, reflecting a compound annual growth rate (CAGR) of around 10.35% depending on the metric (digital services, cloud, and software), underscoring the scale of and momentum behind this shift.[51] Several interlinked trends are fueling growth, which, together, create a high-growth environment for software and SaaS providers:

1. Government-led digitization

Saudi Arabia's government has taken a central role in driving digital transformation across public services. Under Vision 2030, the National Transformation Program launched a comprehensive e-government initiative, with platforms including "Absher" and "Watani" being deployed to enhance citizen engagement and streamline bureaucracy.[52] 98% of



government services are provided electronically, with the total number of e-government services exceeding 5,300.[53] In line with this, the Cloud First Policy, introduced in 2019, mandates that all new or renewed government IT investments evaluate cloud-based solutions first, with the goal of improving service delivery, reducing costs through shared infrastructure, and strengthening cybersecurity by leveraging accredited cloud providers.[54] To support implementation, the National Transformation Program also established the Cloud Computing Special Economic Zone in 2023, enabling government agencies to transition legacy systems to secure, scalable cloud platforms, laying the foundation for public sector SaaS adoption at scale.[55]

2. Cloud infrastructure expansion

Saudi Arabia is rapidly building its cloud infrastructure to support both public and private sector digital ambitions. This bolstered infrastructure meets rising enterprise demand for cloud-native SaaS solutions and underlines the shift to cloud-first architectures across sectors.

3. Adoption of AI, IoT, and 5G

Saudi Arabia is making rapid strides in emerging technologies, embedding them deeply into key sectors. The government's AI strategy, supported by SDAIA and heavy investment in state-owned firms like HUMAIN, aims to anchor the Kingdom as a regional AI leader.[56] In the healthcare sector, IoT solutions reached USD 387 million in 2023, with projected growth driven by smart diagnostics, electronic medical records (EMRs), and remote monitoring platforms.[57] The expansion of 5G networks, supported by continued investment from STC and other operators, has transformed connectivity, enabling real-time analytics, edge computing, autonomous logistics, and smart-city solutions.[58] Together, these technologies amplify demand for high-performance, scalable SaaS platforms tailored to AI, IoT, and data-intensive workflows.

4. SME and private sector momentum

With 1.7 million active commercial records and rising registrations, Saudi Arabia's private sector is expanding rapidly, creating a larger addressable base for cloud-enabled tools and services.[59] Small and medium-sized enterprises (SMEs), which comprise over 99% of Saudi Arabia's private sector firms, are rapidly embracing digital tools. A 2024 report from the SME General Authority (Monsha'at) found that 65% of newly registered SMEs adopted at least one SaaS solution (often CRM, accounting, or HR) as their first technology choice, reflecting the affordability and agility of cloud services.[60] Monsha'at reports that technology SMEs accounted for 34% of government demand for digital solutions in 2023. Total demand amounted to approximately SAR 32 billion (USD 8.5 billion), implying a technology-SME share of approximately SAR 10.9 billion (USD 2.9 billion). This activity has been supported by SME development programmes, financing and policy reforms under Vision 2030.[61] Additionally, the Mastercard SME Confidence Index confirms sustained confidence in digital-first strategies, driving sustained demand for scalable SaaS tools.[62] Together, these dynamics translate into a robust pipeline for SaaS adoption led by entrepreneurial ventures seeking operational efficiency and rapid innovation cycles.

3.2 Overview of software industry landscape: Stakeholders, sub-sectors, key customer segments

Saudi Arabia's software industry has evolved into a dynamic, multi-layered ecosystem, bringing together global cloud leaders, strong local players, and a rapidly diversifying customer base across sectors. This section outlines the key stakeholders driving this growth, the main software sub-sectors shaping Saudi Arabia, and the priority customer segments creating sustained demand for advanced digital solutions.

1. Stakeholders

Saudi's technology ecosystem involves a mix of public and private players:

- **Public sector regulators and enablers**
  - **Regulators & Guardrails:** Key regulatory bodies, including MCIT, SDAIA, CST, NCA, and SAMA, are responsible for establishing the essential guardrails for digital platforms, cybersecurity, and data protection. For example, SAMA's cyber regulations impose specific requirements on financial institutions as data controllers, which software vendors must be aware of.
  - **Enablers & Strategic Initiatives:** Beyond regulation, several entities are actively driving Saudi Arabia's digital transformation through concrete programs and platforms. DGA is strengthening public sector digital delivery and performance measurement, while Monsha'at is scaling SME competitiveness through targeted growth and advisory programs. Sector leaders such as the Ministry of Health (MOH) are also executing flagship initiatives that expand digital service access, modernize infrastructure, and strengthen trust through improved security and service availability.

Examples include:

- **DGA's Digital Transformation Measurement (Qiyas)/Digital Transformation Index** to assess government entities' digital maturity and compliance with digital standards.[63]
- Monsha'at's **Tomoh** program supporting fast-growing SMEs.[64]
- MOH's **Sehhaty** national platform providing access to a wide range of digital health services.[65]

- **Local ICT champions:** Companies such as STC, Elm, Aramco Digital (NextEra JV) are building digital infrastructure and services nationwide.

2. Subsectors

Software solutions are segmented into the following subsectors, with illustrative representatives provided below.

Category	Subcategories	
Enterprise Software	• Enterprise Resource Planning (ERP) • Customer Relationship Management (CRM) • Supply Chain Management (SCM)	• Business Intelligence (BI) & Analytics • Human Capital Management (HCM) • Enterprise Asset Management (EAM)
Industry-Specific Solutions	• Smart City Platforms • Healthcare Information Systems • Financial Services Software	• Manufacturing Execution Systems • Education Management Systems • Retail Management Solutions
Infrastructure Software	• Operating Systems • Database Management Systems • Virtualization & Containerization	• Cloud Infrastructure Services • Network Management • IT Service Management (ITSM)
Security Software	• Endpoint Protection • Network Security • Identity & Access Management	• Data Security & Encryption • Threat Intelligence • Security Information and Event Management (SIEM)
Development Tools	• Integrated Development Environments (IDEs) • DevOps & CI/CD (Continuous Integration/Delivery) Tools • API (Application Programming Interface) Management	• Low-code/No-code Platforms • Testing & QA (Quality Assurance) Solutions • Version Control Systems
Emerging Technology	• Artificial Intelligence/Machine Learning Platforms • Internet of Things (IoT) Solutions • Augmented/Virtual Reality Software	• Blockchain Applications • Robotic Process Automation (RPA) • Edge Computing Software
Consumer & Productivity	• Office Productivity Suites • Collaboration & Communication Tools • Media & Entertainment Software	• Personal Finance Applications • Mobile Applications • Creative Design Software

3. Key Customer Segments

The segments below demonstrate substantial demand for both foundational and industry-specific digital tools, with further opportunity driven by regulatory compliance and digital modernization. While these are not unique to Saudi Arabia, they represent the highest-probability cloud demand clusters in the Kingdom given current transformation and investment priorities.



Government & Public Sector agencies implementing e government, urban mobility, and cybersecurity frameworks.

Financial services firms seeking regulatory-compliant digital channels and fintech infrastructure.

Healthcare & Life Sciences providers adopting telehealth platforms, electronic health records, and AI-driven diagnostics to improve patient outcomes and operational efficiency.

Education institutions moving to digital learning platforms.

Retail and E-Commerce businesses managing inventory and order management.

Utilities & Energy companies digitizing operations through AI, digital twins, and predictive maintenance to optimize assets, reduce downtime and emissions, and advance smart infrastructure.

Manufacturing companies embracing Industry 4.0 technologies, IoT, and automation to improve productivity and quality.

Transportation & Logistics providers leveraging smart mobility solutions, fleet tracking, and digital platforms to enable efficient supply chains.

Telecommunications operators expanding 5G networks, fiber connectivity, and cloud-based services to accelerate digital transformation.

Media & Entertainment entities driving growth through streaming platforms, immersive content, and data-driven digital advertising ecosystems.

Agriculture businesses implementing precision farming techniques, IoT sensors, and analytics to optimize crop yields and resource utilization.

Construction & Real Estate companies using Building Information Modelling, smart building systems, and digital project management tools to deliver sustainable developments.

Hospitality & Tourism operators enhancing guest experiences with AI-driven personalization, mobile apps, and smart service platforms.

04

Endnotes

1 Access Partnership analysis based on Gartner and World Bank data.

2 Pinsent Masons (2024). "Updated Saudi Arabia Investment Law." Available at: https://www.pinsentmasons.com/out-law/news/updated-saudi-arabia-investment-law-pivotal-moment

3 Saudi Gazette. (2026). "Saudi Arabia permits exemptions to enable government contracting with international companies lacking regional headquarters." Available at: https://saudigazette.com.sa/article/659065/saudi-arabia/saudi-arabia-permits-exemptions-to-enable-government-contracting-with-international-companies-lacking-regional-headquarters

4 The content in section 1.2 is provided for general information only and does not constitute legal advice. ISVs should obtain independent legal counsel before relying on or acting upon any regulatory guidance outlined in this report.

5 SDAIA (2023). "Personal Data Protection Law." Available at: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

6 SDAIA (Saudi Data & Artificial Intelligence Authority) (n.d.). "Personal Data Protection." Available at: https://sdaia.gov.sa/en/Research/Pages/DataProtection.aspx

7 CST (2023). Cloud Computing Services Provisioning Regulations (CCSPR). Available at: https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1550

8 Communications, Space & Technology Commission (CST) (2023). "Guide for Cloud Computing Service Providers." Available at: https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1552

9 Communications, Space & Technology Commission (CST) (2023). "Registration Guide in the Qualifying Category for Provision of Cloud Computing Services." Available at: https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1551

10 National Cybersecurity Authority (NCA) (2024). "Essential Cybersecurity Controls (ECC 2-2024)". Available at: https://nca.gov.sa/en/regulatory-documents/controls-list/ecc/

11 National Cybersecurity Authority (NCA) (2024). "Cloud Cybersecurity Controls (CCC 2-2024)". Available at: https://nca.gov.sa/en/regulatory-documents/controls-list/ccc/

12 National Cybersecurity Authority (NCA) (2026). "The National Cybersecurity Authority launches public consultation on 'Regulatory Framework for Licensing Cybersecurity Services, Products, and Solutions'." Available at: https://nca.gov.sa/en/news/2149/

13 Regulatory information reviewed October 2026.

14 National Platform for Health and Insurance Exchange Services (NPHIES) (n.d.). "Message Structure – Healthcare Financial Services Implementation Guide." Available at: https://portal.nphies.sa/ig/message-structure.html; NPHIES (n.d.). "Home – Healthcare Financial Services Implementation Guide (Edition 1 v1.0.0)." Available at: https://portal.nphies.sa/ig/index.html; HL7 International (n.d.). "FHIR Specification (v4.0.1: R4) – Permanent Home." Available at: https://hl7.org/fhir/R4/

15 Ministry of Health (2015). "Saudi Health Information Exchange Policies". Available at: https://www.moh.gov.sa/en/Ministry/ehealthstd/Documents/eHealth%20Standards%20Files/Policies/IS0303%20Saudi%20Health%20Information%20Exchange%20Policies%20v1.0.pdf; Saudi Health Council (2016). "Enabling Standards-Based eHealth Interoperability: IS0304 Saudi Health Information Exchange Testing and Certification Policies." Available at: https://nhic.gov.sa/standards/Policies/IS0304-Saudi-Health-Information-Exchange-Testing-and-Certification-Policies-v1.0.pdf

16 A cloud or data center operator that has registered under CCSPR and met NCA Cloud Cybersecurity Controls.

17 SDAIA (2023). "Personal Data Protection Law." Available at: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf; SDAIA (2024). "Regulation on Personal Data Transfer Outside the Kingdom." Available at: https://dgp.sdaia.gov.sa/wps/wcm/connect/e5bbede0-1119-4f70-b4ef-f043ce58d780/Regulation%2Bon%2BPersonal%2BData%2BTransfer%2BOutside%2Bthe%2BKingdom..pdf?CACHEID=ROOTWORKSPACE-e5bbede0-1119-4f70-b4ef-f043ce58d780-p6OMj1M&CONVERT_TO=url&MOD=AJPERES

18 Saudi Health Council (n.d.). "Privacy Policy." Available at: https://shc.gov.sa/en/Pages/PrivacyPolicy.aspx and SDAIA (2023). "Personal Data Protection Law." Available at: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

19 Saudi Central Bank (2017). "Cloud Computing Regulation" Available at: https://rulebook.sama.gov.sa/en/343-cloud-computing-0 and Saudi Central Bank (2019). "Rules on Outsourcing" Available at: https://www.sama.gov.sa/en-US/Laws/FinanceRules/Outsourcing%20Rules%20-%20Revised%20v2%20Final%20Draft-Dec-2019.pdf

20 Saudi Central Bank (2017). "Cyber Security Framework." Available at: https://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf; Saudi Central Bank (2017). "Cybersecurity Framework Rulebook." Available at: https://rulebook.sama.gov.sa/en/cyber-security-framework-2

21 Saudi Central Bank (SAMA) (2026). “SAMA Commences Licensing of Fintech Companies to Provide Open Banking Services.” Available at: https://www.sama.gov.sa/en-US/News/Pages/news-1135.aspx

22 Ministry of Finance (2019). “Government Tenders and Procurement Law.” Available at: https://www.mof.gov.sa/en/Documents/Government_Tenders_and_Procurement_Law.pdf

23 Communications, Space & Technology Commission (2023). “Regulation No. 1482.” Available at: https://www.cst.gov.sa/en/regulations-and-licenses/decisions/Regulation-1482

24 National Cybersecurity Authority (NCA) (2024). ‘Cloud Cybersecurity Controls (CCC 2-2024).’ Available at: https://nca.gov.sa/en/regulatory-documents/controls-list/ccc/

25 Digital Government Authority (2023). “Guideline for Cloud Computing Adoption by Government Agencies.” Available at: https://dga.gov.sa/sites/default/files/2023-09/Guideline%20for%20Cloud%20Computing%20Adoption%20by%20Government%20Agencies%20–%20V1.0.pdf

26 Minors’ Data Protection Policy National Data Management Office (2020). Children and Incompetents’ Data Protection Policy. Available at: https://sdaia.gov.sa/ar/SDAIA/about/Documents/Children%20and%20Incompetents’%20Data%20Protection%20Policy.pdf

27 Learning Management System (LMS) MOE (2020). The Minimum Standards for a Learning Management System. Available at: https://www.moe.gov.sa/en/education/generaleducation/Documents/TheMinimum-Standards-for-Learning-Management-System-f.pdf

28 Gmedia (n.d.) Age Classification Guidelines. Available at: https://gmedia.gov.sa/en/age-classification

29 Ministry of Commerce (2019). E-Commerce Law. Available at: https://mc.gov.sa/en/Regulations/Pages/details.aspx?lawId=aaa4d4cf-ca57-41ff-a3f9-aa8500a3512c

30 Zakat, Tax and Customs Authority (ZATCA) (2024). “Detailed Guidelines for E-Invoicing.” Available at: https://www.zatca.gov.sa/en/E-Invoicing/Introduction/Guidelines/Documents/E-Invoicing_Detailed__Guideline.pdf; ZATCA (n.d.). “Solution Providers Directory.” Available at: https://zatca.gov.sa/en/E-Invoicing/SolutionProviders/Pages/SolutionProvidersDirectory.aspx; and ZATCA (2026). “ZATCA Determines the Criteria for Selecting the Targeted Taxpayers in Wave 25 for ‘Integration Phase’ of E-invoicing.” 24 July 2026. Available at: https://zatca.gov.sa/en/MediaCenter/News/Pages/Wave25-E-invoicing.aspx

31 Saudi Central Bank (2022). Counter-Fraud Framework. Available at: https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Counter_Fraud_Framework.pdf

32 Ministry of Commerce (2023). Guide to Consumer Rights and Responsibilities. Available at: https://mc.gov.sa/en/guides/Documents/CustomerGuide.pdf

33 Gmedia (n.d.). License for Producing Visual and Audio Media Content. Available at: https://gmedia.gov.sa/en/services/license-for-producing-visual-and-audio-media-content and Gmedia (n.d.). Age Classification Guidelines. Available at: https://gmedia.gov.sa/en/age-classification

34 Communications, Space & Technology Commission (2023). Data Center Services Regulations. Available at: https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1550

35 SDAIA (2023). Personal Data Protection Law. Available at: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf, SDAIA (2023). Children and Incompetents’ Data Protection Policy. Available at: https://sdaia.gov.sa/ar/SDAIA/about/Documents/Children%20and%20Incompetents’%20Data%20Protection%20Policy.pdf and Gmedia (n.d.). Age Classification Guidelines. Available at: https://gmedia.gov.sa/en/age-classification

36 Announced at the 2025 KSA ICT Indicators Forum. Livestream available at: ةيnق تlاو تاlاصتlا تارشؤم يدتنم 2025م - YouTube

37 Middle East Briefing (2025), “Saudi Arabia’s ICT Hits USUSD10 Billion: Trends and Implications.” Available at: https://www.middleeastbriefing.com/news/saudi-arabias-ict-hits-us10-billion-trends-and-implications/

38 United Nations Department of Economic and Social Affairs (UNDESA). (2024). “UN E-Government Knowledgebase – Data Center”. Available at: https://publicadministration.un.org/egovkb/en-us/Data-Center

39 Saudi Gazette. (2025). “Saudi Arabia launches new initiatives to boost digital economy and tech innovation.” Available at: https://saudigazette.com.sa/article/631227

40 KPMG (2024), KPMG tech report Saudi Arabia. Available at: https://assets.kpmg.com/content/dam/kpmg/sa/pdf/2024/02/tech-report-saudi-arabia.pdf

41 Saudi Press Agency (SPA). (2025). “CST launches initiatives to enhance digital infrastructure and innovation at LEAP25.” Available at: https://www.spa.gov.sa/en/N2077392

42 Communications, Space & Technology Commission (CST). (2025). “H.E. @msTamimi during his opening remarks at #LEAP25.” Available at: https://x.com/CST_KSA/status/1889325620401705247

43 Amazon. (2025). “Amazon and HUMAIN announce strategic partnership to invest in AI infrastructure and services in Saudi Arabia.” Available at: https://www.aboutamazon.com/news/company-news/amazon-aws-humain-ai-investment-in-saudi-arabia

44 Sources include Gartner (2025), “Gartner Forecasts MENA IT Spending to Reach USD169 Billion in 2026.” Available at: https://www.gartner.com/en/newsroom/press-releases/2025-08-04-gartner-forecasts-mena-it-spending-to-reach-169-billion-us-dollars-in-2026; and World Bank (2024), “GDP (current US$).” Available at: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

45 CST (2025), “Communications and Technology Market in 2024.” Available at: https://www.cst.gov.sa/en/media-center/news/N2025051201

46 The breakdown of software expenditure in Saudi Arabia by sectors is estimated based on Access Partnership’s previous works on the cloud computing sector in the Kingdom. The breakdown for cloud computing expenditure was applied, with the key assumption being that as most software are now provided through cloud, the software expenditure would also be proportionate to cloud expenditure.

47 Access Partnership analysis. The growth rate of the Middle East and North Africa (MENA) region is used as a conservative estimate to project the growth rate in Saudi Arabia. The growth in the Kingdom may be much larger because of increased investments into the sector. Gartner (2025), “Gartner Forecasts MENA IT Spending to Reach USD169 Billion in 2026.” Available at: https://www.gartner.com/en/newsroom/press-releases/2025-08-04-gartner-forecasts-mena-it-spending-to-reach-169-billion-us-dollars-in-2026

48 Ministry of Communications and Information Technology (MCIT) (2020). “Digital Economy Policy.” Available at: https://www.mcit.gov.sa/sites/default/files/digitaleconomypolicy_en.pdf

49 Announced at the 2025 KSA ICT Indicators Forum. Livestream available at: ةيزقتلاو تالاصتالا تارشؤم يدتنم 2025م - YouTube

50 Communications, Space & Technology Commission (CST). (2025). “Saudi Arabia ranks first globally in the 2025 ICT Development Index.” Available at: https://www.cst.gov.sa/en/N2025070301

51 Mordor Intelligence (2025). “KSA Digital Transformation Market Size & Share Analysis – Growth Trends & Forecasts (2025-2030)”. Available at: https://www.mordorintelligence.com/industry-reports/ksa-digital-transformation-market

52 Vision 2030 (2016). “National Transformation Program.” Available at: https://www.vision2030.gov.sa/en/explore/programs/national-transformation-program

53 Digital Government Authority (2024). “Saudi Arabia Ranks First in Electronic Government Services.” Available at: https://dga.gov.sa/en/news/Saudi-arabia-ranks-first-in-E-Government-services

54 Ministry of Communications and Information Technology (MCIT) (2020). “Cloud First Policy.” Available at: https://www.mcit.gov.sa/sites/default/files/cloud_policy_en.pdf

55 Communications, Space & Technology Commission (CST) (n.d.). “Cloud Computing Special Economic Zone”. Available at: https://www.cst.gov.sa/en/about/program-and-initiatives/cloud-computing-special-economic-zone-technology and Access Partnership (2023), “Access Alert | Saudi Arabia’s Cloud Computing Special Economic Zone.” Available at: Access Alert: Saudi Arabia’s Cloud Computing Special Economic Zone - Access Partnership

56 SDAIA (2020). “National Strategy for Data and AI.” Available at: https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/NationalStrategyForDataAndAI.aspx

57 Research and Markets (2024). “Saudi Arabia IoT Market Report.” Available at: https://www.researchandmarkets.com/reports/5562151/saudi-arabia-internet-of-things-iot-market-by

58 Telecoms.com (2024). “How STC helped Saudi Arabia become a digital hub.” Available at: https://www.telecoms.com/digital-ecosystem/how-stc-helped-saudi-arabia-become-the-middle-east-s-new-digital-hub

59 Arab News (2025). “Saudi business sector surpasses 1.7m registrations.” Available at: https://www.arabnews.com/node/2618852/business-economy.

60 Monshaat (2025). “Quarterly Report Q4 2024.” Available at: https://monshaat.gov.sa/sites/default/files/2025-03/Quarterly_Report_Q4_2024_EN.pdf

61 Monshaat (2025). “Quarterly Report Q4 2024.” Available at: https://monshaat.gov.sa/sites/default/files/2025-03/Quarterly_Report_Q4_2024_EN.pdf

62 Mastercard (2025). “SME Confidence Index Saudi Arabia.” Available at: https://www.mastercard.com/news/eemea/en/newsroom/press-releases/en/2025-1/february/mastercard-sme-confidence-index-smes-in-saudi-arabia-drive-digital-transformation-with-strong-optimism-for-2025/

63 Digital Government Authority (DGA) (n.d.). “Digital Transformation Index.” Available at: https://dga.gov.sa/en/DT-indicators

64 Monsha’at (n.d.). “Tomoh – Fast-growing SMEs Services.” Available at: https://www.monshaat.gov.sa/en/node/12842

65 Ministry of Health (MOH) (2025). “Sehhaty Platform.” Available at: https://www.moh.gov.sa/en/eservices/sehhaty/pages/default.aspx

Access Partnership

accesspartnership.com

Need a problem solved?

Our dedicated experts, located around the world, are here to help.

Europe

London

Thomas House, 84 Eccleston Square
Office 5.06, 5th floor,
SW1V 1PX, London
United Kingdom

+44 20 3143 4900
london@accesspartnership.com

Brussels

8th Floor, Silversquare Europe
Square de Meeûs 35
B-1000 BrusselsBelgium

brussels@accesspartnership.com

North America

Washington DC

1300 Connecticut Avenue NW,
Suite 250
Washington, DC 20036
USA

+1 202 503 1570
washingtondc@accesspartnership.com

Asia

Bangkok

188 Spring Tower
11th Floor, Unit 106, Phayathai RoadThung
Phayathai, Ratchathewi, 10400
Thailand

+ 66 (2)-8216148

Jakarta

Revenue Tower 21st Floor
Unit 104 SCBD Lot 13, Jl. Jend. Sudirman Kav.
52-53
Provinsi DKI Jakarta, 12190
Indonesia

+62 21 5020 0949

Kuala Lumpur

Common Ground Q Sentral
Level 39, Unit 39-02 (East Wing), 2A,
Jalan Stesen Sentral 2, Kuala Lumpur
Sentral, 50470
Malaysia

Hanoi

19th floor, Tower 1
Capital Place Building
No 29 Lieu Giai Street
Ngoc Khanh Ward, Ba Dinh District
Vietnam

Manila

CG8ROCKWELL Level 21, 8 Rockwell,
Hidalgo Dr., Rockwell Center, Bgy.
Poblacion, 1210
Makati City, Metro Manila
Philippines

Singapore

12 Marina View
#11-20, Asia Square Tower 2
Singapore 018961

+65 8323 7855
singapore@accesspartnership.com

Follow us