ESJ Social Sciences Peer-reviewed

Artificial Intelligence for IT Governance in Saudi Arabia: Opportunities, Challenges, and Future Directions within COBIT 2019 and ISO/IEC 38500 Frameworks

Fatma Abudaqqa
Devoteam, Saudi Arabia

Doi:10.19044/esj.2025.v21n25p125

Submitted: 21 July 2025
Accepted: 31 August 2025
Published: 30 September 2025

Cite As:
Abudaqqa, F. (2025). *Artificial Intelligence for IT Governance in Saudi Arabia: Opportunities, Challenges, and Future Directions within COBIT 2019 and ISO/IEC 38500 Frameworks.* European Scientific Journal, ESJ, 21 (25), 125. https://doi.org/10.19044/esj.2025.v21n25p125

Abstract

Saudi Arabia's Vision 2030 and the National Strategy for Data & AI have accelerated the use of artificial intelligence across public services and regulated industries, creating a need to understand how AI can support information-technology governance (ITG) through established frameworks such as COBIT 2019 and ISO/IEC 38500/38507. This study carried out a structured review of academic, industry, and policy sources published between 2008 and 2025. A total of 236 records were identified; after removing duplicates and applying clear inclusion criteria (focus on AI or ITG, relevance to Saudi Arabia, and transparent methods), 78 were included. The review process followed PRISMA principles, with quality checks rating most evidence as moderate to high. Results show that AI can strengthen ITG by improving compliance monitoring, decision-making, and delivery of benefits. Reported outcomes include stronger governance links in empirical models, national adoption intent of about 63% of firms, projected government productivity gains of up to $56 billion a year, and a case reporting reductions of 93% in monitoring costs and 92% in accident fatalities. A comparison with EU, NIST, and OECD frameworks revealed gaps in Saudi guidance but also near-term opportunities such as creating an AI risk taxonomy, adapting impact assessment templates, and setting clearer rules for incident reporting. Limitations include reliance on mixed-quality data, policy-based estimates, and limited post-deployment evidence. Overall, the findings suggest that AI can measurably enhance ITG in Saudi Arabia when supported by risk-based obligations, lifecycle controls, and board-level oversight, providing regulators and boards with practical steps for improvement.

Keywords: Artificial Intelligence (AI), Governance, Transformation, Saudi Arabia, AI Policy, COBIT 2019, ISO/IEC 38500/38507, NIST AI RMF

Introduction

Saudi Arabia's Vision 2030 sets an ambitious course to transform the Kingdom into a diversified, knowledge-based economy. Central to this strategy is the rapid and intentional adoption of artificial intelligence (AI) to enhance efficiency, transparency, and global competitiveness. The establishment of the Saudi Data and Artificial Intelligence Authority (SDAIA) and the launch of the National Strategy for Data and AI (NSDAI) underscore the Kingdom's determination to become a global AI leader by 2030 (Memish et al., 2021).

However, this speed also introduces significant risks. As Saudi organizations integrate AI into core processes (e.g., in healthcare diagnostics, financial services, and smart city initiatives), they introduce new risks related to data privacy, algorithmic bias, cybersecurity, and accountability. For example, AI-driven predictive models can improve decision-making but may also embed opaque reasoning that complicates oversight. Similarly, AI in finance or healthcare offers efficiency gains, but without proper controls, it can lead to discriminatory outcomes or privacy breaches. The strategic ambition to leverage AI must therefore be counterbalanced by structured, auditable governance.

Without clear frameworks, the unintended consequences of AI, such as unfair outcomes or privacy violations, could undermine public trust. While Saudi studies emphasize AI ambition, they rarely progress to a concrete governance artefact. This study addresses that gap by proposing an operational model aligned to COBIT 2019 and ISO/IEC 38500/38507, tailored to Saudi institutions. This study explores how AI can enhance IT governance in Saudi Arabia by evaluating opportunities and challenges through the lens of COBIT 2019 and ISO/IEC 38500.

The review includes a comparative alignment of the EU AI Act, NIST AI RMF, OECD AI Principles, and ISO/IEC 38507 with PDPL, SDAIA–NDMO, and DGA frameworks, highlighting key gaps and quick wins. The central question guiding this research is: How can Saudi Arabia transition from high-level AI ambition to robust, effective, and ethically grounded IT governance practices?

Methods

Review Design

This study employed a qualitative literature and policy review, guided by PRISMA 2020 recommendations. The aim was to examine how information technology governance (ITG) frameworks, particularly COBIT 2019 and ISO/IEC 38500/38507, are applied within the Saudi context of artificial intelligence (AI) adoption and Vision 2030 initiatives.

The review encompassed a broad evidence base, including peer-reviewed academic publications, industry reports, international standards, and government documents relevant to AI governance and ITG.

Sources and Search Strategy

Data sources were identified through systematic searches in Scopus, Web of Science Core Collection, and Google Scholar (first 200 results per query). Grey literature was gathered from recognized industry and standards bodies (ISACA, ISO, ITU, NIST, OECD) and Saudi government portals (SDAIA, MCIT, DGA, NDMO, NCA, SAMA, CST).

Searches covered January 2008–August 2025, reflecting both baseline ITG practice and contemporary AI governance. The last search was completed on August 28, 2025.

Representative keywords combined AI terms, IT governance frameworks, and the Saudi context (English and Arabic). Full search strings and a search log are available in Appendix B.

Eligibility and Screening

Inclusion criteria required sources to:

1. Explicitly address AI or IT governance,
2. Be published between 2008 and 2025, and
3. Provide conceptual, policy, or implementation insights relevant to Saudi Arabia.

Exclusion criteria included opinion pieces lacking evidence, marketing-oriented reports, and items with insufficient methodological transparency or no governance focus.

The screening process followed PRISMA 2020 guidelines. An initial 236 records were identified. After removing 34 duplicates, 202 items were screened by title and abstract, with 112 excluded. 90 full texts were assessed, and 12 were excluded for reasons such as insufficient Saudi context, lack of governance content, commentary-only nature, or inaccessible full text. This left 78 included studies, detailed in Appendix E. A PRISMA flow diagram is provided in Appendix A.

Analytical Process and Coding

The 78 included documents were imported into NVivo for qualitative analysis. A mixed coding approach was applied:

- Deductive coding using COBIT 2019 governance and management objectives (EDM, APO, BAI, DSS, MEA) and ISO/IEC 38500/38507 principles (Responsibility, Strategy, Acquisition, Performance, Conformance, Human Behavior).
- Inductive coding based on themes emerging from the literature, such as predictive analytics, compliance automation, ethical risks, cybersecurity threats, regulatory readiness, Vision 2030 program delivery, PDPL implementation, and workforce reskilling.

For interpretive clarity, themes were grouped into two overarching domains: Opportunities (e.g., predictive analytics, compliance automation, improved service delivery) and Challenges (e.g., ethical risks, cybersecurity vulnerabilities, regulatory gaps, capacity constraints).

Reliability safeguards. Two coders double-coded a 20% stratified sample. Inter-coder agreement was strong (Cohen's κ = 0.84 at domain level; median κ = 0.80 at sub-theme level, range 0.74–0.88). Discrepancies were resolved by discussion; the refined codebook was then applied to the full set.

Framework Selection Rationale

The choice of COBIT 2019 and ISO/IEC 38500 (with 38507 for AI-specific governance) was deliberate. COBIT provides granular, process-oriented detail suited for aligning IT with organizational objectives, while ISO/IEC 38500 offers a principle-driven, board-level perspective. Together, they form a complementary analytical structure balancing operational depth with strategic oversight.

Alternative frameworks were considered. ITIL was not adopted due to its service-management focus, and the NIST AI Risk Management Framework was used only as a comparative reference, given its limited uptake so far in the Saudi governance environment.

Quality Appraisal

Given the mix of sources, a hybrid appraisal framework was applied:

- Empirical studies were assessed with the Mixed Methods Appraisal Tool (MMAT, 2018).
- Policy and grey literature were evaluated on authority, accuracy, and currency (AAC).
- Standards were assessed on scope clarity and evidence base.

Each source was rated High, Moderate, or Low quality. Of the 78 included items, 29 were high quality, 38 moderate, and 11 low. Sensitivity checks excluding low-quality items showed no change in the overall direction of findings.

Heterogeneous evidence was consolidated in a structured matrix mapping each major claim to its primary source, source type (peer-reviewed, policy/grey, or consulting), method/data, temporal window, and evidence strength rating. Strength ratings were anchored to previously applied MMAT/AAC quality appraisals and intercoder reliability checks. “High” strength denotes peer-reviewed empirical studies with transparent methods and fit-for-purpose measures; “Moderate” refers to peer-reviewed qualitative work or policy/consulting reports with partial transparency; “Low” denotes single-organization or promotional case write-ups without auditable methods. Bold numerical estimates were triangulated across multiple source types when available, while single-source claims were flagged as indicative only. The full evidence matrix is presented in Table 2.

Validation Measures

Findings were validated through triangulation across academic, industry, and official policy sources. This multi-source corroboration strengthened the credibility of the conclusions and ensured alignment with both global best practice and the realities of Saudi Arabia’s governance environment.

All supplementary materials are presented in the appendices.

- The PRISMA flow diagram and exclusion reasons (Appendix A),
- Search strings and collection log (Appendix B),
- Codebook and reliability outputs (Appendix C),
- Quality appraisal matrix (Appendix D),
- The full list of 78 included records (Appendix E).

In addition to literature synthesis, this research adopts a light design-science approach. Insights from COBIT 2019 and ISO/IEC 38500/38507 were distilled into requirements for roles, controls, KPIs, and roadmaps. The artefact was evaluated analytically by framework traceability, with field validation recommended for future studies.

Results

Strategic Analysis of Saudi Arabia’s AI Vision and Regulatory Framework

Saudi Arabia’s approach to AI governance is driven by Vision 2030 and related national strategies and shaped by a rapidly evolving regulatory environment. Understanding this context is essential to appreciating both the opportunities and challenges for IT governance.

Vision 2030 is Saudi Arabia’s wide-ranging reform agenda aimed at diversifying the economy and driving innovation. Central to this vision are digital transformation and artificial intelligence (AI), which are identified as key engines of future growth (Accenture, 2025). To translate this vision into action, the Saudi Data and AI Authority (SDAIA) launched the National Strategy for Data and AI (NSDAI) in 2020. It focuses on attracting investment, strengthening research and innovation, as well as accelerating technology adoption through strong digital infrastructure.

The Saudi Data and Artificial Intelligence Authority (SDAIA), established by royal decree in August 2019, is the central coordinating body for AI in the Kingdom. SDAIA oversees the NSDAI and drives its implementation, serving as a national regulator for data and AI by formulating policies, standards, and guidelines. For example, SDAIA leads the development of the regulatory framework for data (including data governance and protection) and promotes ethical AI practices across sectors. In practice, SDAIA has collaborated with global partners to build infrastructure, such as the National Data Bank and cloud services. They have also focused on talent development, upskilling over 45,000 professionals to date, with plans to train an additional 25,000 women in AI skills (Accenture, 2025).

Moreover, these sectoral priorities align with observed AI-driven transformations: in healthcare, institutions are deploying AI tools for diagnostics and operational efficiency, improving image interpretation in radiology and monitoring COVID-19 infection patterns to manage resources (Memish et al., 2021; Saeed et al., 2023). In finance, banks use algorithms for credit scoring, positioning Saudi Arabia as a budding fintech hub (Al-Baity, 2023). In education, adaptive learning platforms tailor instructional materials to individual student needs, though effective adoption demands teacher training and ethical guidelines (Alshehri & Alotaibi, 2023; Elhajji et al., 2020). These examples illustrate the momentum behind AI adoption and underscore why robust governance is needed to sustain growth while addressing challenges like data privacy, talent gaps, and regulatory maturity (Muafa et al., 2024).

AI Enhancements in Saudi IT Governance: Case Studies and Evidence

Saudi public and private organizations report concrete benefits from embedding AI into their IT governance and operations. For example, the Saudi Digital Government Authority (DGA) highlights that Generative AI (GenAI) adoption is expected to "revolutionize digital governance", making government services more efficient, proactive, and data-driven. DGA experts note GenAI can improve regulatory compliance, with smart-regulation use cases "enhancing compliance, reducing monitoring costs, and streamlining administration" (Digital Government Authority, 2025, p. 26). A Ministry of Transport case report on IoT-enabled lighting reported monitoring cost reductions of 93%, accident fatality reductions of 92%, and efficiency gains of 80%. As a single policy case, this evidence is rated moderate in strength and not independently audited (Digital Government Authority, 2024, p. 52). Recent research highlights that AI governance outcomes depend heavily on organizational context and the influential support of leadership (Alshahrani et al., 2022). Drawing on this qualitative case study of Saudi public-sector organizations, the study found that effective AI adoption requires both technical readiness and a shift in organizational focus. The findings also show that while AI dashboards and analytics enhance oversight, such as through real-time risk alerts, they introduce challenges related to ethics and data sharing.

Empirical data from national surveys, econometric analyses, and documented implementation cases provide robust evidence of AI's measurable influence on decision-making and operational efficiency within Saudi IT governance frameworks. By 2024, Saudi Arabia had emerged as a leading regional investor in IT and AI, with official estimates projecting government expenditure exceeding USD 11 billion in that year, primarily directed toward cloud computing and AI initiatives. A survey cited in Almaqtari (2024) indicates that approximately 63% of Saudi firms are using or planning AI adoption. The evidence is secondary and is therefore graded as moderate in strength.

Findings from a national survey of accountants, auditors, and IT leaders, analyzed using structural equation modelling, demonstrated a substantial positive relationship between AI adoption and IT governance efficacy ($\beta = 1.002$, $p < 0.01$) (Almaqtari, 2024, p. 11). Organizations integrating AI exhibited markedly stronger governance practices, including enhanced data policy enforcement and the institutionalization of oversight committees.

As noted in the same econometric analysis (Almaqtari, 2024), improvements in IT governance enabled by AI had a significant positive impact on both accounting and auditing activities. Organizations with AI-enabled governance were consequently able to execute financial controls and audits more effectively. Scenario modelling by the Digital Government Authority (2025) estimates potential public-sector productivity gains of up to ≈$56 billion annually. This figure is derived from a single policy model and is treated as indicative pending independent replication.

Across various case studies and reports, recurring patterns indicate that embedding AI tools within governance systems accelerates decision-making, strengthens compliance, and improves service delivery efficiency.

Framing the Literature and Research Context

The literature on IT governance (ITG) and artificial intelligence (AI) has expanded considerably, with Saudi Arabia emerging as a focal point due to Vision 2030 and the National Strategy for Data and AI. Governance frameworks such as COBIT 2019 and ISO/IEC 38500, alongside its AI-specific extension ISO/IEC 38507, provide the principal theoretical scaffolding for examining how AI can strengthen ITG processes and oversight mechanisms. COBIT offers a process-oriented lens that maps AI applications to specific governance domains, including benefits delivery, risk optimization, compliance monitoring, and assurance. ISO/IEC standards, in turn, articulate broader principles of responsibility, conformance, and human-centered governance, which are particularly relevant when addressing ethical challenges of AI adoption. Together, these frameworks provide a multi-layered perspective that enables both operational mapping and normative evaluation of AI in governance contexts.

Previous Saudi studies have documented significant progress in AI integration across public administration, finance, healthcare, and education. There are indications of quantitative increments of the quality of decision making, monitoring, and productivity, much of which, however, is descriptive and not rigorously evaluative. Reports of governments and of the sector, particularly those of the Saudi Data and AI Authority (SDAIA) and the Digital Government Authority (DGA), reflect huge advantages from flagships and from pilot projects of generative AI. These reports are usually fraught with the risk of optimism bias and methodologically uninformative and so their results are more marketing material than empirical. Scholar contributions, while methodologically more demanding, are often constructed on inhomogeneous concepts such as “digital readiness” or “AI assimilation” and so are not always directly transferable between studies.

Qualitative investigations emphasize leadership commitment and organizational readiness as prerequisites for effective AI governance, but they seldom benchmark outcomes against COBIT or ISO standards. A smaller body of empirical research in regulated sectors, such as accounting and auditing, offers more robust evidence by employing statistical models that link AI adoption directly to ITG performance, yet these studies remain the exception.

In combination, the Saudi scholarship displays breadth and fragmentation. As much as there is a strong narrative of sectoral experimentation and national ambition, there also runs a hiatus of systematically bridging AI results with generally accepted models of governance. In doing so, the work extends the scholarship further by critically assessing the quality, bias, and comparability of sources. It particularly matches Saudi evidence with COBIT and ISO controls and recodes divergent results into commensurable governance outcome categories. In doing so, the process at the same time lays bare the limitations of scholarship heretofore and indicates how AI contributions to ITG best might be theorized and observed empirically in the Saudi context.

To synthesize the state of the art, the following table concentrates core Saudi contributions, noting sectoral scope, methodological approach, governance framing, key findings, and potential biases. This enables sharper positioning of Saudi research relative to international best practices, while also providing a structured benchmark for future studies.

Table 1: State of the art: Synthesis Table (Saudi context)

Study / Source (Saudi)	**Sector / Scope**	**Method / Data**	**Governance lens used**	**Normalized ITG outcome (COBIT/ISO)**	**Key finding (Saudi context)**	**Quality & bias notes**	**Comparability notes**
Early COBIT use in KSA orgs (legacy ITG baseline) - Abu Musa (2009)	Cross-sector	Empirical (pre-AI)	COBIT (general)	APO/MEA setup maturity	Established baseline ITG processes pre-AI; sets context for later AI mapping	Peer-reviewed; dated re: AI	Good baseline; no AI endpoints
ITG frameworks in KSA (exploratory scan) - Almaawi, Alsaggaf, & Fasihuddin (2020)	Cross-sector	Exploratory	COBIT/ISO (catalog)	Governance adoption visibility	Describes adoption; no AI-specific effect testing	Peer-reviewed; descriptive	Mapable to EDM/APO; lacks outcomes
AI assimilation in public sector - Alshahrani, Dennehy, & Mäntymäki (2022)	Government	QLR (interviews/ cases)	Implicit governance	EDM (leadership attention), APO (strategy)	Leadership attention/readiness predict AI assimilation	Peer-reviewed; solid qualitative rigor	Lacks control-level COBIT/ISO alignment
AI & ITG in accounting/auditing - Almaqtari (2024)	Regulated functions	SEM (quantitative)	Explicit ITG	EDM03/ MEA03	AI adoption → stronger ITG (significant effect)	Peer-reviewed; quantified effect	Highly comparable; effect size anchors
SDAIA / DGA reports (GenAI, readiness) - Digital Government Authority (2024; 2025)	Digital government	PR (metrics & cases)	Policy framing	APO13/MEA03 (compliance), DSS (service)	Compliance & efficiency gains; dramatic cost/safety improvements in pilots	Potential optimism bias; partial transparency	Useful operational anchors; triangulate with academic
Sector reviews (finance/health/education) - Memish et al. (2021); Al-Baity (2023); Alotaibi & Alshehri (2023); Saeed et al. (2023); Muafa et al. (2024)	Domain-specific	Literature reviews / cases	Mixed	EDM02 (benefits), APO12 (risk), DSS05 (security)	Rapid AI uptake; governance risks around privacy, bias, auditability	Varies; some conceptual	Endpoints re-coded to COBIT/ISO here

Table 2 consolidates major claims with their source type, method, time frame, and evidence strength. It flags single-source or indicative figures, notes triangulation where available, and links each claim to COBIT/ISO governance domains.

Table 2: Evidence matrix

Major claim (short)	**Primary source(s)**	**Source type**	**Method / data**	**Time window**	**Strength**	**Triangulation / caveat (and COBIT/ISO hook)**
GenAI can enhance compliance & reduce monitoring/admin costs in government	DGA (2025, p.26)	Policy/grey	Concept note + exemplars	2025	Moderate	Single-source (policy); converges with quantitative ITG effects below. (COBIT MEA03/APO13; ISO Conformance)
Government GenAI productivity up to ≈$56B/yr	DGA (2025, p.26)	Policy/grey	Model-based estimate (scenario)	2025	Low–Moderate	Single-source model; treat as indicative; needs independent replication. (EDM02 benefits)
IoT lighting case: monitoring cost ↓93%, accident deaths ↓92%, efficiency ↑80%	DGA (2024, p.52)	Policy/grey	Case study (project report)	2024	Moderate	Single case; unknown auditability; plausibility supported by smart-infra literature. (DSS/MEA)
~63% Saudi firms using/planning AI	Deloitte survey as cited in Almaqtari (2024, p.4)	Scholarly (secondary)	Survey (business adoption)	2024	Moderate	Secondary citation; direct instrument not reproduced here. (EDM05 stakeholder readiness)
AI adoption → stronger IT governance (β=1.002, p<0.01)	Almaqtari (2024)	Peer-reviewed	SEM (quant)	2024	High	Convergent with policy narratives; provides effect size anchor. (EDM03/MEA03)
SDAIA talent: >45k upskilled; plan +25k women	Accenture (2025)	Consulting	Program metrics	2019–2025	Moderate	Single consulting source; treat as directional; aligns with SDAIA mandate. (APO07 workforce)
Healthcare: AI improves image interpretation/ops; COVID monitoring	Memish et al. (2021); Saeed et al. (2023)	Peer-reviewed	Reviews/cases	2020–2023	Moderate	Convergent across two sources; generalizable to APO12 risk/EDM02 benefits.
Public-sector AI assimilation depends on leadership attention & readiness	Alshahrani et al. (2022)	Peer-reviewed	Qualitative case study	2022	Moderate	Convergent with your thematic synthesis; maps to EDM/APO.
Adversarial ML risks in clinical AI	Finlayson et al. (2019)	Peer-reviewed	Experimental / review	2019	High	Strong external validity for risk posture; apply with local caveats. (APO12/13, DSS05)
Cybersecurity awareness only moderate among students/staff	Aljohni et al. (2021)	Peer-reviewed	Survey	2021	Moderate	Supports skills/awareness gap claims; action for APO12/EDM05.

Discussion

Analytical Framework: COBIT 2019 and ISO/IEC 38500 Series

To systematically assess AI's impact on IT governance, the study focuses on two established frameworks:

- **COBIT 2019**

COBIT (Control Objectives for Information and Related Technologies) is an ISACA framework for enterprise IT governance and management. COBIT 2019 is the latest version, building on a 20-year legacy (Almaawi et al., 2020). This framework is organized into domains (EDM: Evaluate, Direct and Monitor; APO: Align, Plan and Organize; BAI: Build, Acquire and Implement; DSS: Deliver, Service and Support; MEA: Monitor, Evaluate and Assess) and defines 40 high-level processes and numerous management objectives. COBIT emphasizes a governance system that is holistic, end-to-end, and dynamic, and it distinguishes governance (overarching control by the board) from management (implementation by executives). For example, COBIT's EDM domain focuses on board-level practices, while APO and DSS deal with operational processes. The COBIT framework was used to map AI initiatives and challenges to specific processes and objectives, and to ensure alignment between technology use and enterprise goals.

- **ISO/IEC 38500 (and 38507)**

The second framework is ISO/IEC 38500, which is an international standard for corporate governance of IT. It provides six guiding principles, including: Responsibility, Strategy, Acquisition, Performance, Conformance and Human Behavior (Calder, 2008). These principles are intended for boards and executives. For AI, ISO/IEC 38507:2022 is a companion standard that addresses the governance implications of AI specifically (ISO/IEC 38507, 2022). ISO/IEC 38507 guides governing bodies to oversee the use of AI so that it remains effective, efficient, secure, and ethical. ISO/IEC 38500 offers a high-level, principle-based lens (e.g. requiring conformance with laws and ethics and ensuring accountability) that complements COBIT's process-level detail.

Using both frameworks in the Saudi context helps identify where AI supports governance goals. For example, AI's strength in predictive analytics (an opportunity) and the risk of algorithmic bias (a challenge) can be linked to COBIT processes and ISO principles. This combined approach provides a clear and organized way to assess AI governance.

Developing a Comprehensive National AI Governance Framework

Establishing a robust AI governance ecosystem in Saudi Arabia requires the creation of a comprehensive national framework that integrates ethical, legal, and operational standards across all stages of AI deployment.

Such a framework should move beyond voluntary principles toward legally binding regulations. Research by Jobin et al. (2019) indicates a global convergence around five core ethical principles for AI: transparency, justice/equity, non-maleficence, responsibility, and privacy. However, this research also highlights substantive divergence in how these principles are interpreted and implemented across different contexts. The inherent ethical dilemmas of AI present a profound challenge to public trust and societal acceptance. This necessitates a proactive, multi-faceted approach that not only develops technical solutions, such as explainable AI (XAI) and bias testing, but also integrates cultural values, such as Islamic principles, and fosters broad public engagement.

Adopting insights from international models such as the European Union’s AI Act, the National Institute of Standards and Technology’s AI Risk Management Framework (NIST AI RMF), and the Organization for Economic Co-operation and Development (OECD) AI Principles can help incorporate established global best practices. The NIST AI RMF provides a structured approach to identifying, assessing, and mitigating AI-related risks through four key functions: Govern (establishing governance structures), Map (identifying risks), Measure (evaluating performance and risks), and Manage (implementing risk mitigation) (NIST, 2023). Likewise, the OECD AI Principles - adopted as the first intergovernmental standard for AI emphasize trustworthy AI that promotes human rights and democratic values, focusing on inclusive growth, human-centered fairness, transparency, safety, and accountability (OECD, 2019).

While leveraging these international frameworks can strengthen Saudi Arabia’s AI governance, customization is essential to reflect the Kingdom’s cultural, economic, and regulatory environment. Balancing universal standards with local adaptation will be critical for ensuring societal acceptance and policy effectiveness (Zeng et al., 2021).

AI Opportunities in Enhancing IT Governance in Saudi Arabia

Saudi Arabia’s aggressive AI agenda presents concrete opportunities for IT governance professionals to enhance their roles. Aligning AI capabilities with COBIT 2019 objectives and ISO/IEC 38500 principles empowers professionals to seize these opportunities and drive positive change in their organizations.

The following table presents the mapping of AI opportunities to specific COBIT processes and ISO principles.

Table 3: Mapping AI Opportunities to COBIT 2019 Domains and ISO/IEC 38500 Principles

AI Opportunity	Description of AI Capability	Relevant COBIT 2019 Domain/Process	Relevant ISO/IEC 38500 Principle	Impact on IT Governance
Data-Driven Decision-Making	AI enables predictive analytics, processing vast data to detect patterns, anomalies, and risks in real time for proactive decisions.	EDM (Evaluate, Direct and Monitor), EDM01, EDM02	Strategy, Performance	Enhances strategic foresight, optimizes IT investments, allows dynamic adaptation of governance processes.
Automation of Governance Tasks	AI systems automate compliance monitoring, audit reporting, and policy enforcement, reducing human error and administrative costs.	APO (Align, Plan and Organize), DSS (Deliver, Service and Support)	Performance, Conformance	Increases efficiency and accuracy in governance, frees up professionals for strategic tasks.
Advanced Risk Management & Cybersecurity	AI techniques (anomaly detection, threat intelligence) continuously monitor networks, identifying unusual patterns and preventing breaches.	APO12 (Managed Risk), APO13 (Managed Security), DSS05 (Managed Security Services)	Performance, Conformance	Transforms cybersecurity to a proactive, adaptive posture, reduces vulnerability window, enhances resilience.
Enhanced Transparency & Accountability	AI turns complex data into user-friendly dashboards/reports, and NLP/chatbots provide real-time explanations of governance information.	EDM05 (Ensure Stakeholder Engagement)	Human Behavior, Conformance	Builds public trust, improves oversight, fosters stronger public engagement, aligns decisions with strategic goals.
Optimized Resource Allocation	AI-driven tools prioritize IT initiatives by evaluating risk and value.	EDM04 (Ensure Resource Optimization), APO (Align, Plan and Organize)	Strategy, Performance	Ensures resources are allocated to most impactful projects, streamlines portfolio management, improves efficiency and strategic outcomes.
Fostering Continuous Improvement	AI spots inefficiencies and suggests process enhancements, supporting continuous improvement and fostering an agile governance culture.	MEA (Monitor, Evaluate and Assess)	Performance	Makes organizations more adaptive and forward-thinking, aligns with innovation goals, ensures governance frameworks remain relevant.
Upholding Ethical Standards	AI identifies biases in decision-making algorithms and encourages fairness and inclusivity within IT governance.	EDM05 (Ensure Stakeholder Engagement)	Responsibility, Human Behavior	Strengthens public trust, ensures AI aligns with societal values and human-rights norms, supports ethical oversight.

Traditional IT governance relies on retrospective analyses of past data, whereas AI enables predictive analytics to anticipate future challenges and opportunities. Machine learning models can process vast amounts of operational data to detect patterns, anomalies, and risks in real time, allowing IT leaders to make more informed, proactive decisions (Kumar et al., 2025). For organizations undergoing rapid digital transformation, the ability to generate predictive insights will be pivotal for maintaining competitiveness and modernizing governance practices. Within COBIT, AI strengthens the EDM (Evaluate, Direct, and Monitor) domain by improving several governance processes, with the greatest impact seen in EDM02: Ensure Benefits Delivery, EDM03: Ensure Risk Optimization, and EDM04: Ensure Resource Optimization. In EDM02, AI can predict the value of IT investments, track actual results, and guide better decision-making. In EDM03, AI tools can detect risks early and recommend timely solutions.

AI-based systems can now handle activities like compliance monitoring, audit reporting, and policy enforcement, freeing up time for professionals to focus on more strategic tasks. These tools not only lower administrative costs and reduce human error, but they also enhance accuracy in governance processes, making professionals more productive and effective (Alshehri & Mulyata, 2024).

AI also significantly impacts risk management and cybersecurity. For example, AI techniques such as anomaly detection and threat intelligence can continuously monitor network traffic, identifying unusual patterns and alerting administrators before minor issues escalate into major breaches (Abdallah et al., 2025).

Moreover, AI plays a significant role in promoting transparency and accountability through advanced reporting and visualization. By turning complex data into clear, user-friendly dashboards and reports (Farraj, 2024), it enables stakeholders to understand key insights better and improve oversight. In environments where trust from both citizens and the private sector is essential, such transparency strengthens institutional credibility and fosters stronger public engagement, making professionals feel more trusted and responsible.

AI can also improve stakeholder communication and engagement, addressing ISO/IEC 38500's Human Behavior principle by respecting stakeholders' need to understand IT decisions. Natural language processing and AI-driven chatbots can provide real-time, user-friendly explanations of governance information to diverse stakeholders, including non-technical audiences (Alshehri & Mulyata, 2024). Enhanced stakeholder engagement promotes better alignment between IT governance policies and organizational objectives, further strengthening governance effectiveness.

As Saudi Arabia navigates the ethical challenges posed by emerging technologies, leveraging AI to oversee and implement ethical guidelines will be essential for sustaining public trust. In this way, AI holds considerable promise for strengthening ethical governance practices.

Key Challenges for AI-Enhanced IT Governance

While the opportunities for AI in Saudi IT governance are substantial, realizing its full potential necessitates addressing several key challenges. The urgency to establish robust regulatory and legal frameworks, for instance, becomes increasingly apparent as AI takes center stage. The Saudi Data and Artificial Intelligence Authority (SDAIA) has introduced voluntary ethical principles, while the newly enacted Personal Data Protection Law (PDPL) strengthens privacy safeguards. Nevertheless, the absence of binding legislation specifically governing AI leaves organizations without definitive guidance on issues such as fairness, safety, liability, and reporting. This regulatory uncertainty complicates compliance, undermining ISO/IEC 38500's Conformance principle by leaving requirements undefined. Furthermore, it weakens COBIT 2019's APO01 (Managed I&T Management Framework) and makes MEA03 (Monitor Compliance with External Requirements) difficult to execute, as the scope of "external requirements" remains ambiguous. Bridging this gap is not a future consideration, but a pressing need that requires Saudi regulators to codify ethics principles into enforceable standards rather than incentives alone (Polok & Dussin, 2025).
Simultaneously, a significant shortage of skilled professionals in AI and data science is posing a serious challenge to advancing governance efforts. Surveys reveal that while approximately 56% of employees have been exposed to AI, a similar percentage lack the deeper programming or analytical skills that are truly necessary (AlQahtani, 2023). This skills gap makes it difficult to meet the Responsibility principle in ISO/IEC 38500. Although the addition of international experts has brought valuable expertise to Saudi Arabia, achieving the National Strategy for Data and AI's goal of training 20,000 specialists by 2030 will require substantial investment in local education and the establishment of strong strategic partnerships.

Furthermore, infrastructure disparities are a significant constraint to nationwide AI deployment. While urban hubs like NEOM demonstrate the potential with 5G networks and advanced data centers, many rural areas still lack reliable high-speed connectivity, hindering e-government and telemedicine services. Addressing these gaps will necessitate the extension of high-speed networks to remote regions and the modernization of legacy systems, as well as the careful management of data-sovereignty concerns tied to foreign cloud and AI vendors (Aljijakli & Akkari, 2025).

The adoption of AI broadens the cybersecurity attack surface, introducing threats that traditional measures may not address. In Saudi healthcare systems, for instance, adversarial machine-learning attacks could involve altering MRI scan pixels, leading an AI diagnostic tool to misclassify a malignant tumor as benign (Finlayson et al., 2019). In financial services, data poisoning may occur when attackers insert false transaction records into training datasets, causing the AI to overlook fraudulent activity (Barreno et al., 2010). Model theft is another risk, whereby repeated queries to a Saudi smart-city traffic prediction system could allow reconstruction of its proprietary algorithms. These vulnerabilities are exacerbated by inconsistent cybersecurity awareness among stakeholders. Mitigation can be guided by COBIT 2019 and ISO/IEC, which recommend access controls, dataset integrity checks, adversarial testing, and regular security training.

Studies show only moderate familiarity with best practices among non-technical staff and non-computing students (Aljohni et al., 2021). This further threatens ISO/IEC 38500's Performance principle and COBIT's DSS05 (Managed Security Services), as well as APO12/APO13 (Managed Risk/Security). Saudi organizations must therefore develop AI-specific security controls such as continuous model monitoring and anomaly detection, as well as establish a dynamically adaptive cybersecurity posture in line with COBIT's Dynamic Governance principle.

Finally, ethical and societal considerations are significant. Government use of AI for surveillance or control can erode public trust and reinforce authoritarian structures (Ibrahim, 2024), while biased training data may perpetuate discrimination in hiring or policing. The "black box" nature of many advanced models hinders accountability. In this situation, such concerns implicate ISO/IEC 38500's Responsibility and Human Behavior principles and COBIT's EDM05 (Stakeholder Engagement), calling for both technical measures (bias testing, explainability tools) and cultural initiatives (ethics training, reporting mechanisms) to make sure AI aligns with Islamic values and human-rights norms.

The following table summarizes key AI governance challenges and their corresponding implications for COBIT 2019 and ISO/IEC 38500.

Table 4: Key AI Governance Challenges and Their Impact on COBIT 2019 and ISO/IEC 38500

AI Governance Challenge	**Description of Challenge**	**Specific Impact on COBIT 2019**	**Specific Impact on ISO/IEC 38500 Principle**	**Broader Implication**
Regulatory & Legal Framework Gaps	Absence of binding AI-specific legislation on fairness, safety, liability, and reporting.	Undermines APO01 (Managed I&T Management Framework) by creating ambiguity; makes MEA03 (Monitor Compliance with External Requirements) difficult to execute.	Undermines Conformance (leaving requirements undefined).	Creates legal and reputational risks for organizations; potentially stifles responsible innovation due to legal uncertainty; hinders consistent accountability.
Shortage of Skilled Professionals	Significant lack of deep programming and analytical skills in AI and data science among the workforce.	Hinders effective implementation of all domains, particularly APO (Align, Plan and Organize) and BAI (Build, Acquire and Implement) objectives related to AI development and deployment.	Difficult to meet Responsibility (lack of expertise for effective management).	Impedes effective AI governance and risk management; creates a bottleneck for national AI ambitions; limits the ability to ensure ethical deployment.

Infrastructure Disparities	Uneven distribution of high-speed connectivity and advanced data centers, particularly in rural areas.	Affects DSS (Deliver, Service and Support) by hindering equitable service delivery; complicates data management across distributed environments.	Challenges Performance (uneven service delivery); raises concerns for Strategy (limited nationwide AI adoption).	Creates a digital divide, limiting equitable access to AI services; raises data sovereignty concerns with foreign cloud/AI vendors; impedes national AI adoption.
Expanded Cybersecurity Attack Surface & Adversarial AI	AI introduces new vulnerabilities (e.g., evasion, data poisoning, model extraction attacks) that traditional defenses cannot address.	Threatens DSS05 (Managed Security Services), APO12 (Managed Risk), APO13 (Managed Security) by creating new, complex attack vectors.	Threatens Performance (AI system reliability); undermines Conformance (security standards); challenges Responsibility (accountability for breaches).	Leads to sophisticated cyber threats; compromises AI system integrity and trustworthiness; erodes public trust due to potential for widespread harm.
Ethical & Societal Considerations	Risks of algorithmic bias, "black box" opacity, potential for surveillance/control, and erosion of public trust.	Implicates EDM05 (Ensure Stakeholder Engagement) by requiring proactive communication; challenges all domains to integrate ethical considerations.	Implicates Responsibility (accountability for ethical outcomes); Human Behavior (respecting individuals); Conformance (adherence to ethical norms).	Risks public trust and societal acceptance of AI; perpetuates discrimination; hinders accountability; necessitates alignment with cultural values and human rights.

However, it's important to remember that AI, when governed effectively, has the potential to significantly enhance decision-making. Only by addressing regulatory uncertainty, talent shortages, infrastructure gaps, cybersecurity vulnerabilities, and ethical risks in a coordinated, framework-driven manner can Saudi governance bodies fully realize this potential.

To move from mapping evidence to practical application, this study proposes a Saudi-specific AI–ITG governance model, detailed below.

Comparative Regulatory Alignment

A structured alignment was conducted between global and Saudi governance instruments. International frameworks emphasize risk-based regulation, operational guidance, and high-level governance principles, while Saudi instruments focus on binding privacy and data-management obligations. The comparison reveals points of convergence, gaps in AI-specific regulation, and opportunities for near-term improvements.

Table 5: Alignment of international AI instruments with Saudi PDPL/SDAIA guidance, with gaps and quick wins

Dimension	**EU AI Act**	**NIST AI RMF**	**OECD AI Principles**	**ISO/IEC 38507**	**Saudi PDPL / NDMO / DGA**	**Gap vs. Saudi**	**Quick wins (≤ 12 months)**
Legal status & scope	Binding AI law, phased duties	Voluntary framework	Non-binding values	Governance guidance	Binding privacy/data laws; no AI law	No AI-specific statute	Issue SDAIA/DGA circular adopting risk-tiered AI obligations

ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Dimension	**EU AI Act**	**NIST AI RMF**	**OECD AI Principles**	**ISO/IEC 38507**	**Saudi PDPL / NDMO / DGA**	**Gap vs. Saudi**	**Quick wins (≤ 12 months)**
							pending legislation
Risk classification	Unacceptable / high / limited	Risk profiling via Map/Measure	Proportional, risk-based	Board duty	PDPL risk lens privacy-centric	No AI taxonomy	Publish Saudi AI Risk Taxonomy aligned to EU/NIST
Governance & accountability	Provider/deployer obligations; post-market monitoring	"Govern" function	Accountability principle	Board oversight	Controller duties (PDPL); DGA baseline	No AI incident duty; weak post-market norms	Mandate incident notification + AI registries
Data governance & privacy	Data quality, logging, rights protection	Data lineage, context	Human rights anchors	Conformance principle	PDPL, PDP Standards	No AI-specific DPIA	Extend DPIA templates into AI Impact Assessments with model/dataset cards
Transparency & oversight	Transparency for high-risk/GPAI; human oversight	Explainability outcomes	Transparency principle	Human behavior principle	General openness duties only	No explainability artefacts	Require public-facing model summaries for high-risk gov't AI
Lifecycle risk management	Documentation, testing, monitoring	Map–Measure–Manage	Safety and robustness	Performance oversight	Fragmented, non-AI-specific	Guidance dispersed	Issue unified AI Control Catalogue mapped to COBIT/ISO
Conformity/assurance	Conformity assessments, market surveillance	Assurance profiles	Multi-stakeholder oversight	Board assurance	Internal audit only	No conformity regime	Pilot external assurance for gov't AI using ISO 42001/23894
GPAI / foundation models	GPAI transparency & systemic risk duties	Risk-based treatment	Broad applicability	Board oversight	No GPAI guidance	Gap on GPAI disclosure	Publish GPAI Guidance (data summaries, safety tests, copyright policy)
Incident reporting	Serious incident reporting timelines	Manage function; no deadlines	Encourages ecosystems	Escalation expected	No AI incident timelines	Reporting gap	Align timelines with EU (≤ 15 days; 2–10 for critical harms)
Security & robustness	Security-by-design	Robustness monitoring	Safety principle	Conformance oversight	NCA controls, not AI-specific	No adversarial testing	Add adversarial testing & drift monitoring clauses

A Saudi AI–ITG Governance Model

Moving from thematic mapping to a practical framework, this study proposes a Saudi-specific AI IT governance (AI–ITG) model that integrates both COBIT 2019 domains and ISO/IEC 38500 principles. The model rests on clearly defined roles across the three lines of defence, beginning with board oversight through a dedicated AI and Data Ethics Committee. This committee ensures that AI initiatives align with Vision 2030 priorities and are consistent with national frameworks such as PDPL and NDMO standards. Executive leadership, particularly CIOs and CDOs, takes direct responsibility for the AI portfolio and chairs cross-functional review boards, while risk, compliance, and legal functions form the second line to approve high-risk deployments and enforce conformance. Internal audit provides the third line, delivering independent assurance over model lifecycle controls and KPI integrity.

The governance process is anchored with a catalog of controls embedded across the AI lifecycle. All projects are eligible for an AI Impact and Risk Assessment (AIRA) before deployment, with standardized model and dataset cards, robustness and fairness tests, and security-by-design validations supporting them. Go-live decisions are regulated with a formal stage-gate process and model review board, with particular review of sensitive applications via canary releases or shadow deployment. In deployment, continuous monitoring of drift, bias, and robustness is necessary with automated escalation processes and regulator alerts as needed. Regular re-validation and immutable audit records allow for transparency and accountability over time.

To measure effectiveness, the model includes a concise suite of KPIs that can be reported to the board on a quarterly basis. Benefits delivery is assessed through metrics such as an AI benefits realization index and time-to-value for new use cases. Risk optimization is captured by tracking the frequency and severity of AI incidents, residual risk scores, and robustness test results. Resource optimization is monitored through cost-per-prediction, infrastructure utilization, and model reuse ratios. Finally, conformance is gauged by coverage of AIRA and model documentation, closure times for audit findings, and PDPL or DGA compliance outcomes.

Implementation looks ahead with a multi-step roadmap. In the first six months, agencies would establish governance bodies, issue templates, and risk-tier current models in a centralized registry. In the following twelve months, monitoring platforms would be implemented, contractual clauses standardized, and preliminary thematic reviews and audit work completed. In year two, optimization activities such as portfolio rationalization, cross-agency playbooks, and external assurance would be implemented, solidifying AI governance as an auditable and measurable practice among Saudi institutions.

In this way, the proposed model translates abstract mapping into an operational artefact: it clarifies roles and accountabilities, defines auditable controls, links governance to measurable outcomes, and provides a realistic pathway for phased implementation. This contribution addresses a critical research gap by showing how Vision 2030 ambitions can be anchored in concrete governance mechanisms, thereby advancing both policy and practice in the Saudi context.

Future Directions for Policy and Practice

Building upon the identified challenges, this section outlines critical future directions for policy and practice.

Future work should pilot the proposed governance model across agencies, testing controls and KPIs under varying risk tiers. At the core of establishing a robust AI governance ecosystem in Saudi Arabia lies the development of a comprehensive national framework. This framework, integrating ethical, legal, and operational standards at every stage of AI deployment, is pivotal. It should clearly define developer and user responsibilities, mandate regular algorithm audits, and establish stringent data management and cybersecurity guidelines. Drawing from international models such as the European Union’s AI Act, while customizing regulations to Saudi Arabia’s cultural and economic context, can ensure adherence to global best practices without compromising local relevance (Jobin et al. 2019; European Commission, 2021).

Another important strategy is building a workforce that’s not only technically skilled in AI but also understands its ethical and governance dimensions. This means expanding university programs, investing in specialized research centers, and providing government-funded scholarships to develop talent in areas like data governance, machine learning, and related disciplines. Encouraging participation from women and people in underrepresented regions is crucial for unlocking more innovative and inclusive AI solutions. Their diverse perspectives can lead to breakthroughs that a homogenous workforce might overlook (Alsaeed, 2022).

Ensuring public confidence in AI-driven decisions is paramount. To achieve this, future systems should be designed with explainability at their core. The establishment of internal ethics committees or independent regulatory bodies can play a crucial role in overseeing these efforts, ensuring that AI systems remain transparent, free from bias, and aligned with societal values (Arrieta et al., 2020).

Building a resilient and inclusive AI ecosystem also requires broad-based AI literacy and a strong innovation environment. Governments can engage citizens through workshops, town halls, and educational campaigns that demystify AI concepts and illustrate real-world use cases and risks. This empowers the public to contribute feedback on policy proposals, flag emerging concerns, or co-design AI safeguards. This active participation is not just encouraged, but integral to the success of the AI governance ecosystem (Cave et al., 2019). Simultaneously, investing in national AI hubs, incubators, and collaborative research parks, especially those focused on strategic areas such as Arabic-language natural language processing (NLP), cybersecurity analytics, and smart city management, will catalyze homegrown breakthroughs. Cross-sector partnerships with international academic and industry leaders can further amplify these efforts by enabling resource sharing, joint research projects, and rapid diffusion of best practices, ensuring that AI systems reflect and serve the collective interest (Salah et al., 2022).

No AI strategy can truly succeed without a solid digital infrastructure behind it. It is not just essential but also urgent to ensure that everyone has access to fast internet, dependable cloud services, and edge computing, especially in rural and underserved areas. Key investments like nationwide 5G coverage and robust data centers need to be backed up with strong contingency plans to handle cyberattacks or system failures. This ensures that critical governance services can continue to operate without interruption (Alsharif et al., 2021).

Another key area is active engagement in international AI ethics bodies and standards-setting forums. This will position Saudi Arabia as both contributing to and benefiting from global best practices. By aligning domestic regulations with emerging international norms and participating in cross-border dialogues on data governance and digital trade, the Kingdom can strengthen its credibility and better anticipate regulatory trends that may affect its AI ecosystem (Floridi et al., 2018).

Ethical Considerations and Limitations

This study is based solely on publicly available academic, policy, and industry sources; no human participants or personal data were involved, so IRB approval was not required. Ethical issues are addressed conceptually, with attention to risks of bias, opacity, surveillance, and governance challenges for accountability and trust.

Several limitations shape the findings. Selection bias may result from reliance on indexed databases, official portals, and mainly English-language materials, with limited Arabic coverage. The evidence base is heterogeneous, combining peer-reviewed studies, standards, policy papers, and consulting reports of uneven transparency, which reduces comparability. Generalizability is limited, as many estimates, such as adoption rates and projected productivity gains, stem from single-source models or surveys and remain indicative. Lastly, the review lacks direct empirical confirmation; individual audits and longitudinal analyses are necessary for determining governance impacts in practice.

Conclusions

Artificial intelligence presents substantial opportunities to strengthen IT governance in Saudi Arabia, directly aligning with Vision 2030 ambitions. The review shows that AI can improve decision-making through predictive analytics, automate control processes for efficiency gains, reinforce cybersecurity through continuous monitoring, and increase transparency to build public trust. Yet these benefits come with clear risks such as regulatory gaps, skills shortages, uneven digital infrastructure, rising adversarial threats, and ethical concerns around bias and opacity, which require systematic governance responses.

To address these challenges, policy and practice should codify ethical principles into binding legislation, expand human capital through targeted skilling and leadership training, reduce infrastructure disparities to ensure equitable service delivery, adopt multi-layered cybersecurity tailored to AI threats, and embed explainability and oversight into every stage of the AI lifecycle. These directions are consistent with international frameworks such as the EU AI Act, NIST AI RMF, and OECD AI Principles, and can be operationalized within COBIT 2019 and ISO/IEC 38500/38507 structures.

It will be necessary to have pa hased roadmap to make progress tangible. In the near term, Saudi institutions will need to stabilize foundations with the issuance of interim risk-tiered obligations, with impact and risk assessment before deployment, and with registries of high-risk AI systems and incident reporting processes. In the medium term, there will need to be a focus on measurement and assurance: cataloguing control standardization, implementing explainability and transparency requirements, and experimenting with external audit of government AI deployments. In the longer term, optimization will include rationalizing AI portfolios across agencies, establishing guidance for foundation models, and increasing external conformity assessment as part of budget and performance rounds. Staging here leaves space for initial "quick wins" as well as long-term institutionalization.

Progress must also be tracked through clear, auditable indicators. Relevant benchmarks include the percentage of AI projects covered by risk assessments, the completeness of registries for high-risk models, timeliness of incident reporting, the proportion of systems subject to adversarial testing and bias audits, and the coverage of explainability measures in high-impact deployments. These KPIs, aligned with COBIT's monitoring objectives and ISO's conformance principles, allow boards and regulators to measure maturity rather than ambition, and to adjust policy accordingly.

By embedding this phased and measurable approach, Saudi Arabia can not only safeguard trust and accountability but also demonstrate global leadership in responsible AI governance. The combination of binding rules, capacity-building, infrastructural support, adaptive cybersecurity, and transparent oversight provides a comprehensive pathway to realizing AI's potential responsibly and sustainably.

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. Abdallah, R., Alshumayri, S., & Bukassim, L. (2025). Automated Motawif Monitoring Hajjis through the Pilgrimage Period. Proceedings of the 22nd International Conference on Computer and Information Technology. IEEE Link
2. Abu Musa, A. (2009). Exploring COBIT Processes for ITG in Saudi Organizations An empirical Study. The International Journal of Digital Accounting Research. https://doi.org/10.4192/1577-8517-v9_4
3. Accenture. (2025). Saudi Arabia transforms with data and AI. Accenture. https://www.accenture.com/us-en/case-studies/artificial-intelligence/reimagining-saudi-arabia-economy
4. Al-Baity, H. H. (2023). The Artificial Intelligence Revolution in Digital Finance in Saudi Arabia: A Comprehensive Review and Proposed Framework. Sustainability, 15(18), 13725. https://doi.org/10.3390/su151813725
5. Aljijakli, M., & Akkari, N. (2025). Toward AI-Driven Solutions for Smart Cities in KSA. 2025 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC), 1–6. https://doi.org/10.1109/icaisc64594.2025.10959599
6. Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. International Journal of Advanced Computer Science and Applications, 12(3). https://doi.org/10.14569/ijacsa.2021.0120334
7. Almaawi, A., Alsaggaf, L., & Fasihuddin, H. (2020). The Application of IT Governance Frameworks in Saudi Arabia: An Exploratory Study. International Journal of Computer Applications, 176(30), 40–44. https://doi.org/10.5120/ijca2020920351

8. Almaqtari, F. A. (2024). The Role of IT Governance in the Integration of AI in Accounting and Auditing Operations. Economies, 12(8), 199. https://doi.org/10.3390/economies12080199
9. Alotaibi, N. S., & Alshehri, A. H. (2023). Prospers and Obstacles in Using Artificial Intelligence in Saudi Arabia Higher Education Institutions - The Potential of AI-Based Learning Outcomes. Sustainability, 15(13), 10723. https://doi.org/10.3390/su151310723
10. Alqahtani, F., Alshehri, A., Mulyata, J., & Cranfield, D. (2024). Assessing the Potential Effects of Disruptive Technologies on Business Models: A Case of Saudi Arabia. Open Journal of Business and Management, 12(05), 3417–3445. https://doi.org/10.4236/ojbm.2024.125171
11. AlQahtani, M. S. (2023). Artificial intelligence and its influence on digital transformation, development, and productivity in Saudi Arabian organizations: A critical evaluation. EKB Journal Management System. Advance online publication. https://doi.org/10.21608/aja.2023.233880.1518
12. Alsaeed, K. (2022). Building an AI Workforce in Saudi Arabia: Challenges and Prospects. International Journal of Computer Applications, 184(47), 15–23. https://doi.org/10.5120/ijca2022922028
13. Alshahrani, A., Dennehy, D., & Mäntymäki, M. (2022). An attention-based view of AI assimilation in public sector organizations: The case of Saudi Arabia. Government Information Quarterly, 39(4), 101617. https://doi.org/10.1016/j.giq.2021.101617
14. Alsharif, M. H., Al-Samman, A. M., & Alzahrani, B. (2021). Future 5G Technologies in Saudi Arabia: Challenges and Opportunities. IEEE Access, 9, 10459–10471. https://doi.org/10.1109/ACCESS.2021.3050301
15. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012
16. Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. Machine Learning, 81(2), 121–148. https://doi.org/10.1007/s10994-010-5188-5
17. Calder, A. (2008). ISO/IEC 38500: the IT governance standard. IT Governance Ltd.
18. Cave, S., Coughlan, K., & Dihal, K. (2019). Scary Robots: Examining Public Responses to AI. Paladyn, Journal of Behavioral Robotics, 10(1), 291–301. https://doi.org/10.1515/pjbr-2019-0020

19. Digital Government Authority. (2024). Emerging Technologies Adoption Readiness in Government Agencies [Review of Emerging Technologies Adoption Readiness in Government Agencies]. In https://dga.gov.sa/. Digital Government Authority. https://dga.gov.sa/sites/default/files/202407/Emerging%20Technologies%20Adoption%20Readiness%20in%20Government%20Agencies%202024.V2.1.pdf
20. Digital Government Authority. (2025). Generative AI in Digital Government [Review of Generative AI in Digital Government]. In DGA.GOV.SA. Digital Government Authority. https://dga.gov.sa/sites/default/files/2025-06/Generative%20AI%20in%C2%A0Digital%20Government-V1.0.pdf
21. Elhajji, M., Alsayyari, A. S., & Alblawi, A. (2020). Towards an artificial intelligence strategy for higher education in Saudi Arabia. 2020 3rd International Conference on Computer Applications &amp; Information Security (ICCAIS), 1–7. https://doi.org/10.1109/iccais48893.2020.9096833
22. European Commission. (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
23. Farraj, A. A. (2024). How AI Enhances Justice Administration: Comparative Analysis Between Egypt and Saudi Arabia. Journal of Sharia and Law, Tanta University. Link
24. Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A. L., & Kohane, I. S. (2019). Adversarial attacks on medical machine learning. Science, 363(6433), 1287–1289. https://doi.org/10.1126/science.aaw4399
25. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People - An Ethical Framework for a Good AI Society. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
26. Ibrahim, N. M. H. (2024). Artificial intelligence (AI) and Saudi Arabia’s governance. Journal of Developing Societies, 40(4), 500–530. https://doi.org/10.1177/0169796X241288590
27. ISO/IEC 38507:2022. (2022). ISO. https://www.iso.org/standard/56641.html
28. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

29. Kumar, R., Singh, A., Kassar, A. S. A., Humaida, M. I., Joshi, S., & Sharma, M. (2025). Leveraging Artificial Intelligence to Achieve Sustainable Public Healthcare Services in Saudi Arabia: A Systematic Literature Review of Critical Success Factors. Computer Modeling in Engineering &amp; Sciences, 142(2), 1289–1349. https://doi.org/10.32604/cmes.2025.059152
30. Memish, Z. A., Altuwaijri, M. M., Almoeen, A. H., & Enani, S. M. (2021). The Saudi Data &amp; Artificial Intelligence Authority (SDAIA) Vision: Leading the Kingdom's Journey toward Global Leadership. Journal of Epidemiology and Global Health, 11(2), 140. https://doi.org/10.2991/jegh.k.210405.001
31. Muafa, A., Al-Obadi, S., Al-Saleem, N., Taweili, A., & Al-Amri, A. (2024). The Impact of Artificial Intelligence Applications on the Digital Transformation of Healthcare Delivery in Riyadh, Saudi Arabia (Opportunities and Challenges in Alignment with Vision 2030). Academic Journal of Research and Scientific Publishing, 5(59), 61–102. https://doi.org/10.52132/ajrsp.e.2024.59.4
32. National Institute of Standards and Technology. (2023). AI Risk Management Framework (AI RMF 1.0). NIST. https://doi.org/10.6028/NIST.AI.100-1
33. Organization for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence. OECD. https://oecd.ai/en/ai-principles
34. Polok, B., & Dussin, M. (2025). AI governance in Saudi Arabia: Cultural values and ethical AI regulations in comparative perspective. Yearbook of Islamic and Middle Eastern Law Online, 1–29. https://doi.org/10.1163/22112987-bja00004
35. Saeed, A., Bin Saeed, A., & AlAhmri, F. A. (2023). Saudi Arabia Health Systems Challenging and Future Transformation With Artificial Intelligence. Cureus. https://doi.org/10.7759/cureus.37826
36. Salah, K., Rehman, M. H., Nizamuddin, N., & Al-Fuqaha, A. (2022). Blockchain for AI: Review and Open Research Challenges. IEEE Access, 10, 106783–106800. https://doi.org/10.1109/ACCESS.2022.3195698
37. Zeng, Y., Lu, E., & Huangfu, C. (2021). Linking artificial intelligence principles. arXiv preprint arXiv:1812.04814. https://doi.org/10.48550/arXiv.1812.04814

Appendix A. PRISMA 2020 flow

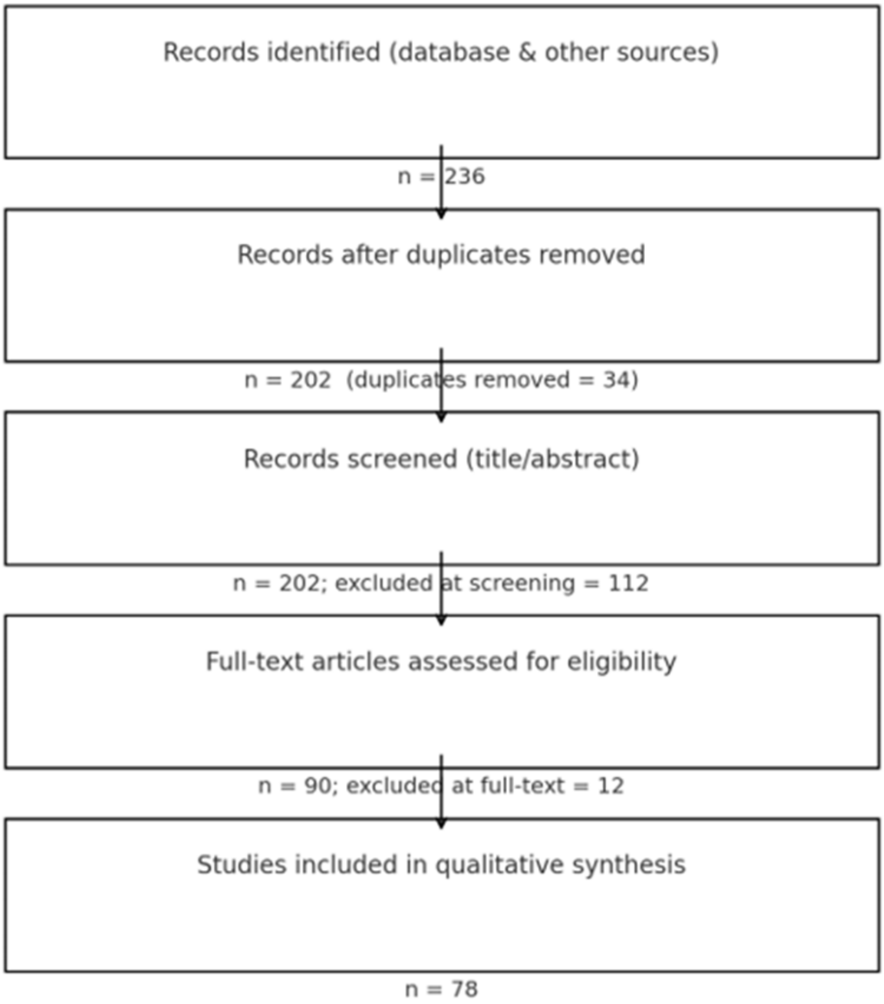
Records identified (database & other sources)
n = 236
Records after duplicates removed
n = 202 (duplicates removed = 34)
Records screened (title/abstract)
n = 202; excluded at screening = 112
Full-text articles assessed for eligibility
n = 90; excluded at full-text = 12
Studies included in qualitative synthesis
n = 78

Figure A1: PRISMA Flow

Appendix B. Full search strings and collection log

Databases: Scopus; Web of Science.
Scholarly search: Google Scholar.
Grey literature portals: ISACA/COBIT; ISO; NIST; OECD; DGA; SDAIA; MCIT.
Languages: English, Arabic.
Date range: 2008–2025.
Last search update: August 28, 2025.

Scopus (TITLE-ABS-KEY):
("artificial intelligence" OR "AI" OR "machine learning" OR "generative AI")
AND ("IT governance" OR "information technology governance" OR COBIT OR "ISO/IEC 38500" OR "38507" OR "NIST AI RMF")
AND ("Saudi Arabia" OR Saudi OR KSA OR "Vision 2030" OR السعودية OR "رؤية 2030")
AND (PUBYEAR > 2007 AND PUBYEAR < 2026)
Web of Science (TS=):
(("artificial intelligence" OR AI OR "machine learning" OR "generative AI")
AND ("IT governance" OR "information technology governance" OR COBIT OR "ISO/IEC 38500" OR 38507 OR "risk management framework")
AND ("Saudi Arabia" OR KSA OR "Vision 2030" OR السعودية))
Timespan: 2008–2025; Indexes: SCI-EXPANDED, SSCI, A&HCI, ESCI
Google Scholar (2008–2025; first 200 results per query):

- "IT governance" (COBIT OR "ISO/IEC 38500" OR 38507) "Saudi Arabia"
- "AI governance" Saudi OR KSA "Vision 2030"
- "generative AI" governance Saudi

Illustrative collection log

- 2025-08-28 10:20: Scopus export (CSV), 94 hits; de-duplicated downstream.
- 2025-08-28 11:05: Web of Science export (CSV), 71 hits.
- 2025-08-28 12:40: Google Scholar screening (first 200 per query), retained 48.
- 2025-08-28 14:00: Grey portals batch download, 23 documents (policy/standards).

Appendix C. Codebook and reliability

Deductive domains (COBIT 2019 & ISO/IEC 38500):

- **COBIT 2019:** EDM (Evaluate, Direct, Monitor); APO (Align, Plan, Organize); BAI (Build, Acquire, Implement); DSS (Deliver, Service, Support); MEA (Monitor, Evaluate, Assess).
- **ISO/IEC 38500 principles:** Responsibility; Strategy; Acquisition; Performance; Conformance; Human Behaviour.

Illustrative inductive sub-themes (Saudi context):

- Vision 2030 execution, national digital strategies, sector programs
- PDPL compliance and data governance (NDMO)
- DGA digital government controls and assessment models
- SDAIA platforms and enablers for AI adoption

- Compliance automation, model risk management, explainability/traceability
- Bias testing, safety evaluation, adversarial robustness
- Workforce capability, skilling, and change management

Inter-coder agreement (20% double-coded):

- κ (top-level domains): 0.84
- Median κ (sub-themes): 0.80 (IQR 0.77–0.86; range 0.74–0.88)

Appendix D. Quality appraisal (MMAT + AAC) and sensitivity

Overall tiers (n = 78): High = 29; Moderate = 38; Low = 11.
By source type (counts, High/Moderate/Low):

- Scholarly/empirical (peer-reviewed): 47 → 18 / 24 / 5
- Policy/grey literature: 31 → 11 / 14 / 6

Sensitivity check: Re-synthesizing without Low-tier items did not change the direction of findings; emphasis on leadership attention, capability building, and compliance alignment (EDM/APO/MEA) remained.

Appendix E. Included records

1. Abdallah, R., Alshumayri, S., & Bukassim, L. (2025). Automated Motawif Monitoring Hajjis through the Pilgrimage Period. Proceedings of the 22nd International Conference on Computer and Information Technology. IEEE
2. Abu Musa, A. (2009). Exploring COBIT Processes for ITG in Saudi Organizations An empirical Study. The International Journal of Digital Accounting Research. https://doi.org/10.4192/1577-8517-v9_4
3. Accenture. (2025). Saudi Arabia transforms with data and AI. Accenture. https://www.accenture.com/us-en/case-studies/artificial-intelligence/reimagining-saudi-arabia-economy
4. Al-Baity, H. H. (2023). The Artificial Intelligence Revolution in Digital Finance in Saudi Arabia: A Comprehensive Review and Proposed Framework. Sustainability, 15(18), 13725. https://doi.org/10.3390/su151813725
5. Aljijakli, M., & Akkari, N. (2025). Toward AI-Driven Solutions for Smart Cities in KSA. 2025 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC), 1â€“6. https://doi.org/10.1109/icaisc64594.2025.10959599
6. Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. International Journal of Advanced Computer Science and Applications, 12(3). https://doi.org/10.14569/ijacsa.2021.0120334

7. Almaawi, A., Alsaggaf, L., & Fasihuddin, H. (2020). The Application of IT Governance Frameworks in Saudi Arabia: An Exploratory Study. International Journal of Computer Applications, 176(30), 40â€“44. https://doi.org/10.5120/ijca2020920351
8. Almaqtari, F. A. (2024). The Role of IT Governance in the Integration of AI in Accounting and Auditing Operations. Economies, 12(8), 199. https://doi.org/10.3390/economies12080199
9. Alotaibi, N. S., & Alshehri, A. H. (2023). Prospers and Obstacles in Using Artificial Intelligence in Saudi Arabia Higher Education Institutionsâ€"The Potential of AI-Based Learning Outcomes. Sustainability, 15(13), 10723. https://doi.org/10.3390/su151310723
10. Alqahtani, F., Alshehri, A., Mulyata, J., & Cranfield, D. (2024). Assessing the Potential Effects of Disruptive Technologies on Business Models: A Case of Saudi Arabia. Open Journal of Business and Management, 12(05), 3417â€“3445. https://doi.org/10.4236/ojbm.2024.125171
11. AlQahtani, M. S. (2023). Artificial intelligence and its influence on digital transformation, development, and productivity in Saudi Arabian organizations: A critical evaluation. EKB Journal Management System. Advance online publication. https://doi.org/10.21608/aja.2023.233880.1518
12. Alsaeed, K. (2022). Building an AI Workforce in Saudi Arabia: Challenges and Prospects. International Journal of Computer Applications, 184(47), 15â€“23. https://doi.org/10.5120/ijca2022922028
13. Alshahrani, A., Dennehy, D., & MÃ¤ntymÃ¤ki, M. (2022). An attention-based view of AI assimilation in public sector organizations: The case of Saudi Arabia. Government Information Quarterly, 39(4), 101617. https://doi.org/10.1016/j.giq.2021.101617
14. Alsharif, M. H., Al-Samman, A. M., & Alzahrani, B. (2021). Future 5G Technologies in Saudi Arabia: Challenges and Opportunities. IEEE Access, 9, 10459â€“10471. https://doi.org/10.1109/ACCESS.2021.3050301
15. Arrieta, A. B., DÃaz-RodrÃguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82â€“115. https://doi.org/10.1016/j.inffus.2019.12.012
16. Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. Machine Learning, 81(2), 121â€“148. https://doi.org/10.1007/s10994-010-5188-5

17. Calder, A. (2008). ISO/IEC 38500: the IT governance standard. IT Governance Ltd.
18. Cave, S., Coughlan, K., & Dihal, K. (2019). Scary Robots: Examining Public Responses to AI. Paladyn, Journal of Behavioral Robotics, 10(1), 291â€“301. https://doi.org/10.1515/pjbr-2019-0020
19. Digital Government Authority. (2024). Emerging Technologies Adoption Readiness in Government Agencies [Review of Emerging Technologies Adoption Readiness in Government Agencies]. In https://dga.gov.sa/. Digital Government Authority. https://dga.gov.sa/sites/default/files/202407/Emerging%20Technologies%20Adoption%20Readiness%20in%20Government%20Agencies%202024.V2.1.pdf
20. Digital Government Authority. (2025). Generative AI in Digital Government [Review of Generative AI in Digital Government]. In DGA.GOV.SA. Digital Government Authority. https://dga.gov.sa/sites/default/files/2025-06/Generative%20AI%20in%C2%A0Digital%20Government-V1.0.pdf
21. Elhajji, M., Alsayyari, A. S., & Alblawi, A. (2020). Towards an artificial intelligence strategy for higher education in Saudi Arabia. 2020 3rd International Conference on Computer Applications &amp; Information Security (ICCAIS), 1â€“7. https://doi.org/10.1109/iccais48893.2020.9096833
22. European Commission. (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
23. Farraj, A. A. (2024). How AI Enhances Justice Administration: Comparative Analysis Between Egypt and Saudi Arabia. Journal of Sharia and Law, Tanta University.
24. Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A. L., & Kohane, I. S. (2019). Adversarial attacks on medical machine learning. Science, 363(6433), 1287â€“1289. https://doi.org/10.1126/science.aaw4399
25. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4Peopleâ€”An Ethical Framework for a Good AI Society. Minds and Machines, 28(4), 689â€“707. https://doi.org/10.1007/s11023-018-9482-5
26. Ibrahim, N. M. H. (2024). Artificial intelligence (AI) and Saudi Arabiaâ€™s governance. Journal of Developing Societies, 40(4), 500â€“530. https://doi.org/10.1177/0169796X241288590

27. ISO/IEC 38507:2022. (2022). ISO. https://www.iso.org/standard/56641.html
28. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389â€“399. https://doi.org/10.1038/s42256-019-0088-2
29. Kumar, R., Singh, A., Kassar, A. S. A., Humaida, M. I., Joshi, S., & Sharma, M. (2025). Leveraging Artificial Intelligence to Achieve Sustainable Public Healthcare Services in Saudi Arabia: A Systematic Literature Review of Critical Success Factors. Computer Modeling in Engineering &amp; Sciences, 142(2), 1289â€“1349. https://doi.org/10.32604/cmes.2025.059152
30. Memish, Z. A., Altuwaijri, M. M., Almoeen, A. H., & Enani, S. M. (2021). The Saudi Data &amp; Artificial Intelligence Authority (SDAIA) Vision: Leading the Kingdomâ€™s Journey toward Global Leadership. Journal of Epidemiology and Global Health, 11(2), 140. https://doi.org/10.2991/jegh.k.210405.001
31. Muafa, A., Al-Obadi, S., Al-Saleem, N., Taweili, A., & Al-Amri, A. (2024). The Impact of Artificial Intelligence Applications on the Digital Transformation of Healthcare Delivery in Riyadh, Saudi Arabia (Opportunities and Challenges in Alignment with Vision 2030). Academic Journal of Research and Scientific Publishing, 5(59), 61â€“102. https://doi.org/10.52132/ajrsp.e.2024.59.4
32. National Institute of Standards and Technology. (2023). AI Risk Management Framework (AI RMF 1.0). NIST. https://doi.org/10.6028/NIST.AI.100-1
33. Organization for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence. OECD. https://oecd.ai/en/ai-principles
34. Polok, B., & Dussin, M. (2025). AI governance in Saudi Arabia: Cultural values and ethical AI regulations in comparative perspective. Yearbook of Islamic and Middle Eastern Law Online, 1â€“29. https://doi.org/10.1163/22112987-bja00004
35. Saeed, A., Bin Saeed, A., & AlAhmri, F. A. (2023). Saudi Arabia Health Systems Challenging and Future Transformation With Artificial Intelligence. Cureus. https://doi.org/10.7759/cureus.37826
36. Salah, K., Rehman, M. H., Nizamuddin, N., & Al-Fuqaha, A. (2022). Blockchain for AI: Review and Open Research Challenges. IEEE Access, 10, 106783â€“106800. https://doi.org/10.1109/ACCESS.2022.3195698
37. Zeng, Y., Lu, E., & Huangfu, C. (2021). Linking artificial intelligence principles. arXiv preprint arXiv:1812.04814. https://doi.org/10.48550/arXiv.1812.04814

38. Saudi Data & AI Authority (SDAIA). (2020). National Strategy for Data & AI (NSDAI). Riyadh: SDAIA.
39. Kingdom of Saudi Arabia. (2023). Personal Data Protection Law (PDPL) (English translation). Riyadh: SDAIA.
40. SDAIA. (2023). Implementing Regulations of the Personal Data Protection Law. Riyadh: SDAIA.
41. National Data Management Office (NDMO). (2021). Data Management and Personal Data Protection Standards (v1.5). Riyadh: SDAIA/NDMO.
42. NDMO. (2020). National Data Governance Interim Regulations (including Data Classification, Data Sharing, FOI and Open Data). Riyadh: SDAIA/NDMO.
43. NDMO. (2020). Data Classification Policy. Riyadh: SDAIA/NDMO.
44. Digital Government Authority (DGA). (2022). Digital Government Regulatory Framework (v1.0). Riyadh: DGA.
45. Digital Government Authority (DGA). (2023). Digital Government Regulatory Framework (v2.0). Riyadh: DGA.
46. Digital Government Authority (DGA). (2024). Digital Government Policies (v2.0). Riyadh: DGA.
47. Digital Government Authority (DGA). (2022). Digital Government Policy. Riyadh: DGA.
48. Digital Government Authority (DGA). (2025). Generative AI in Digital Government (v1.0). Riyadh: DGA.
49. Ministry of Health (MoH). (2025). Data Governance Policy. Riyadh: MoH.
50. Saudi Central Bank (SAMA). (2017). Cyber Security Framework. Riyadh: SAMA.
51. National Cybersecurity Authority (NCA). (2022). Operational Technology Cybersecurity Controls (OTCC-1:2022). Riyadh: NCA.
52. National Cybersecurity Authority (NCA). (2025). Guide to Essential Cybersecurity Controls (ECC) Implementation. Riyadh: NCA.
53. Communications, Space & Technology Commission (CST). (2023). Cloud Computing Regulatory Framework (v3). Riyadh: CST.
54. Ministry of Communications and Information Technology (MCIT). (2019). Cloud First Policy. Riyadh: MCIT.
55. NDMO. (2020). Open Data Policy. Riyadh: SDAIA/NDMO.
56. NDMO. (2020). Freedom of Information Policy. Riyadh: SDAIA/NDMO.
57. NDMO. (2020). Data Sharing Policy. Riyadh: SDAIA/NDMO.
58. NDMO. (2025). General Rules for Secondary Use of Data. Riyadh: SDAIA/NDMO.

59. ISO/IEC. (2015). ISO/IEC 38500:2015â€"Governance of IT for the organization. Geneva: ISO/IEC.
60. ISO/IEC. (2022). ISO/IEC 38507:2022â€"Governance implications of the use of AI by organizations. Geneva: ISO/IEC.
61. ISO/IEC. (2023). ISO/IEC 23894:2023â€"Artificial intelligenceâ€"Guidance on risk management. Geneva: ISO/IEC.
62. ISO/IEC. (2023). ISO/IEC 42001:2023â€"Artificial intelligence management system (AIMS) requirements. Geneva: ISO/IEC.
63. NIST. (2023). AI Risk Management Framework 1.0 (NIST AI 100-1). Gaithersburg, MD: NIST.
64. OECD. (2019). OECD Principles on Artificial Intelligence. Paris: OECD.
65. Alshahrani, A., Dennehy, D., & MÃ¤ntymÃ¤ki, M. (2021). An attention-based view of AI assimilation in public sector organizations: The case of Saudi Arabia. Government Information Quarterly, 39(4), 101617.
66. Almaawi, A., Alsaggaf, L., & Fasihuddin, H. (2020). The Application of IT Governance Frameworks in Saudi Arabia: An Exploratory Study. International Journal of Computer Applications, 176(30), 40â€"44.
67. Fasihuddin, H., Alharbi, N., Alshehri, A., Alzahrani, B., & Fatani, A. (2022). Measuring the maturity of information technology governance based on COBIT in Saudi Arabia. Romanian Journal of Information Technology and Automatic Control, 32(2), 57â€"68.
68. Aljarallah, S., & Lock, R. (2020). An Investigation into Sustainable e-Government in Saudi Arabia. Electronic Journal of e-Government, 18(1), 1â€"13.
69. Alaqla, M. F. (2023). The impact of IT governance and administrative information quality on decision-making in Saudi banking. Corporate Governance and Organizational Behavior Review, 7(4), 228â€"241.
70. Hashim, H. (2024). E-government and smart cities in Saudi Arabia: Influencing factors and implications. Ain Shams Engineering Journal, 15(??), Article 102381.
71. Hakeem, M. M. M. (2024). Evaluation of E-governance Implementation: A Multi-attribute Decision Model for Hajj Services in Saudi Arabia (Doctoral dissertation). Long Island University.
72. Alreemy, Z. (2016). A Framework for Successful IT Governance Implementation in the Saudi Public Sector (Doctoral thesis). University of Southampton.
73. Abu-Musa, A. A. (2009). Exploring IT Governance (COBIT) processes in Saudi organizations. International Journal of Digital Accounting Research, 9, 99â€"126.

74. Alharbi, Z. H., & colleagues. (2022). Exploring Areas of Improvement in IT Innovation Management in the Saudi Healthcare Sector Using COBIT 2019. SAR Journal, March 2022, 18â€“28.
75. Alnifayei, H. (2021). A review of the current status of e-government in Saudi Arabia. Journal for Research on Business and Social Science, 4(11), 1â€“12.
76. Al-Khalifa, H., Mashaabi, M., Al-Yahya, G., & Alnashwan, R. (2023). The Saudi Privacy Policy Dataset (arXiv:2304.02757).
77. ISACA. (2020). COBIT Case Study: Saudi Bank aligns compliance and governance using COBIT. Rolling Meadows, IL: ISACA.
78. Digital Government Authority (DGA). (2025). Digital Government Legislation (overview). National Platform for Government Services (my.gov.sa).