International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI Strategy as a National Priority: A Governance-to-Execution Framework for Saudi Arabia Led by SDAIA (2020–2026 Evidence)

Sreeraj Cherukat

Research Scholar, Ph.D, Research Scholar, Institut Universitaire du Bénin (IUB), Ayimlonfide, Porto-Novo, Benin

Abstract

Saudi Arabia has made AI a national priority aligned with Vision 2030. Strategic leadership and orchestration have been delivered by the Saudi Data & AI Authority (SDAIA) and the National Strategy for Data and AI (NSDAI). Few studies, however, operationalize how national objectives are translated into quantifiable execution across ministries, regulated sectors, and data ecosystems. Based on this, a proposed governance-to-execution framework in the Saudi context would be helpful because there is a need to integrate concepts such as (i) strategic alignment, (ii) national data governance, (iii) responsible AI controls, (iv) capability building, and (v) sector deployment pathways. This paper is developed through the execution of a structured synthesis of recent scholarship on national AI strategies and AI governance and Saudi policy artifacts that describe the NSDAI's KPI orientation and SDAIA's coordinating mandate. The paper contributes on three dimensions: a unique, testable set of objectives for the national level execution of AI, over and above generic claims of "innovation;" a KPI logic model linking policy instruments to adoption outcomes; and a risk-control matrix for ethical, legal, and operational governance of national AI. The findings stress that national AI success depends not only on funding and infrastructure but also on enforceable

Keywords: Saudi Arabia, SDAIA, NSDAI, national AI strategy, AI governance, responsible AI, data governance, Vision 2030

1. Introduction

Since 2020, national artificial intelligence strategies have shifted from aspirational declarations to instruments that must withstand scrutiny during delivery. Early waves of strategy writing focused on ethics, research funding, and competitiveness, but recent comparative work highlights the "execution gap" between commitments and tangible outcomes such as interoperable datasets, scaled deployments, and audit-ready governance (Radu, 2021; Fatima, 2022). This gap is particularly visible in the public sector, where AI adoption is constrained by legacy systems, procurement rules, and heightened accountability to citizens and regulators (Almeida & dos Santos Júnior, 2025; Chen, 2023). In this context, national AI success is less about whether a country can announce goals, and more about whether it can convert goals into coordinated delivery across ministries and sectors, while sustaining trust and managing high-impact risks.

Saudi Arabia's policy stance frames AI as a central lever for economic diversification, public-service modernization, and global competitiveness under Vision 2030. Within the Saudi ecosystem, SDAIA is frequently described as the central orchestrator that coordinates data and AI governance, sets strategic direction, and supports national execution through guidance, platforms, and measurement (Memish et al., 2021). The NSDAI similarly signals an ambition to scale adoption in government and priority industries, alongside a KPI-oriented approach to monitoring progress. However, academic and practitioner discourse still needs a clearer mapping from "national priority" to enforceable execution: what operational objectives matter, how they are measured, and how governance is translated into delivery mechanics and assurance routines.

This paper addresses that need by proposing a Saudi-fit governance-to-execution framework grounded in 2020–2026 evidence. The framework positions national execution as a chain of capabilities that starts with data stewardship and policy alignment, moves through responsible AI lifecycle controls and delivery pipelines, and is sustained by assurance mechanisms such as auditing and continuous monitoring (Akbarighatar, 2024; Papagiannidis et al., 2025; Mökander et al., 2024). Importantly, it treats public values—equity, transparency, accountability, and legitimacy—not as optional add-ons, but as measurable outcomes that must be tracked alongside service efficiency and economic value (Chen, 2023; Mišić et al., 2025).

2. Review of Literature

2.1 National AI strategies and the execution gap

National AI strategies are often studied as policy signals that aim to attract investment, mobilize research communities, and communicate intent to citizens and partners. Yet cross-country assessments show recurring weaknesses: unclear ownership across ministries, limited guidance for implementation, and measurement systems that focus on inputs rather than adoption outcomes (Radu, 2021; OECD, 2021). In Telecommunications Policy, Fatima (2022) argues that interpreting national plans requires attention to how ambitions are translated into mechanisms such as standards, incentives, and governance structures. Where these mechanisms are absent, strategies risk becoming rhetorical rather than operational.

A public-sector lens sharpens this critique. Strategies that frame AI mainly as an efficiency tool may underweight citizen participation, democratic values, and legitimacy. Government Information Quarterly research on public values and strategy discourse suggests that the framing of AI affects what governments prioritize in their measurement systems and governance models (Hjaltalin & Sigurdarson, 2024). Therefore, the execution gap is not only technical; it is also a governance and legitimacy gap. A national strategy can scale AI technically while still failing to scale legitimacy if transparency and accountability are weak. For Saudi Arabia, which seeks rapid modernization while sustaining trust, this implies that execution frameworks must contain explicit public-value outcomes and evidence-based assurance.

2.2 AI governance: from principles to capabilities

Across 2020–2026 scholarship, AI governance increasingly shifts from high-level principles toward capability-based operating models. Systematic reviews describe governance as spanning structural elements (institutions, roles, and policies), relational elements (stakeholder engagement, accountability relationships), and procedural elements (processes, documentation, monitoring, and audits) (Papagiannidis et al., 2025). This multi-level perspective is critical for national governance because AI systems are created and used within organizations, but are also shaped by national laws, strategies, and

shared platforms. National frameworks must therefore connect these levels rather than assuming that organizational ethics statements will automatically deliver consistent outcomes. Operationalizing responsible AI is now treated as an engineering, management, and compliance challenge rather than an abstract ethics debate. Akbarighatar (2024) explicitly argues for "responsible AI capabilities," suggesting that governance must be expressed through concrete practices such as risk classification, validation, documentation, monitoring, and incident management. Batool et al. (2025) reinforce this view by mapping governance mechanisms across policy, organizational, and technical domains, highlighting that practical controls are required to reduce harms and to make oversight feasible. These findings motivate the paper's emphasis on evidence artifacts: model registries, validation reports, monitoring dashboards, and incident logs are not optional paperwork, but the operational backbone of accountable AI.

2.3 Public sector AI governance: implementation realities

Public organizations face distinctive constraints that affect AI governance and delivery. Empirical research shows that public agencies must navigate procurement rules, budget cycles, human resource constraints, and compliance obligations, while managing reputational and legal risk from automated decisions (Almeida & dos Santos Júnior, 2025). These realities influence the feasibility of "rapid experimentation" models often celebrated in private-sector AI narratives. As a result, governance-to-execution frameworks must incorporate delivery mechanics that work under public constraints, such as stage gates, portfolio oversight, and standardized evidence requirements that allow reuse and reduce reinvention across agencies.

Public values research provides an additional layer. Chen (2023) emphasizes that AI in government can affect transparency, accountability, equity, and autonomy, and that governance should track these impacts rather than treating them as purely normative ideals. Mišić et al. (2025) propose a combined value framework for "good order" (rule-following, predictability, accountability) and "a good society" (justice, inclusion, legitimacy). For national strategy execution, these perspectives imply that value realization must be defined broadly: service improvements are necessary but insufficient if fairness is compromised or if citizens cannot contest decisions. A national KPI system that ignores these dimensions may over-report success while under-detecting trust erosion.

2.4 AI auditing and assurance as national-scale instruments

As regulatory attention grows, auditing is emerging as a central mechanism to translate principles into enforceable practice. Kamphorst (2025) discusses AI auditing through performance appraisal lenses, emphasizing that audits can become routine governance tools that assess systems over time rather than one-time compliance checks. Mökander et al. (2024) focus on access and evidence: what information auditors need, what documentation should exist, and how evidence must be organized to make audits meaningful. These contributions underline a key challenge for national execution: without defined evidence access requirements, auditing remains superficial, and risk management becomes reactive.

Auditing research also links to broader governance regimes. Schmitt (2022) describes global AI governance as fragmented and nascent, suggesting that national frameworks must be resilient to evolving standards and regulatory expectations. Camilleri (2024) highlights ethical and regulatory perspectives, reinforcing that national execution requires alignment with emerging norms and the ability to update controls as standards mature. In practice, this means building adaptable assurance infrastructure: evidence standards should be stable enough for consistency, but flexible enough to accommodate new regulations, new model types, and new risks.

2.5 Data governance maturity as a prerequisite for AI execution

Data governance scholarship expands rapidly after 2020, with systematic reviews and mapping studies emphasizing maturity models, stewardship practices, and quality management as enablers of analytics and AI (Bernardo et al., 2024; Bližnák et al., 2024; Hassani et al., 2025). These works converge on a practical point: AI deployment at scale requires discoverable, well-documented, high-quality datasets with clear ownership, lineage, and access controls. Without this foundation, AI programs often devolve into repeated data wrangling and localized fixes. This "hidden tax" slows delivery, increases cost, and raises risk, because teams cannot reliably reproduce results or validate models against consistent data baselines.

Documentation standards such as datasheets for datasets provide an accountability instrument. Gebru et al. (2021) propose dataset documentation that clarifies intended use, collection methods, and limitations, supporting transparency and risk management. In national contexts, dataset documentation can also enable cross-entity reuse by making dataset suitability and constraints explicit, reducing duplication and increasing consistency in how data risks are assessed. Therefore, data governance is not just a technical prerequisite; it is a governance mechanism that supports auditability, interoperability, and responsible deployment.

3. Methodology

This paper uses a structured synthesis approach designed for policy-to-practice research in complex public ecosystems. The method prioritizes integration over narrow hypothesis testing, consistent with literature review approaches used to propose governance frameworks and implementation models (Batool et al., 2025; Almeida & dos Santos Júnior, 2025). The steps are:

1. Identification: select 2020–2026 peer-reviewed studies on national AI strategies, AI governance, public sector AI adoption, AI auditing, and data governance maturity, including works that propose conceptual models and empirical findings.
2. Coding: code findings into categories that map to national execution needs: governance structures, lifecycle controls, measurement systems, delivery pipelines, capability building, and public-value outcomes.
3. Synthesis: integrate categories into a governance-to-execution framework that links policy instruments to operational processes and evidence artifacts.
4. Derivation: derive operational objectives and example indicators that are measurable, auditable, and aligned with the implementation realities found in the literature.

How can a national AI strategy be translated into measurable, responsible, cross-sector execution—linking governance, delivery, and assurance—under centralized strategic leadership (2020–2026 evidence)?

Contributions and unique operational objectives

Unlike many strategy papers that emphasize general adoption, this paper proposes five operational national objectives that are measurable and auditable:

1. Interoperable Data Readiness: prioritize data cataloging, lineage, and quality measurement across entities, enabling cross-agency use and reuse (Bernardo et al., 2024; Bližnák et al., 2024).
2. Lifecycle Responsible-AI Assurance: enforce risk tiering, documentation, monitoring, and incident response for high-impact systems (Akbarighatar, 2024; Papagiannidis et al., 2025).

3. Sector Delivery Pipelines: increase pilot-to-scale conversion rates and reduce time-to-scale using standardized intake, stage gates, and portfolio governance (Almeida & dos Santos Júnior, 2025; Hjaltalin & Sigurdarson, 2024).
4. Capability Depth (not only headcount): measure maturity of MLOps, audit readiness, and assurance competencies rather than only counting trained staff (Reda et al., 2025; Yeung, 2025).
5. Value Realization and Public Trust: track service outcomes plus public-value impacts (transparency, equity, accountability) and trust signals such as complaints and perceived fairness (Chen, 2023; Mišić et al., 2025).

The synthesis is intentionally "Saudi-fit" in the sense that it assumes centralized orchestration is possible and that national entities can be aligned through standards, platforms, and measurement systems. This assumption is consistent with descriptions of SDAIA's coordinating mandate and Saudi's national strategy posture in peer-reviewed literature (Memish et al., 2021; Ibrahim, 2024). At the same time, the framework is written to be adaptable: it emphasizes mechanisms that can be implemented incrementally and audited, rather than presuming that all entities will reach the same maturity at the same time. In other words, the framework is designed to support staged progression, where entities can move from foundational data readiness to governed delivery and then to robust lifecycle assurance.

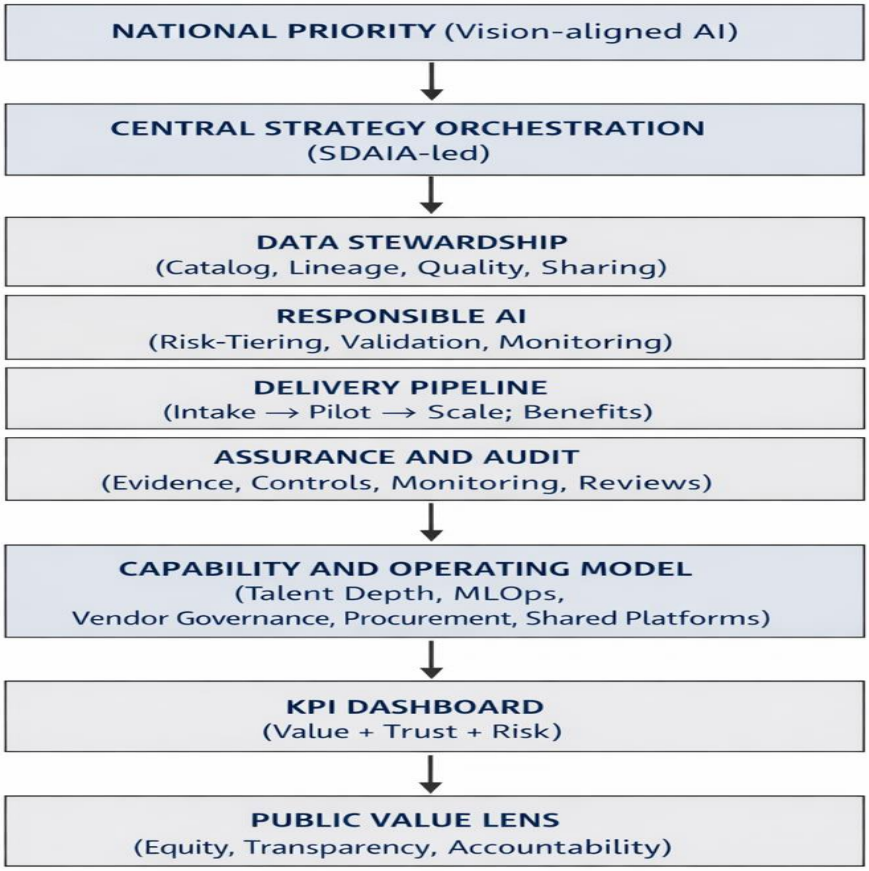
Proposed Governance-to-Execution Framework (Saudi-fit, 2020–2026)

The proposed framework translates "AI as a national priority" into a chain of operational building blocks that can be managed, measured, and audited. It begins with national alignment and central orchestration, and is realized via data stewardship, delivery pipelines, responsible AI controls, capability building, and assurance.

Why this structure is evidence-based

First, it mirrors responsible AI governance as a combination of structural, relational, and procedural practices, which is useful for connecting national institutions to operational controls (Papagiannidis et al., 2025). Second, it embeds the operationalization of responsible AI principles via concrete capabilities that can be deployed as standard requirements across entities (Akbarighatar, 2024). Third, it aligns with empirical findings about how public organizations implement governance guidance through processes and documentation that fit public-sector realities (Almeida & dos Santos Júnior, 2025). Fourth, it explicitly integrates public values and strategy discourse findings, ensuring that legitimacy and trust are measured alongside efficiency (Chen, 2023; Hjaltalin & Sigurdarson, 2024; Mišić et al., 2025).

Figure 1. Governance-to-Execution Model (Graphical Representation)



4. Framework interpretation in a Saudi national context

Strategic orchestration implies setting common standards, providing shared platforms, and creating incentives or requirements that shape how ministries and regulated sectors act. In practice, centralized leadership should focus on removing coordination failure: duplicated data efforts, inconsistent governance interpretations, fragmented tooling, and siloed pilots. The framework therefore treats SDAIA-led orchestration as a mechanism to harmonize the rules and to provide enabling infrastructure that lowers barriers to adoption while raising governance quality.

Data stewardship is the foundational layer because data readiness determines whether AI systems can be trained and evaluated reliably, and whether models can be reused across organizations. Responsible AI is treated as lifecycle control, not a one-time checklist. Delivery pipeline governance ensures that projects move from intake to pilot to production with clear stage gates, portfolio oversight, and benefits tracking. Assurance and audit ensure that evidence exists, controls are enforced, and systems remain reliable and fair over time. Capability building supports all layers: without MLOps competence, audit readiness, and a clear operating model, standards remain aspirational.

5. Objectives, Indicators, and Evidence (KPI logic)

A core challenge in national AI strategies is that measurement systems often track inputs—funding, number of training programs, or number of pilots—without proving that adoption is scaling responsibly or producing sustained public value (Radu, 2021; OECD, 2021). The proposed KPI logic model

addresses this by linking objectives to indicators and evidence artifacts that are audit-ready. Evidence artifacts matter because they enable verification by internal oversight units, external auditors, and regulators, and they reduce the risk that "progress" is reported without consistent documentation.

Table 1. National Objectives → Indicators → Evidence Artifacts (audit-ready) → Supporting literature

Dimension	**Description**
Objective	**Interoperable Data Readiness**
Purpose	Ensure that high-priority national datasets are discoverable, interoperable, and fit-for-use across public and semi-public entities through standardized governance, quality assurance, and controlled sharing mechanisms.
Key National Indicators (Examples)	• Percentage of priority datasets cataloged with complete metadata and lineage documentation
	• Coverage of data quality scoring across priority datasets
	• Number of cross-entity datasets shared through standardized data-sharing agreements
	• Mean time required to discover, request, and access a priority dataset
Measurement Scope	National-level priority datasets across ministries, regulators, and strategic public-sector entities
Evidence Artifacts	• National data catalog entries and metadata records
	• Automated and manual data lineage logs
	• Data quality assessment and monitoring reports
	• Access-control policies and cross-entity data-sharing agreements
	• Dataset documentation and stewardship records
Governance Ownership	Central data authority or national AI governance body in coordination with entity-level data stewards
Audit and Assurance Use	Provides verifiable evidence for compliance reviews, interoperability audits, AI readiness assessments, and cross-sector data governance maturity evaluations
Supporting Literature	Bernardo et al. (2024); Bližnák et al. (2024); Hassani et al. (2025); Gebru et al. (2021)

Objective: Responsible-AI Assurance

Key national indicators (examples): percentage of high-impact systems assigned a risk tier; percentage with documented validation and monitoring; number of incidents per system-year; mean time to detect and mitigate drift or harm events.

Evidence artifacts: model registry entries; risk-tiering decisions; validation and testing reports; monitoring dashboards; incident response playbooks and logs.

Supporting literature: Akbarighatar (2024); Batool et al. (2025); Papagiannidis et al. (2025).

Objective: Delivery Pipeline Performance

Key national indicators (examples): pilot-to-scale conversion rate; median time-to-scale; stage-gate compliance rate; benefits realization rate at 6 and 12 months after go-live.

Evidence artifacts: portfolio dashboards; stage-gate documentation; project charters; benefits realization reports; post-implementation review documents.

Supporting literature: Almeida & dos Santos Júnior (2025); Hjaltalin & Sigurdarson (2024).

Objective: Capability Depth

Key national indicators (examples): percentage of AI teams meeting defined MLOps maturity thresholds; percentage with audit-readiness capabilities; training depth measures such as assessed competency levels; retention and career pathway metrics for critical roles.

Evidence artifacts: skills matrices; MLOps checklists; training records; certification evidence; internal assessments; operating model documents.

Supporting literature: Reda et al. (2025); Yeung (2025); Schneider et al. (2023).

Objective: Value Realization and Public Trust

Key national indicators (examples): service outcome improvements (time, cost, accuracy); equity and fairness metrics; transparency and explainability coverage for relevant services; complaint rates and appeal outcomes; citizen satisfaction and trust survey measures.

Evidence artifacts: benefits realization reports; fairness test reports; explainability documentation; transparency notices; complaint and incident logs; oversight committee minutes.

Supporting literature: Chen (2023); Mišić et al. (2025); Kamphorst (2025).

6. KPI logic model: how instruments connect to outcomes

The KPI logic model can be read as a causal chain. Policy instruments such as national standards, shared platforms, procurement guidance, and funding programs influence organizational behaviors: cataloging data, documenting models, adopting monitoring tooling, and following stage gates. These behaviors produce intermediate outputs such as reusable datasets, standardized evidence packs, and repeatable delivery pipelines. Intermediate outputs then enable outcomes: more scaled deployments, reduced duplication, improved service performance, and higher trust because decisions are explainable and contestable. Finally, assurance mechanisms such as audits and incident response close the loop by detecting failures, enforcing remediation, and feeding lessons into updated standards.

Responsible AI Risk-Control Matrix (Operational)

Responsible AI becomes actionable when risks are defined, controls are assigned, and evidence is produced to demonstrate compliance and performance. The matrix below translates national-scale risk categories into minimum controls and standard evidence for auditing, consistent with capability-based governance and AI auditing literature (Akbarighatar, 2024; Mökander et al., 2024; Kamphorst, 2025).

Table 2. National-scale controls for high-impact AI

Risk Category	Typical Failure Modes	Minimum Control Requirements	Standard Evidence for Audit
Data Risk	Bias from unrepresentative samples; missing or incomplete data; data leakage; weak or missing lineage; unauthorized use; low data quality	Dataset documentation; automated and manual data quality checks; access controls; explicit purpose limitation; formal change management for critical datasets	Datasheets for datasets; data quality rulesets and reports; access and usage logs; lineage documentation
Model Risk	Model drift; instability across subgroups; brittle performance under distribution shifts; poor calibration; reproducibility failures	Formal validation protocols; continuous monitoring with drift triggers; controlled deployment; retraining and rollback plans; reproducible pipelines	Validation reports; drift and stability reports; retraining triggers; post-deployment test results; MLOps pipeline logs
Fairness and Equity	Disparate impact; proxy discrimination; inconsistent outcomes across demographic groups; feedback loops reinforcing inequality	Risk-tiering for high-impact use cases; subgroup performance thresholds; bias and impact testing; human-in-the-loop escalation for contested decisions	Fairness testing reports; subgroup performance metrics; bias mitigation documentation; governance and ethics approvals
Transparency and Explainability	Non-explainable outcomes in services requiring reasons; opaque vendor models; insufficient disclosure to affected parties	Decision traceability; explainability methods aligned to risk tier; transparency notices; ability to provide reasons and appeal pathways	Documentation packages; model cards; explanation samples; disclosure artifacts; appeal process documentation
Governance and Accountability	Unclear ownership; inconsistent approval pathways; weak policy enforcement; misalignment between technical teams and service owners	RACI matrices; formal stage gates; oversight committees; escalation paths; procurement clauses mandating evidence and audit access	Governance charters; RACI documents; stage-gate records; committee meeting minutes; vendor and procurement contracts
Auditability and Assurance	Insufficient evidence; restricted auditor access; missing logs; inability to reproduce outcomes; lack	Evidence planning; standardized logging; access and retention requirements; periodic	Audit evidence plans; system and access logs; data retention policies; completed

	of monitoring history	audits for high-impact systems; independent review mechanisms	audit reports; remediation and tracking records

7.Discussion:

What "National Priority" Means in Practice

7.1 Strategy leadership must be coupled with delivery mechanics

National priority is not only a political announcement; it is an ability to coordinate cross-entity delivery, set enforceable standards, and monitor implementation. OECD (2021) notes that national strategies vary in governance architecture and policy coherence, which affects implementation outcomes. Radu (2021) similarly highlights that national strategies require steering mechanisms that clarify ownership and align agencies.

In the Saudi case, peer-reviewed literature describes SDAIA as an authority with a vision to lead the Kingdom's journey toward global leadership, implying a coordinating mandate that can shape national execution (Memish et al., 2021). This positioning suggests that SDAIA's value is not only in promoting AI, but in building the plumbing of execution: shared standards, shared platforms, and cross-entity accountability. A governance-to-execution framework therefore treats strategic leadership as the ability to translate national ambition into enforceable requirements and repeatable processes that can be audited. This includes defining what counts as a high-impact system, what minimum evidence is required, and how benefits and harms are monitored after deployment.

7.2 Governance maturity is a prerequisite for scaling AI

Data governance maturity strongly predicts whether AI can move beyond pilots. Systematic reviews treat data governance as a measurable discipline with practices such as stewardship roles, data catalogs, quality metrics, lineage, and access controls (Bernardo et al., 2024; Bližnák et al., 2024; Hassani et al., 2025). Without maturity, AI initiatives struggle with inconsistent definitions, low-quality data, and uncertainty about permissible use. These issues slow delivery and create risk, leading to a pattern where pilot projects proliferate but few systems reach stable, scaled production.

For national strategies, the implication is that data readiness must be treated as a national program with prioritized datasets, common metadata standards, and incentives for sharing. Dataset documentation is also crucial for cross-agency trust: agencies are more likely to reuse datasets when suitability and limitations are clearly described (Gebru et al., 2021). Therefore, governance maturity is not a bureaucratic burden; it is a scaling engine that reduces duplication, improves reliability, and accelerates time-to-value. In Saudi Arabia's context, this supports rapid modernization by ensuring that AI deployments are not repeatedly delayed by data discovery and quality issues.

7.3 Responsible AI is now an operational requirement, not a statement

Responsible AI has become operational due to increasing regulation, public scrutiny, and the recognized risks of automated decision-making in high-impact contexts. Akbarighatar (2024) argues that responsible AI principles must be translated into capabilities, and Papagiannidis et al. (2025) emphasize embedding ethics into procedures, roles, and monitoring. In public services, the stakes are higher: biased or opaque AI can harm citizens, trigger legal challenges, and reduce trust in government, which in turn undermines strategic goals.

A key point is that responsible AI is not achieved by a single policy document. It requires lifecycle governance: risk-tiering at intake, validation before deployment, monitoring after deployment, and

incident response when harms are detected. This lifecycle approach aligns with emerging AI management system thinking and governance research that frames reliability and ethical performance as ongoing obligations rather than one-time approvals (Yeung, 2025; Camilleri, 2024). For national execution, the policy challenge is to standardize lifecycle controls without suffocating innovation. Capability-based requirements address this by specifying outcomes and evidence, while allowing technical implementation choices to vary by agency and use case.

7.4 AI auditing becomes the enforcement bridge

Auditing connects governance to enforcement by requiring evidence and by creating accountability for outcomes. Mökander et al. (2024) argue that audits require defined access and evidence; without them, audits cannot assess real performance or compliance. Kamphorst (2025) frames auditing as continuous performance appraisal, suggesting that oversight should evaluate systems over time. For national execution, auditing serves multiple purposes: it deters shortcuts, improves documentation discipline, identifies systemic weaknesses, and provides a mechanism for remediation tracking. It also helps standard setters refine what evidence is actually useful, by learning from audit findings and recurring failure modes.

8. Implementation Roadmap (Practical, 2020–2026 aligned)

A phased rollout makes the framework implementable, supports change management, and enables learning. The phases are designed to build foundations first, then scale delivery with responsible controls, and finally institutionalize assurance and continuous improvement.

Phase 1: Foundation (Data and standards)

Establish a national data catalog for priority datasets, including metadata, lineage, ownership, and access mechanisms. Define minimum dataset documentation standards and data quality scoring. Adopt common identifiers and interoperability standards to enable cross-agency linking where lawful and appropriate (Gebru et al., 2021; Bernardo et al., 2024). Build governance roles such as data owners and stewards and define escalation mechanisms for data quality and access disputes (Bližnák et al., 2024; Hassani et al., 2025).

Phase 2: Governed delivery (portfolio and stage gates)

Create a standardized pipeline from intake to pilot to scale. Intake includes problem statements, data readiness checks, and initial risk-tiering. Stage gates require documented validation, security checks, and benefits plans before production deployment. Portfolio governance tracks conversion rates, time-to-scale, and benefits realization, enabling national prioritization and resource allocation (Almeida & dos Santos Júnior, 2025). This phase reduces the pilot trap by requiring evidence of scalability and by creating a common language for progress reporting.

Phase 3: Responsible AI lifecycle controls (capability-based governance)

Operationalize responsible AI through capabilities: model registries, documentation, validation protocols, monitoring dashboards, and incident response playbooks (Akbarighatar, 2024; Batool et al., 2025). Define risk tiers and corresponding control requirements, ensuring that high-impact uses receive stronger scrutiny and continuous monitoring. Integrate controls into MLOps pipelines so that governance is automated where possible and evidence is generated by default (Reda et al., 2025).

Phase 4: Audit and public trust (assurance programs)

Define evidence access requirements and audit programs for high-impact systems, including periodic reviews and independent assessments where appropriate (Mökander et al., 2024; Kamphorst, 2025).

Establish transparent communication mechanisms such as public-facing AI registers for selected services, explanation channels, and complaint handling processes. Measure trust and public value impacts, not only operational performance (Chen, 2023; Mišić et al., 2025).

9. Conclusion

Using 2020–2026 literature, this paper proposed a Saudi-fit governance-to-execution framework to translate "AI as a national priority" into measurable and auditable delivery. The framework integrates data stewardship, responsible AI lifecycle controls, delivery pipelines, capability depth, and assurance mechanisms such as auditing and continuous monitoring. It emphasizes that national success depends on interoperable data readiness, enforceable responsible AI capabilities, and cross-entity assurance routines. The practical contribution is a set of operational national objectives, a KPI logic structure, and a risk-control matrix that can be implemented across government entities and regulated sectors to scale AI responsibly. By connecting governance to delivery mechanics and audit-ready evidence, the framework supports execution that is not only fast, but also trustworthy, measurable, and sustainable.

References

1. Akbarighatar, P. (2024). Operationalizing responsible AI principles through responsible AI capabilities. AI and Ethics. https://doi.org/10.1007/s43681-024-00524-4
2. Alboaneen, D., et al. (2025). Siyasat: AI-powered AI governance tool to generate and align AI policies. Computers. https://doi.org/10.3390/computers14110452
3. Almeida, P. G. R. de, & dos Santos Júnior, C. D. (2025). Artificial intelligence governance: Understanding how public organizations implement it. Government Information Quarterly, 42(1), 102003. https://doi.org/10.1016/j.giq.2024.102003
4. Bernardo, B. M. V., et al. (2024). Data governance & quality management—Innovation and breakthroughs across different fields. Journal of Innovation & Knowledge. https://doi.org/10.1016/j.jik.2024.100379
5. Bližnák, K., Munk, M., & Pilková, A. (2024). A systematic review of recent literature on data governance (2017–2023). IEEE Access. https://doi.org/10.1109/ACCESS.2024.3476373
6. Camilleri, M. A. (2024). Artificial intelligence governance: Ethical considerations and regulatory perspectives. Expert Systems. https://doi.org/10.1111/exsy.13406
7. Chen, Y.-C. (2023). Artificial intelligence and public values: Value impacts and governance in the public sector. Sustainability, 15(6), 4796. https://doi.org/10.3390/su15064796
8. Demaidi, M. N., & Qawasmeh, S. (2023). Artificial intelligence national strategy in a developing country. AI & Society. https://doi.org/10.1007/s00146-023-01779-x
9. Fatima, S. (2022). Interpreting national artificial intelligence plans. Telecommunications Policy. https://doi.org/10.1016/j.telpol.2022.102348
10. Gebru, T., et al. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92. https://doi.org/10.1145/3458723
11. Golbin, I. (2020). Responsible AI: A primer for the legal community. IEEE BigData 2020. https://doi.org/10.1109/BigData50022.2020.9377738
12. Gunasekara, L., et al. (2025). A systematic review of responsible artificial intelligence. Applied System Innovation, 8(4), 97. https://doi.org/10.3390/asi8040097

13. Hassani, H., Huang, X., & Silva, E. (2025). Mapping the evolution of data governance scientific research. Data & Policy, 7, e51. https://doi.org/10.1017/dap.2025.10014
14. Hjaltalin, I. T., & Sigurdarson, I. B. (2024). The strategic use of AI in the public sector: A public values analysis of national AI strategies. Government Information Quarterly. https://doi.org/10.1016/j.giq.2024.101914
15. Ibrahim, N. M. H. (2024). Artificial intelligence (AI) and Saudi Arabia's governance. SAGE Open. https://doi.org/10.1177/0169796X241288590
16. Kamphorst, B. A. (2025). AI auditing through performance appraisals. AI & Society. https://doi.org/10.1007/s00146-025-02674-3
17. Memish, Z. A., Alharthy, A., Alqahtani, S. A., Karakitsos, D., & Alqahtani, M. (2021). The Saudi Data & Artificial Intelligence Authority (SDAIA) vision: Leading the Kingdom's journey toward global leadership. Journal of Epidemiology and Global Health. https://doi.org/10.2991/jegh.k.210405.001
18. Mišić, J., van Est, R., & Kool, L. (2025). Good governance of public sector AI: A combined value framework for good order and a good society. AI and Ethics. https://doi.org/10.1007/s43681-025-00751-3
19. Mökander, J., et al. (2024). A discussion of access and evidence in AI auditing. ACM Conference Proceedings. https://doi.org/10.1145/3689904.3694711
20. OECD. (2021). An overview of national AI strategies and policies. OECD Going Digital Toolkit. https://doi.org/10.1787/726fd39d-en
21. Papagiannidis, E., et al. (2025). Responsible artificial intelligence governance: A review and research agenda. Journal of Strategic Information Systems. https://doi.org/10.1016/j.jsis.2024.101885
22. Papyshev, G. (2023). The state's role in governing artificial intelligence. Global Public Policy and Governance. https://doi.org/10.1080/25741292.2022.2162252
23. Peters, D., & others. (2020). Responsible AI—Two frameworks for ethical design practice. IEEE Transactions on Technology and Society. https://doi.org/10.1109/TTS.2020.2974991
24. Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. Policy and Society, 40(2), 178–193. https://doi.org/10.1080/14494035.2021.1929728
25. Reda, A., et al. (2025). Hybrid MLOps framework for automated lifecycle governance. Scientific Reports. https://doi.org/10.1038/s41598-025-23600-z
26. Schmitt, L. (2022). Mapping global AI governance: A nascent regime in a fragmented landscape. AI and Ethics. https://doi.org/10.1007/s43681-021-00083-y
Schneider, J., et al. (2023). Artificial intelligence governance for businesses. Behaviour & Information Technology. https://doi.org/10.1080/10580530.2022.2085825
27. Yeung, S. M. C. (2025). AI management system ISO 42001 and SDG for impacts. Journal of Ecohumanism. https://doi.org/10.62754/joe.v4i4.6985
28. Batool, A., et al. (2025). AI governance: A systematic literature review. AI and Ethics. https://doi.org/10.1007/s43681-024-00653-w
29. Wiley-Online. (2026). Lifecycle-based governance to build reliable ethical AI. Systems Research and Behavioral Science. https://doi.org/10.1002/sres.70014