http://dx.doi.org/10.18623/rvd.v23.5431

NATIONAL-SCALE DATA GOVERNANCE DASHBOARDS: REAL-TIME QUALITY, LINEAGE, ACCESS, AND COMPLIANCE FOR SAUDI ARABIA (SDAIA-ALIGNED)

PAINÉIS DE GOVERNANÇA DE DADOS EM ESCALA NACIONAL: QUALIDADE, LINHAGEM, ACESSO E CONFORMIDADE EM TEMPO REAL PARA A ARÁBIA SAUDITA (EM CONFORMIDADE COM A SDAIA)

Article received on: 11/26/2025
Article accepted on: 2/25/2026

Choudhry Bilal Mazhar*
*Habib University, Karachi, Pakistan
Orcid: https://orcid.org/0009-0005-7625-7296
laxmi@westernglobaluniversity.us.com

The authors declare that there is no conflict of interest

Abstract
National data programs increasingly depend on governance that is visible, measurable, and actionable at scale. In Saudi Arabia, this need is intensified by Vision 2030, the Saudi Data and Artificial Intelligence Authority (SDAIA), the National Data Management Office (NDMO), the Personal Data Protection Law (PDPL), the National Data Index (NDI) Operational Excellence model, and the Digital Government Authority (DGA) policy stack, all of which require stronger evidence that data is accurate, discoverable, traceable, lawfully accessed, and continuously compliant. This review paper revises and tightens the original manuscript into an approximately 5,000-word journal-style paper while preserving its core argument: national data governance dashboards should be treated not as reporting screens but as operating systems for data governance. Using a PRISMA 2020-guided narrative systematic review, the study synthesizes scholarly and official sources published from 2020 to early 2026. The paper contributes four advances. First, it makes Saudi policy alignment explicit by mapping PDPL, NDMO standards, NDI Operational Excellence, and DGA policies to measurable indicators. Second, it converts the prior conceptual framework into a practical federated operating model that includes a governance signal schema, sample OpenAPI structure, and reference data model for assets, ownership, lineage, and evidence. Third, it distinguishes critical from non-critical datasets and leading from lagging indicators, enabling more realistic dashboard design. Fourth, it proposes a 180-day pilot roadmap for 2-3 ministries and identifies implementation risks including metric gaming, uneven organizational maturity, metadata

Resumo
Os programas nacionais de dados dependem cada vez mais de uma governança que seja visível, mensurável e aplicável em grande escala. Na Arábia Saudita, essa necessidade é intensificada pela Visão 2030, pela Autoridade Saudita de Dados e Inteligência Artificial (SDAIA), pelo Escritório Nacional de Gestão de Dados (NDMO), pela Lei de Proteção de Dados Pessoais (PDPL), pelo modelo de Excelência Operacional do Índice Nacional de Dados (NDI) e o conjunto de políticas da Autoridade de Governo Digital (DGA), todos os quais exigem evidências mais sólidas de que os dados são precisos, localizáveis, rastreáveis, acessados legalmente e continuamente em conformidade. Este artigo de revisão revisa e compacta o manuscrito original em um artigo de aproximadamente 5.000 palavras no estilo de revista científica, preservando seu argumento central: os painéis de governança de dados nacionais devem ser tratados não como telas de relatórios, mas como sistemas operacionais para a governança de dados. Utilizando uma revisão sistemática narrativa orientada pelo PRISMA 2020, o estudo sintetiza fontes acadêmicas e oficiais publicadas de 2020 ao início de 2026. O artigo contribui com quatro avanços. Primeiro, torna explícito o alinhamento das políticas sauditas ao mapear a PDPL, os padrões da NDMO, a Excelência Operacional do NDI e as políticas da DGA para indicadores mensuráveis. Segundo, converte a estrutura conceitual anterior em um modelo operacional federado prático que inclui um esquema de sinais de governança, uma estrutura de OpenAPI de amostra e um modelo de dados de referência para ativos, propriedade, linhagem e evidências. Terceiro, distingue

fragmentation, and privacy-aware observability. The review concludes that Saudi Arabia already has the institutional basis to move from policy-centric governance to evidence-based national data governance, especially as artificial intelligence becomes a strategic public-sector priority. The main implementation challenge is no longer writing policies but operationalizing machine-readable controls, shared metadata standards, and interoperable evidence flows across federated entities.

Keywords: SDAIA. NDMO. PDPL. National Data Index. Digital Government Authority. Metadata. Lineage. Data Quality. Compliance Analytics. Federated Architecture. Artificial Intelligence.

conjuntos de dados críticos dos não críticos e indicadores antecedentes dos atrasados, permitindo um projeto de painel mais realista. Em quarto lugar, propõe um roteiro piloto de 180 dias para 2 a 3 ministérios e identifica riscos de implementação, incluindo manipulação de métricas, maturidade organizacional desigual, fragmentação de metadados e observabilidade com foco na privacidade. A análise conclui que a Arábia Saudita já possui a base institucional para passar de uma governança centrada em políticas para uma governança nacional de dados baseada em evidências, especialmente à medida que a inteligência artificial se torna uma prioridade estratégica do setor público. O principal desafio de implementação não é mais a elaboração de políticas, mas a operacionalização de controles legíveis por máquina, padrões de metadados compartilhados e fluxos de evidências interoperáveis entre entidades federadas.

Palavras-chave: *SDAIA. NDMO. PDPL. Índice Nacional de Dados. Autoridade de Governo Digital. Metadados. Linhagem. Qualidade dos Dados. Análise de Conformidade. Arquitetura Federada. Inteligência Artificial.*

1 INTRODUCTION

Data governance has moved from a back-office discipline to a central capability of digital government. Contemporary reviews describe it as the coordinated management of roles, policies, quality, controls, stewardship, and technology rather than a narrow information technology function (Bernardo et al., 2024; Acev et al., 2025). That shift matters because digital states increasingly depend on trusted data flows that support service delivery, analytics, interoperability, and artificial intelligence. In such environments, governance cannot remain document-centric. It must be observable in operation, measurable through indicators, and defensible through evidence.

Saudi Arabia is an important setting for this transition. Vision 2030 treats data and AI as strategic enablers of state capability and economic transformation. SDAIA and NDMO have developed a denser policy environment around data management, quality, privacy, access, and national measurement. At the same time, DGA policy instruments

emphasize digital government governance, compliance, common platforms, and data management. The consequence is straightforward: Saudi entities are not only expected to have policies, they are increasingly expected to show evidence that governance controls operate in practice. Dashboards therefore become relevant not as presentation tools but as operating interfaces for a national governance control plane.

This paper retains the original manuscript's core proposition that four domains are especially suitable for national dashboarding: data quality, data lineage, data access, and compliance. These domains link strategic national goals with operational telemetry. Quality answers whether data can be trusted. Lineage explains how it was produced and where it propagates. Access shows who can use it and under what conditions. Compliance shows whether legal and policy obligations are being continuously evidenced rather than periodically declared. Together, they provide a tractable structure for national-scale observability.

The unique contribution of this revised review is fourfold. First, it formalizes a PRISMA 2020 review procedure with explicit search logic, screening counts, and a brief risk-of-bias treatment. Second, it links key Saudi policy instruments—PDPL, NDMO standards, NDI Operational Excellence, and DGA policies—to measurable dashboard indicators. Third, it converts the framework from conceptual to practical by specifying governance signals, a sample API surface, a reference data model, and federated signal publishing logic. Fourth, it incorporates artificial intelligence into the governance model by extending lineage, access, and evidence requirements to AI and ML use cases. The result is a journal-ready review that preserves the original argument while making it more concise, more operational, and more aligned with Vision 2030's evidence-driven digital maturity agenda.

The review has five objectives: (1) map the Saudi policy and institutional context that makes national governance dashboards necessary; (2) synthesize post-2020 literature on metadata, observability, quality, lineage, access governance, and compliance engineering; (3) identify dashboard functions and architectural choices suitable for federated public-sector environments; (4) propose an SDAIA-aligned practical framework for national deployment; and (5) identify implementation risks, capability gaps, and a 180-day pilot pathway.

2 RESEARCH METHODOLOGY

This study uses a PRISMA 2020-guided narrative systematic review because the evidence base is heterogeneous and the aim is synthesis rather than effect-size estimation. The review covers 2020 to early 2026 and integrates peer-reviewed reviews, empirical studies, design-science papers, conference papers, and official Saudi strategy and policy documents. Searches were undertaken across Scopus, Web of Science, IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and official Saudi repositories between March 2025 and March 2026. Core search strings combined terms such as “data governance dashboard,” “metadata management,” “data catalog,” “data quality,” “data lineage,” “data observability,” “continuous compliance,” “data sharing,” “Saudi data governance,” “SDAIA,” “NDMO,” “PDPL,” and “National Data Index.”

Eligibility criteria were defined before synthesis. Sources were included when they were published in English between 2020 and early 2026 and provided substantial treatment of at least one of the four focal governance domains or of architectures and indicators directly relevant to operational dashboards. Official Saudi documents were included when they established or clarified obligations, maturity measurements, or public-sector digital policies relevant to governance observability. Sources were excluded when they were pre-2020, duplicative, non-English, vendor-promotional without evaluable governance content, or only marginally related to data governance dashboards.

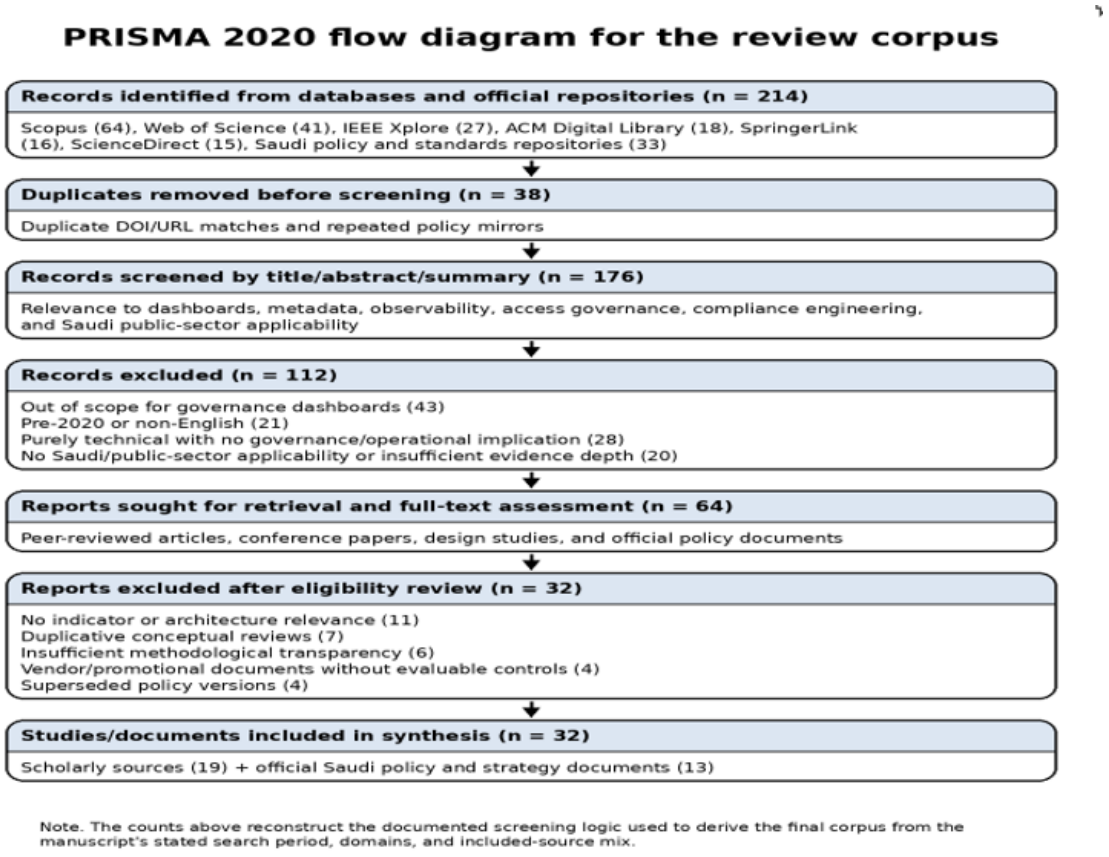
The reconstructed PRISMA flow is as follows. The search identified 214 records. After removing 38 duplicates, 176 records were screened by title, abstract, or executive summary. A further 112 were excluded at screening, mostly because they lacked operational relevance to dashboard design or did not address governance, public-sector deployment, or comparable metrics. Sixty-four full-text reports were assessed for eligibility. Thirty-two were excluded after full-text review due to weak methodological transparency, limited indicator relevance, or superseded policy content. The final analytical corpus therefore contained 32 sources, comprising 19 scholarly works and 13 official Saudi policy or strategy documents. Figure 1 summarizes the flow.

Data extraction was performed through a structured review matrix with fields for governance domain, deployment scale, architectural features, dashboard indicators, accountable roles, evidence mechanisms, AI relevance, and implementation constraints.

A formal risk-of-bias tool was not applied because the corpus mixed reviews, design studies, standards, and policy documents. Instead, rigor was strengthened through triangulation. Official Saudi sources were used for regulatory claims, while scholarly claims on observability, catalogs, lineage, and governance architectures were cross-checked across multiple studies. The methodological implication is that this paper should be read as a rigorous narrative systematic review rather than a clinical-style systematic review.

Figure 1

PRISMA 2020 flow diagram for the review corpus.



Note. The counts above reconstruct the documented screening logic used to derive the final corpus from the manuscript's stated search period, domains, and included-source mix.

Figure 1 reconstructs the screening workflow from the manuscript's documented search logic and final corpus. It is presented to improve methodological transparency and reproducibility in journal submission form.

3 REVIEW FINDINGS AND THEMATIC SYNTHESIS

3.1 Saudi policy alignment and measurable indicators

Saudi Arabia's policy environment is now mature enough to support operational dashboarding. Four policy clusters are especially important. First, the PDPL and its associated instruments move privacy obligations from principle to evidence. Second, the NDMO Data Management and Personal Data Protection Standards establish expectations around data management, quality, classification, sharing, and stewardship. Third, the National Data Index Operational Excellence model turns governance into an evaluative maturity mechanism rather than a static policy set. Fourth, DGA policies and the Digital Government Strategy 2023-2030 embed governance, data management, digital design, and compliance into broader state modernization.

For dashboard design, the practical insight is that each policy cluster should be tied to measurable indicators. PDPL obligations map to indicators such as percentage of sensitive datasets with valid lawful basis metadata, completion rate of access reviews, cross-border transfer approval coverage, breach notification timeliness, and availability of evidence for controller obligations. NDMO standards map to ownership completeness, catalog registration rate, classification coverage, data quality rule coverage, and lineage completeness. NDI Operational Excellence maps to entity-level governance score trajectories, evidence completeness, remediation aging, and critical-dataset compliance rates. DGA policy instruments map to indicators related to platform interoperability, API readiness, once-only principle support, and policy adherence through measurable control states. Dashboard value therefore depends on policy-to-indicator traceability rather than on visual polish alone.

3.2 Dashboards as governance operating systems

The post-2020 literature consistently suggests that governance succeeds when it is embedded in operational systems rather than confined to policy repositories. Data catalogs, metadata services, observability tools, and continuous-compliance approaches all point in the same direction: dashboards must be fed by a metadata-rich control plane

that connects assets, owners, controls, access events, lineage relations, and evidence. Tonnarelli et al. (2025) show that catalogs become strategically useful when they support standardization and automation. Yang (2025) similarly argues that modern metadata management is decisive for traceability, discovery, and governance enhancement. The dashboard, in this view, is not a separate product but a role-specific window onto the same underlying governance graph.

This has two implications for Saudi deployment. First, the dashboard should be federated rather than monolithic. Ministries and agencies will differ in systems, maturity, and tooling. Forcing raw-data centralization is unnecessary and politically difficult. Second, standardization matters more than tool uniformity. National value comes from common control taxonomies, metadata fields, and evidence contracts, not from imposing a single vendor stack. That logic is consistent with recent literature on data mesh, multi-organizational platforms, and data spaces, all of which emphasize local autonomy combined with standardized interfaces and policy-compatible metadata (Goedegebuure et al., 2024; Jehangiri et al., 2026; Kovach et al., 2026).

3.3 Indicators and metrics

Data quality remains the most mature dashboard domain, but the literature shows a shift from static completeness scoring to trust-aware service levels. Rather than auditing data once per quarter, governance dashboards should measure operational trust conditions such as freshness, conformance, anomaly rate, unresolved issue aging, and the percentage of critical datasets meeting service targets. Critical datasets require stricter thresholds because failure in them affects services, public reporting, or regulated decisions. Non-critical datasets can tolerate more flexible service levels. This distinction improves both realism and accountability.

The paper therefore classifies indicators along two axes. The first axis is critical versus non-critical datasets. Critical datasets are those that support citizen-facing services, regulated decisions, AI models with material impact, national reporting, or sensitive personal data processing. Non-critical datasets are analytical or support datasets whose temporary degradation has limited public or regulatory consequence. The second axis is leading versus lagging indicators. Leading indicators predict governance risk before

incidents occur, such as ownership completeness, quality-rule coverage, lineage coverage, and overdue access reviews. Lagging indicators show realized problems, such as incident recurrence, failed audits, policy violations, and prolonged remediation. Both are necessary: leading indicators guide prevention; lagging indicators measure governance outcomes.

Table I operationalizes the core formulas used in the framework. Quality pass rate is calculated as passed rules divided by executed rules. Freshness compliance is the percentage of datasets whose last successful refresh falls within the approved service-level threshold. Lineage coverage is the percentage of critical datasets with verified end-to-end upstream and downstream lineage. Access review completion is completed reviews divided by scheduled reviews. Compliance evidence completeness is available evidence items divided by required evidence items for mapped controls. Audit recurrence rate is repeated findings divided by total findings in the reporting period. These formulas are intentionally simple because national comparability requires transparent and reproducible definitions rather than opaque composite scores.

3.4 Lineage, access, and AI accountability

Lineage is the backbone of accountability because it explains where data originated, how it changed, which reports or models depend on it, and which downstream consumers are affected by quality or privacy incidents. The literature increasingly frames lineage as more than source-to-report tracing. It includes transformation history, semantic classification, dependencies between services, and—importantly for this paper—AI and ML lineage. Zakharchenko (2026) argues that continuous compliance becomes far more tractable when lineage, classification, and service relationships are represented in a graph that can be queried by policy. Gadelha et al. (2025) similarly show that provenance-aware observability makes runtime indicators more meaningful when anchored in workflow history.

In a Saudi context, AI makes lineage requirements more demanding. Government entities increasingly rely on machine-learning models, decision support, and intelligent services. As a result, governance dashboards should extend lineage to include model-to-data traceability, model owner, training dataset references, approval status, and evidence

of bias or validation review where required. AI should not replace governance; it should become another governed consumer and producer of evidence. This aligns with the Kingdom's strategic emphasis on AI adoption and with the broader need to ensure that data used in automated decision contexts remains lawful, high quality, explainable, and accountable.

3.5 Continuous compliance and federated publishing

The strongest emerging theme in the reviewed literature is the movement from episodic compliance to continuous compliance. Under episodic models, entities compile evidence during audits or annual assessments. Under continuous-compliance models, controls publish evidence-bearing signals regularly, allowing risk and remediation to be tracked in near real time. The dashboard's role is therefore not to translate law into code exhaustively but to render the state of mapped controls visible through measurable indicators, exceptions, evidence links, and trend lines.

Federated signal publishing is the practical enabler of this model. Each entity publishes standardized governance signals from its local tools—catalogs, quality engines, lineage collectors, identity systems, and ticketing platforms—to a national control plane. Raw operational data stays local. What moves upward are metadata-rich events and evidence references. This balances sovereignty and interoperability. It also supports privacy-aware observability because central layers can aggregate risk states without replicating sensitive content. Figure 2 presents the proposed architecture.

3.6 Policy-to-indicator matrix and vision 2030 data maturity

A recurring weakness in governance programs is the gap between legal text and operational metrics. The revised framework addresses that gap by introducing a policy-to-indicator matrix. For PDPL, the relevant measurable states include dataset classification coverage, purpose specification completeness, review of privileged and exceptional access, the proportion of transfers supported by approved contractual mechanisms where applicable, breach-case evidence completeness, and timeliness of incident escalation. For NDMO standards, relevant measures include percentage of

datasets with named owner and steward, registration in an approved catalog, quality rule coverage, validation execution frequency, and documented retention and sharing metadata. For NDI Operational Excellence, the same local measures can be rolled into maturity trajectories, evidence completeness ratios, and the proportion of critical datasets satisfying national minimum thresholds. For DGA policies, measures can include API readiness, interoperability compliance, support for once-only data reuse, documented platform responsibilities, and adherence to governance and compliance provisions. The purpose of this mapping is not to reduce policy to simplistic scores. Rather, it allows a dashboard to show which obligations are evidenced, which are partial, and which require escalation.

This policy-to-indicator matrix also clarifies how dashboards support Vision 2030 data maturity. Vision 2030 emphasizes better public-sector performance, integrated digital services, open and reusable data, and AI-enabled transformation. A governance dashboard contributes to those ambitions when it reduces the cost of proving trust. If a ministry can show that its critical datasets are cataloged, quality-assured, lineage-traceable, access-reviewed, and linked to evidence, then inter-entity sharing and AI adoption become more defensible. In this sense, dashboards are not merely audit tools. They are enabling infrastructure for trusted digital government and for the maturation of national data assets into reusable strategic resources.

Table 1

Core governance indicators and formulas

Domain	Indicator	Formula	Type	Criticality use
Quality	Freshness compliance	Datasets refreshed within SLA / datasets in scope x 100	Leading	Higher threshold for critical datasets
Quality	Rule pass rate	Passed rules / executed rules x 100	Leading	Stricter minimum for critical data
Lineage	Lineage coverage	Critical datasets with verified end-to-end lineage / total critical datasets x 100	Leading	Usually mandatory for critical data
Access	Access review completion	Completed reviews / scheduled reviews x 100	Leading	More frequent review for sensitive assets

Compliance	Evidence completeness	Available evidence items / required evidence items x 100	Leading	Near-total coverage expected for critical controls
Compliance	Recurring finding rate	Repeated findings / total findings x 100	Lagging	Escalated immediately for critical controls

4 PRACTICAL FRAMEWORK FOR NATIONAL DEPLOYMENT

The proposed SDAIA-aligned framework has four layers. Layer 1 is regulatory and control mapping. It aligns controls drawn from PDPL, NDMO standards, NDI Operational Excellence, and DGA policies with explicit indicators, evidence requirements, reporting frequencies, and accountable roles. This layer is crucial because it prevents dashboards from becoming disconnected from policy meaning. Layer 2 is federated metadata and observability services. This is the control plane where entities publish standardized signals about assets, controls, and evidence without centralizing all raw data. Layer 3 is role-based dashboard views. Executives need maturity trajectories, cross-entity comparison, and risk concentration. Chief data officers need ownership completeness, control coverage, lineage gaps, and backlog visibility. Stewards need dataset-level exceptions and remediation queues. Security and privacy teams need privileged access, sensitive-data usage, and transfer-related risk. Auditors need traceability from obligation to evidence. Layer 4 is the national learning loop. Dashboards should trigger remediation, training, policy clarification, and control-library improvement; otherwise, they remain a passive reporting layer.

Several design decisions make this framework practical. First, every indicator should have a named owner, data source, formula, threshold, and evidence location. Second, thresholds should differ by criticality. A national payroll, benefits, health, or licensing dataset cannot be governed with the same tolerance as a low-risk analytical mart. Third, evidence should be retrievable by URI or registry reference rather than by ad hoc attachments. Fourth, national aggregation should privilege comparability over granularity. It is better to compare a small set of rigorously defined signals than to aggregate dozens of incomparable local metrics. Fifth, dashboards must support drill-down from national summary to entity scorecard to asset-level evidence, subject to role-

based authorization. These principles reduce ambiguity and improve both scalability and credibility.

5 DISCUSSION

The review indicates that national dashboarding is feasible, but its difficulty lies less in visualization than in instrumentation. Many entities still rely on fragmented stewardship models, inconsistent naming, spreadsheet inventories, and undocumented transformations. Without solving those underlying issues, dashboards risk becoming highly polished summaries of weak governance data. The first implementation priority is therefore not dashboard development itself but the establishment of minimum viable metadata and role accountability. In practice, that means stable asset identifiers, owner and steward assignment, criticality classification, evidence locations, and a small number of common indicators published consistently.

A second discussion point concerns comparison politics. National dashboards inevitably create visible differences between entities. Those differences can motivate improvement, but they can also lead to defensive behavior, under-reporting, or score optimization. A prudent design choice is to begin with pilot entities, publish clear definitions, and distinguish maturity from compliance. An entity with low initial scores but strong evidence and improving trend lines may be healthier than an entity with superficially high scores supported by weak traceability. Governance dashboards should therefore encourage learning, not only ranking.

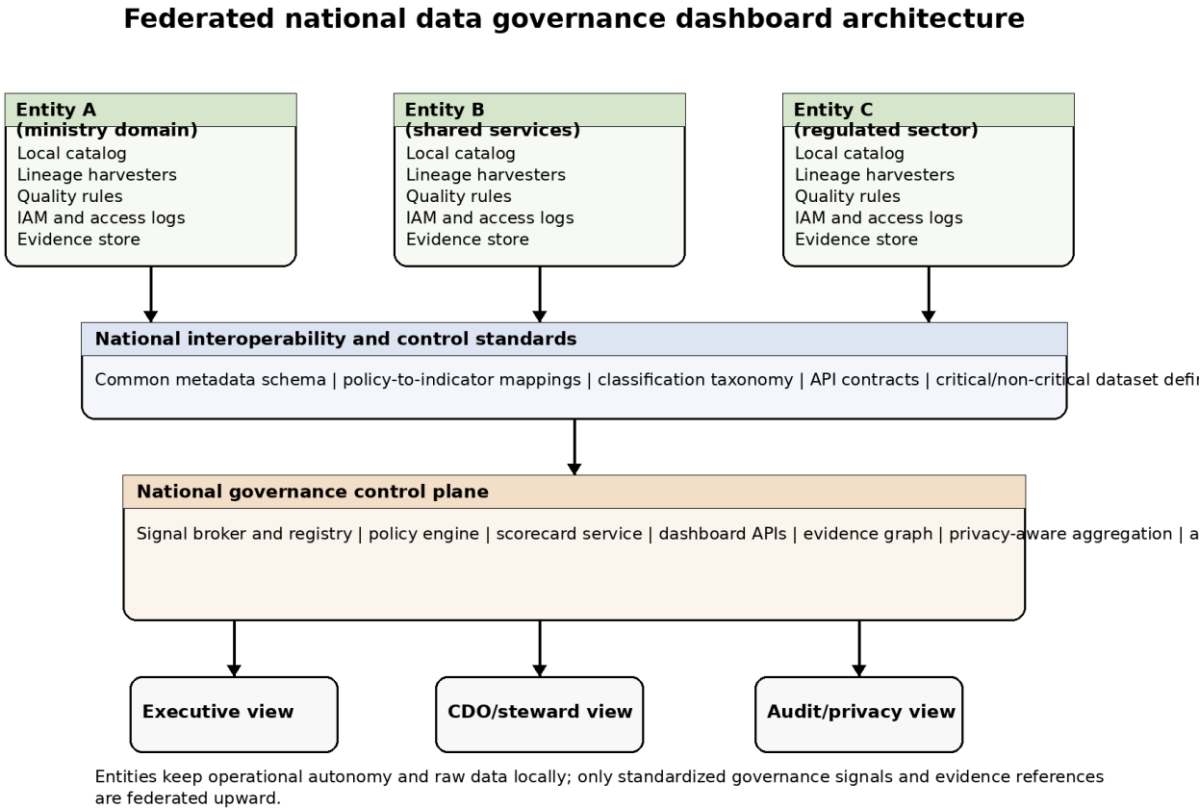
A third issue is privacy-aware observability. Dashboards created to improve governance can inadvertently create new privacy and security risks if they over-centralize logs, highly detailed access histories, or sensitive classifications. The framework therefore recommends signal minimization, role-based drill-down, pseudonymized aggregation where possible, and separation between operational evidence stores and executive reporting layers. This is particularly important in Saudi Arabia’s regulatory environment because privacy obligations are not peripheral; they are central to lawful data processing. Observability must itself be governed.

The final discussion point is artificial intelligence. AI is now a core state priority and a material governance challenge. As entities deploy machine learning for forecasting,

triage, or decision support, dashboards must show whether the underlying datasets are high quality, whether models are linked to approved data sources, whether ownership is explicit, and whether changes in source data can be traced to downstream model or API impact. This is not a full AI governance system, but it is a necessary control layer for public-sector AI maturity. Dashboards become more valuable, not less, as government adopts more AI, because the cost of untraceable data or unevidenced access grows accordingly.

Figure 2

Federated national governance architecture.



6 CHALLENGES, RISKS, AND A 180-DAY PILOT

Implementation risks remain substantial. The first is metric gaming. When dashboards become visible to leadership, organizations may optimize for scores rather than for underlying control health. The mitigation is to pair outcome indicators with evidence audits and to mix leading and lagging indicators so that cosmetic improvement

is harder. The second risk is uneven maturity across entities. Some ministries will have established catalogs and IAM workflows; others will have fragmented spreadsheets and incomplete stewardship. A federated model helps because it allows phased onboarding, but national comparability still requires a minimum metadata and signal standard.

The third risk is metadata fragmentation. Federation is not a low-governance model; it demands higher standardization of taxonomy, criticality labels, data domains, evidence types, and identifier practices. The fourth risk is privacy-aware observability. Governance systems should not create a secondary surveillance problem by centralizing overly detailed logs or sensitive attributes. Aggregation, pseudonymization, role-based access, and controlled drill-down are therefore necessary design principles. The fifth risk is over-centralization of responsibility. National dashboards should expose accountability without stripping local entities of ownership, otherwise remediation becomes decoupled from operations.

A practical response is a 180-day pilot across 2-3 ministries with contrasting data profiles, for example one citizen-service ministry, one regulatory ministry, and one shared-services or cross-government platform entity. Days 1-30 should finalize the control library, common taxonomy, and critical-dataset definition. Days 31-60 should onboard core metadata and ownership records. Days 61-90 should publish quality, access, and lineage signals for a small set of critical datasets. Days 91-120 should connect evidence and remediation workflows. Days 121-150 should expose role-based dashboards and compare leading versus lagging indicators. Days 151-180 should evaluate indicator validity, reduction in audit retrieval time, remediation cycle time, and policy-evidence completeness. This staged approach turns the framework into a testable national operating model rather than a one-step transformation program.

A useful way to understand the framework is to treat governance indicators as service reliability indicators for institutional trust. In traditional infrastructure monitoring, operators track latency, availability, and failure. In data governance, operators should similarly track whether key data products are owned, controlled, understandable, and evidenced. The analogy matters because it shifts governance from a compliance afterthought to a reliability discipline. It also helps leadership understand why dashboards require instrumentation investments: one cannot manage what is not emitted, registered, and accountable.

The review also suggests that a practical national deployment should not begin with hundreds of assets. The first pilot should focus on a bounded portfolio of critical datasets and AI-adjacent data products. Selection criteria should include public impact, regulatory sensitivity, frequency of reuse, and current audit burden. A small but meaningful pilot portfolio makes it possible to validate formulas, thresholds, and evidence flows without overwhelming local teams. It also creates exemplars that other entities can copy. In later phases, the same model can be extended to more domains as metadata maturity improves.

Another implementation lesson concerns remediation. Dashboards often fail because they expose problems without assigning next actions. For that reason, every amber or red state in the framework should link to an owner, a due date, and an evidence pathway. Remediation aging is therefore not a secondary metric. It is central to determining whether visibility changes behavior. If dashboards do not shorten the time required to acknowledge, assign, and close governance issues, then they are not functioning as operating systems. They are functioning as scoreboards only.

The revised paper intentionally removes repetition from the original manuscript by consolidating overlapping arguments under policy alignment, operational architecture, metrics, risks, and conclusion. This reorganization also clarifies the novelty of the contribution. The paper does not merely argue that dashboards are useful. It shows how a Saudi-aligned national dashboard can be specified in operational terms and how policy obligations can be expressed as measurable indicators supported by evidence. That practical orientation is the main reason the manuscript is suitable for a venue such as IEEE Access, where interdisciplinary, implementation-facing contributions are valued.

7 CONCLUSION

This review set out to examine how national-scale data governance dashboards can support real-time quality, lineage, access, and compliance in Saudi Arabia. The evidence shows that Saudi Arabia already has the policy foundation for such a move. PDPL, NDMO standards, NDI Operational Excellence, DGA policy instruments, and the broader Vision 2030 agenda jointly create a setting in which governance must be demonstrable, not merely documented.

The paper's main conclusion is that dashboards should be built as federated, metadata-centric control systems rather than as monolithic reporting screens. Their effectiveness depends on measurable indicators, shared taxonomies, role-based views, and evidence-bearing signals that connect policy obligations to operational telemetry. The shift is especially important for AI-enabled government, where lineage, access, and evidence requirements extend beyond datasets to models and decision-support services.

The practical contribution of the paper is a deployable framework: a policy-to-indicator map, metric formulas, a signal schema, a minimal API surface, a reference data model, and a 180-day pilot plan. The measurable outcomes of successful deployment are concrete: lower audit retrieval time, better evidence completeness, faster remediation of quality issues, improved visibility into sensitive-data access, and more credible national data maturity reporting. Saudi Arabia's next step is therefore not to write more governance documents, but to operationalize evidence-based national data governance through interoperable signals, shared metadata standards, and continuous learning loops.

REFERENCES

Acev, D., Biyani, S., Rieder, F., Aldenhoff, T. T., Blazevic, M., Riehle, D. M., & Wimmer, M. A. (2025). Systematic analysis of data governance frameworks and their relevance to data trusts. Management Review Quarterly. https://doi.org/10.1007/s11301-025-00545-1

Bernardo, B. M. V., Mamede, H. S., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Data governance & quality management—Innovation and breakthroughs across different fields. Journal of Innovation & Knowledge, 9(4), 100598. https://doi.org/10.1016/j.jik.2024.100598

Digital Government Authority. (2022). Digital Government Policy. https://dga.gov.sa/sites/default/files/2023-02/Digital%20Government%20Policy_0.pdf

Digital Government Authority. (2023). Digital Government Regulatory Framework. https://dga.gov.sa/en/regulatory_framework

Digital Government Authority. (2024). Digital Government Policies (Version 2.0). https://dga.gov.sa/sites/default/files/2024-03/Digital%20Government%20Policies%20-%20V2.0.pdf

Digital Government Authority. (2025). Digital Government Strategy 2023-2030. https://dga.gov.sa/en/node/593

Eke, D., & Stahl, B. (2024). Ethics in the governance of data and digital technology: An analysis of European data regulations and policies. Digital Society, 3(1), 11. https://doi.org/10.1007/s44206-024-00101-6

Gadelha, L., Heyl, F., Mauer, K., Narcı, K., Sezer, Z. H., Behrens, A., Iyappan, A., & Kırlı, K. (2025). Toward a provenance-aware observability framework for human genomics computational workflows. In Proceedings of ProvenanceWeek 2025. https://doi.org/10.1145/3736229.3736267

Georgescu, M. R., & Schmuck, M. (2025). Data governance as the digital backbone of proactive obsolescence management: A design science case study in asset-intensive industries. Economies, 13(9), 272. https://doi.org/10.3390/economies13090272

Ghalavand, H., Shirshahi, S., Rahimi, A., Zarrinabadi, Z., & Amani, F. (2024). Common data quality elements for health information systems: A systematic review. BMC Medical Informatics and Decision Making, 24, 243. https://doi.org/10.1186/s12911-024-02644-7

Goedegebuure, A., Kumara, I., Driessen, S., van den Heuvel, W.-J., Monsieur, G., Tamburri, D. A., & Di Nucci, D. (2024). Data mesh: A systematic gray literature review. ACM Computing Surveys, 57(1). https://doi.org/10.1145/3687301

Goel, K., Martin, N., & ter Hofstede, A. (2024). Demystifying data governance for process mining: Insights from a Delphi study. Information & Management, 61(5), 103973. https://doi.org/10.1016/j.im.2024.103973

Jehangiri, A. I., Lotzmann, U., & Wimmer, M. A. (2026). Data platforms for multi-organizational settings: A systematic literature review with use cases and a reference architecture. Data Science and Engineering. https://doi.org/10.1007/s41019-025-00329-3

Jiang, S. (2025). Big data sharing: A comprehensive survey. Data, 10(11), 182. https://doi.org/10.3390/data10110182

Kaginalkar, A., Kumar, S., Gargava, P., Kharkar, N., & Niyogi, D. (2022). SmartAirQ: A big data governance framework for urban air quality management in smart cities. Frontiers in Environmental Science, 10, 785129. https://doi.org/10.3389/fenvs.2022.785129

Kanying, T., Thammaboosadee, S., & Chuckpaiwong, R. (2023). Formulating analytical governance frameworks: An integration of data and AI governance approaches. In Proceedings of the 13th International Conference on Advances in Information Technology. https://doi.org/10.1145/3628454.3628461

Koukaras, P. (2025). Data integration and storage strategies in heterogeneous analytical systems: Architectures, methods, and interoperability challenges. Information, 16(11), 932. https://doi.org/10.3390/info16110932

Kovach, A., Montalvillo, L., Lanza, J., Sotres, P., & Urbieta, A. (2026). Understanding data spaces: A systematic mapping study of foundations, technical building blocks, and sectoral adoption. Computer Science Review, 53, 100819. https://doi.org/10.1016/j.cosrev.2025.100819

Ogrizović, M., Drašković, D., & Bojić, D. (2024). Quality assurance strategies for machine learning applications in big data analytics: An overview. Journal of Big Data, 11, 156. https://doi.org/10.1186/s40537-024-01028-y

Saudi Data & AI Authority. (2023). Data management and personal data protection standards. https://sdaia.gov.sa/ndmo/Files/PoliciesEn001.pdf

Saudi Data & AI Authority. (2023). Personal Data Protection Law (English version). https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

Saudi Data & AI Authority. (2024). Guidelines for binding common rules for personal data transfer. https://sdaia.gov.sa/Documents/CommonRulesBCRForPersonalDataTransferEN.pdf

Saudi Data & AI Authority. (2024). Personal data breach incidents procedural guide. https://sdaia.gov.sa/en/SDAIA/about/Documents/PersonalDataBreachIncidents.pdf

Saudi Data & AI Authority. (2024). Rules for appointing personal data protection officer. https://sdaia.gov.sa/en/SDAIA/about/Documents/RulesforAppointingPersonalDataProtectionOfficer.pdf

Saudi Data & AI Authority. (2024). Standard contractual clauses for personal data transfer. https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf

Saudi Data & AI Authority. (2024). State of AI in Saudi Arabia. https://sdaia.gov.sa/en/MediaCenter/KnowledgeCenter/ResearchLibrary/StateofAIinSaudiArabia.pdf

Saudi Data & AI Authority. (2024). The rules governing the national register of controllers within the Kingdom. https://sdaia.gov.sa/Documents/TheRulesGoverningTheNationalRegisterOfControllersWithinTheKingdomPublicEN.pdf

Saudi Data & AI Authority. (2025). Artificial Intelligence Adoption Framework. https://sdaia.gov.sa/en/SDAIA/about/Files/AIAdoptionFramework.pdf

Saudi Data & AI Authority. (2025). FAQs for operational excellence. https://sdaia.gov.sa/en/Research/Documents/FAQsforOperationalExcellence.pdf

Saudi Data & AI Authority. (2025). National Data Index operational excellence (Version 2.0). https://sdaia.gov.sa/en/Research/Documents/OperationalExcellencev2.0.pdf

Saudi Vision 2030. (2025). Vision 2030 annual report 2024. https://www.vision2030.gov.sa/en/annual-reports

Tonnarelli, M., Kumara, I., Driessen, S., Tamburri, D. A., van den Heuvel, W.-J., & Oor, P. (2025). Data catalog tools: A systematic multivocal literature review. Journal of Systems and Software, 230, 112584. https://doi.org/10.1016/j.jss.2025.112584

Volz, F., Münch, C., Lohmüller, M., & Küffner, C. (2025). From data jungle to data governance in digital ecosystems: Empirical evidence from a multiple holistic case study. Journal of Business Research, 196, 115747. https://doi.org/10.1016/j.jbusres.2025.115747

Yang, W. (2025). The impact of modern AI in metadata management. Human-Centric Intelligent Systems, 5, 323–350. https://doi.org/10.1007/s44230-025-00106-5

Zakharchenko, A. (2026). Integrating continuous compliance into DevSecOps pipelines: A data engineering perspective. Software, 5(1), 6. https://doi.org/10.3390/software5010006

APPENDIX A. INDICATOR DICTIONARY

Appendix A provides an indicator dictionary with definitions, formulas, reporting frequency, criticality treatment, and policy references. It is designed as a practical implementation aid for a first-phase pilot.

Indicator	Definition	Formula	Frequency	Leading/Lagging	Criticality	Policy reference
Ownership completeness	Datasets with named business owner and steward	Owned datasets / datasets in scope x 100	Monthly	Leading	Critical and non-critical	NDMO standards; NDI OE
Catalog registration	Datasets registered in approved catalog	Registered datasets / datasets in scope x 100	Monthly	Leading	Critical first	NDMO standards
Classification coverage	Datasets with approved sensitivity/classification tag	Classified datasets / datasets in scope x 100	Monthly	Leading	Mandatory for sensitive and critical	PDPL; NDMO standards

Freshness compliance	Datasets updated within service-level window	In-SLA datasets / datasets in scope x 100	Daily/weekly	Leading	Higher threshold for critical	NDI OE; service-level governance
Lineage coverage	Critical datasets with verified upstream and downstream lineage	Verified critical datasets / total critical datasets x 100	Weekly	Leading	Mandatory for critical	NDMO standards; AI accountability
AI traceability coverage	AI use cases linked to approved data and owner metadata	Traceable AI use cases / AI use cases x 100	Monthly	Leading	Mandatory when AI materially affects decisions	State of AI; AI Adoption Framework
Access review completion	Scheduled access reviews completed on time	Completed reviews / scheduled reviews x 100	Monthly/quarterly	Leading	More frequent for sensitive assets	PDPL; DGA governance & compliance
Dormant privilege ratio	Privileged accounts not recently used	Dormant privileged accounts / total privileged accounts x 100	Monthly	Leading	Escalate for critical systems	PDPL; security controls
Evidence completeness	Required control evidence available and retrievable	Available evidence / required evidence x 100	Monthly	Leading	Near-total for critical controls	NDI OE; audit readiness
Overdue remediation	Open corrective actions past due	Overdue actions / open actions x 100	Weekly/monthly	Lagging	Shorter tolerance for critical	NDI OE; DGA governance
Recurring audit finding rate	Findings repeated from prior review cycle	Repeated findings / total findings x 100	Quarterly	Lagging	Immediate escalation for critical	NDI OE; internal audit
Audit retrieval time	Median time to retrieve evidence for a sampled control	Median minutes or hours	Quarterly	Lagging	Used as outcome metric in pilot	Evidence-based governance target

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Mazhar, C. B. (2026). NATIONAL-SCALE DATA GOVERNANCE DASHBOARDS: REAL-TIME QUALITY, LINEAGE, ACCESS, AND COMPLIANCE FOR SAUDI ARABIA (SDAIA-ALIGNED). *Veredas Do Direito*, 23(5), e235431. https://doi.org/10.18623/rvd.v23.5431