World Journal of Information Systems 3(3) 63-78
DOI: https://doi.org/10.17013/wjis.v3i3.68

Article

Data Governance Barriers to Reliable Decision Support in Brazil's Public Sector

Mauricio Loureiro Ramos[1], Antonio Augusto Gonçalves[1],* Sandra R. F. S. Morgado de Gois[1], Sandro Luis Freire de Castro Silva[2], Jander Vinicius Pereira[1], and Francisco Santos Sabbadini[3]

[1] Universidade Estácio de Sá, Rio de Janeiro, Brazil

[2] Universidade Federal do Estado do Rio de Janeiro (UNIRIO), Rio de Janeiro, Brazil

[3] Universidade do Estado do Rio de Janeiro (UERJ), Rio de Janeiro, Brazil

* Correspondence: augusto@inca.gov.br

(Article history: Received June 12, 2026; Received in revised form July 24, 2026; Accepted August 20, 2026; Available online September 15, 2026)

Abstract: Reliable decision support in public organizations depends less on the sophistication of dashboards than on the governance of the data that feed them. This study examines how data-governance barriers undermine Decision Support Systems (DSS) in Brazil's public sector. Evidence from experienced information technology managers and coordinators in federal and state organizations identifies six interconnected barriers: limited data-governance awareness, resistance to change, capability gaps and staff turnover, fragmented responsibilities and policies, legacy-system and infrastructure constraints, and difficulties operationalizing security and privacy requirements. The findings show that these barriers do not act independently. Fragmented accountability weakens standards and ownership; turnover erodes institutional memory; legacy environments intensify manual reconciliation; and weak governance awareness reduces adherence to metadata, quality, and access routines. These mechanisms propagate into inconsistent definitions, duplicated records, limited traceability, delayed access, and reduced integration, directly lowering managerial trust in DSS outputs. The analysis advances a barrier-interaction model and a three-stage capability roadmap—stabilize, standardize and integrate, and institutionalize and scale—centered on stewardship, metadata, data quality, interoperability, leadership sponsorship, and auditable access. The study shows that DSS reliability is an organizational governance outcome, not merely a technical property of information systems. For public managers, the results indicate that trustworthy decision support can be strengthened by prioritizing critical data and institutionalizing governance routines before expanding technology investments.

© 2026 ITMA. All rights reserved.

Keywords: data governance; public sector; decision support systems; Brazil; data quality; institutional capacity

1. Introduction

Governments increasingly rely on data to design services, allocate resources, monitor programs, and demonstrate accountability. The data-driven public sector is therefore not simply a technologically advanced administration; it is an institutional arrangement in which data are treated as a strategic asset throughout the policy and service life cycle [1]. This distinction matters because the availability of databases, dashboards, and analytics platforms does not by itself guarantee reliable evidence. Public value depends on whether organizations can define responsibilities, agree on meanings, document provenance, control access, assure quality, and sustain these practices across organizational boundaries and political transitions.

Data governance provides the decision rights, accountabilities, policies, standards, and control mechanisms through which these conditions are established. A widely used conceptual synthesis defines data governance as the exercise of authority and control over the management of data [2]. Earlier information-systems research similarly emphasizes decision domains such as data principles, quality, metadata, access, and life-cycle responsibilities [3]. In practice, governance connects strategic objectives to operational work: it determines who may define a critical data element, who is responsible for correcting an error, which standards apply when systems exchange records, and which evidence is retained to explain an analytical result.

This connection is especially important for Decision Support Systems (DSS). Dashboards and analytical applications transform data into indicators and comparisons that managers use to interpret situations and select courses of action. Their apparent precision, however, can conceal weak definitions, duplicated records, inaccessible sources, or undocumented transformations. Information governance scholarship has therefore argued that the information artifact itself must be governed, not merely the technology that stores or processes it [4]. When governance is weak, a DSS can scale inconsistency: the system produces outputs rapidly, but different units may still dispute which number is authoritative. Trustworthy decision support depends on the organizational capacity to make data interpretable, traceable, secure, and fit for purpose [5].

The public-sector setting adds distinctive challenges. Government data are distributed among agencies with different mandates, legal bases, professional communities, budgets, technologies, and degrees of autonomy. A whole-of-government digital strategy consequently requires both common rules and mechanisms that allow adaptation to specific policy domains [6]. In addition, emerging uses of artificial intelligence intensify the need for reliable data lineage and accountability. Trustworthy automated or augmented decisions require governance arrangements that clarify responsibility for data inputs, models, access,

© 2026 ITMA. All rights reserved.

quality, and redress [7]. Data governance is thus a precondition for advanced analytics rather than a documentation exercise performed after implementation.

Brazil offers a particularly relevant context. The country has expanded digital government, open-data initiatives, and data-protection regulation, while its federal structure and administrative diversity create substantial coordination demands. Institutional analysis has shown that Brazilian data governance is shaped by rules-in-use, interorganizational arrangements, and incentives that are not reducible to formal policy design [8]. Studies of open government data have also identified organizational fragmentation, limited capabilities, and discontinuity as causes of initiative failure [9]. These findings suggest that barriers are not independent items on a checklist; they may reinforce one another and create self-sustaining patterns of low trust and limited use.

The analysis strengthens the link between data governance and DSS reliability by treating governance as part of organizational transformation rather than as a matter of technology adoption alone [10,11]. It also provides a more explicit account of sampling, coding, triangulation, and quality procedures, while moving beyond a descriptive inventory to examine how barriers interact and affect data quality, access, integration, and managerial trust. These relationships are then translated into a staged governance capability roadmap for institutions with uneven maturity and constrained resources. The discussion also considers the operational implications of Brazil's data-protection framework [12] and the role of data literacy in translating governance arrangements into a data-driven culture [13].

The study addresses three research questions: RQ1: How do technical and organizational barriers to data governance manifest in Brazilian public organizations? RQ2: Through which mechanisms do these barriers affect the reliability and use of DSS? RQ3: Which governance practices emerge as feasible levers for improving DSS effectiveness and institutional continuity? By answering these questions, the article contributes to information-systems research on the institutionalization of data governance and provides public managers with an implementation logic that starts from accountability and critical data rather than from the acquisition of additional tools.

2. Methodology

2.1. Research design and context

The study adopted an exploratory qualitative design to investigate how data-governance barriers are experienced and interpreted by managers responsible for information systems in Brazilian public institutions. Qualitative inquiry was appropriate because governance outcomes depend on formal arrangements and on less visible practices, including negotiation over definitions, informal control of information, resistance to new routines, and the preservation or loss of institutional memory. These mechanisms cannot be adequately reconstructed from maturity scores alone. The unit of analysis was the organizational

© 2026 ITMA. All rights reserved.

experience of implementing or sustaining data-governance practices in federal and state public organizations.

Digital transformation research distinguishes the introduction of digital technologies from the organizational changes required to use them effectively [10,11]. Consistent with that distinction, interview questions did not assume that a new platform represented governance progress. Participants were asked to describe concrete situations involving responsibility for data, policy implementation, data quality, system integration, access, privacy, security, staffing, leadership, and the use of information in managerial decisions. DSS were defined as dashboards, reporting suites, analytics portals, and related systems used to query, analyze, visualize, or compare operational and administrative data for tactical or strategic decisions.

2.2. Participants and data collection

Participants were selected purposively because they held direct responsibility for information technology, data management, integration, analytics, or related governance activities. The sample comprised 18 managers and coordinators from federal and state organizations. Professional experience ranged from 10 to more than 22 years, and time in the current role ranged from 6 to more than 15 years. This profile provided access to both current implementation problems and longer-term patterns of administrative continuity and change. Recruitment and interviewing continued until additional accounts no longer altered the central thematic structure. The claim is one of thematic sufficiency for the study's analytic purpose, not statistical representation of the Brazilian public sector.

Semi-structured interviews were conducted between September and November 2024 and lasted approximately one hour. The guide covered five domains: (1) data-management practices; (2) governance policies, roles, and structures; (3) organizational culture and change; (4) technical infrastructure and interoperability; and (5) information security and privacy. Open questions were followed by requests for examples, consequences, and attempted responses. This approach helped distinguish general opinions from events participants had observed in their professional routines. Interviews were transcribed verbatim for analysis.

Table 1. Profile of interview participants.

Institutional level	Position	Professional experience	Years in current position
Federal	IT Manager	15+ years	10+ years
Federal	IT Manager	12 years	8 years
State	IT Manager	18 years	11 years
Federal	IT Coordinator	14 years	9 years
Federal	IT Manager	20 years	12 years
State	IT Manager	10 years	7 years
Federal	IT Manager	16 years	10 years

© 2026 ITMA. All rights reserved.

Institutional level	Position	Professional experience	Years in current position
Federal	IT Manager	22 years	15 years
State	IT Manager	13 years	9 years
Federal	IT Coordinator	17 years	11 years
Federal	IT Manager	19 years	12 years
State	IT Manager	11 years	6 years
Federal	IT Manager	15 years	10 years
Federal	IT Manager	21 years	14 years
Federal	IT Coordinator	18 years	12 years
State	IT Manager	12 years	8 years
Federal	IT Manager	20 years	13 years
State	IT Manager	14 years	9 years

2.3. Analytical procedure and trustworthiness

The transcripts were analyzed in NVivo 12 through an iterative thematic procedure informed by the principles of systematic coding and constant comparison [14]. Analysis began with open coding close to participants' language. Initial codes captured reported conditions, actions, interpretations, and consequences, such as unclear ownership, duplicate datasets, manual access control, resistance to process redesign, delayed procurement, and loss of expertise after staff turnover. Codes were then compared across interviews and grouped into higher-order barrier categories. The developing categories were examined in relation to data-governance concepts and DSS consequences, while preserving a distinction between participant evidence and the researchers' theoretical interpretation.

A second analytical pass focused on relationships among categories. For each barrier, the researchers asked: What organizational mechanism does this barrier activate? Which property of data is affected? What consequence follows for DSS use? This relational analysis transformed a descriptive inventory into an explanatory chain linking institutional conditions to coordination failures, inconsistent controls, reduced data quality or accessibility, and lower trust in decision outputs. The procedure is compatible with qualitative approaches that move from first-order observations to more abstract mechanisms while maintaining an auditable connection to empirical material [15].

Several measures strengthened trustworthiness. Two researchers independently coded 20% of the interviews, compared interpretations, and reconciled differences through discussion before stabilizing the codebook. Successive codebook versions, coding decisions, and analytical notes were retained as an audit trail. Data triangulation compared accounts across federal and state settings; documentary triangulation considered institutional reports and applicable digital-governance and data-protection frameworks; and researcher triangulation subjected categories and interpretations to peer review. Disconfirming or more positive cases were examined to avoid treating all institutions as equally constrained. These procedures support credibility, dependability, and analytic transferability [16].

© 2026 ITMA. All rights reserved.

Participation was voluntary, informed consent was obtained, and transcripts were anonymized. Institutional identifiers were removed, and quotations were selected to illustrate themes without revealing organizations or individuals. The Brazilian General Data Protection Law (LGPD) informed the study's attention to privacy, security, lawful processing, and accountability [12]. Only the minimum participant-profile information required to explain the sample was retained in the manuscript.

The study has two methodological boundaries. First, the evidence represents the perceptions of experienced IT managers and coordinators rather than a direct audit of systems, data quality, or organizational compliance. Second, coding frequencies are used only to show relative salience within the qualitative material. They are not prevalence estimates and should not be generalized to all Brazilian public organizations. The value of the design lies in explaining mechanisms and identifying transferable governance responses.

3. Results and Discussion

3.1. Relative salience of the barrier clusters

The analysis identified six recurring barrier clusters. Limited awareness of data governance and cultural resistance to change were most salient, followed by specialized knowledge gaps, fragmented responsibilities, infrastructure complexity, and difficulties operationalizing security and privacy. Figure 1 presents the indicative frequency summary of the qualitative coding. The counts should be read as signals of thematic emphasis, not as mutually exclusive participant categories: a single account could connect several barriers, and the significance of a theme depended on its mechanism and consequences as well as its frequency.

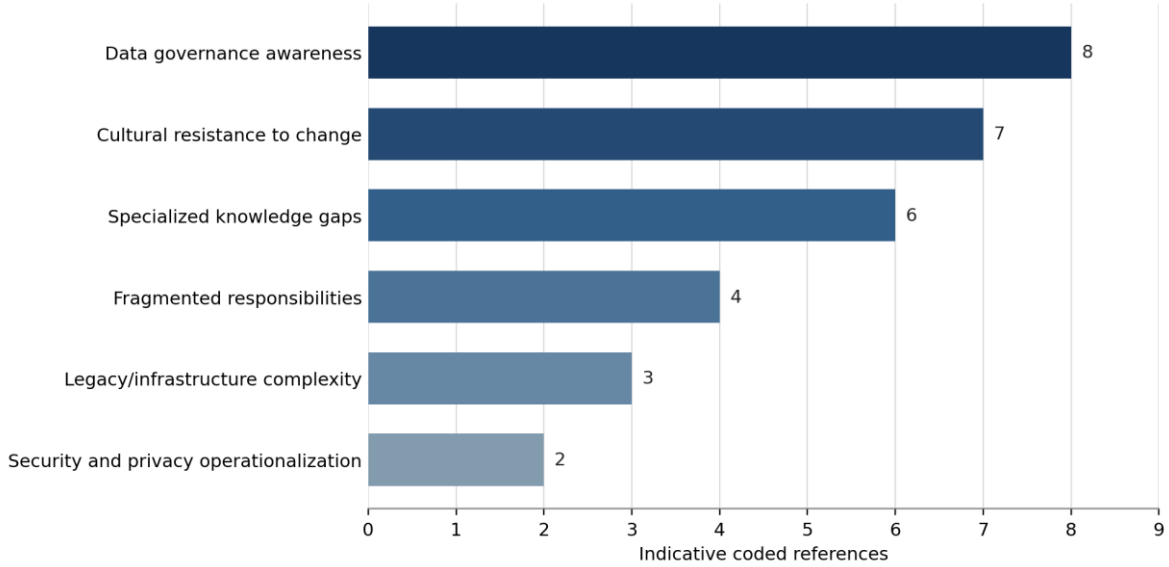


Figure 1. Indicative coded references to the six barrier clusters. Frequencies summarize the qualitative coding and are not statistical prevalence estimates.

© 2026 ITMA. All rights reserved.

The distribution immediately challenges a technology-first interpretation. Infrastructure was consequential, but managers more often described barriers involving meaning, responsibility, incentives, leadership, and acceptance of changed work practices. This pattern is consistent with the view that digital transformation requires organizational redesign rather than technology substitution [10,11]. It also aligns with evidence that data literacy contributes to the development of a data-driven culture in public service organizations [13]. The remaining subsections examine how each cluster operated and how the clusters reinforced one another.

3.2. Fragmented responsibilities and weak policy institutionalization

The first mechanism was ambiguity over who had authority to define, correct, approve, and share data. Participants described governance responsibilities distributed across departments without a common operating model. One manager noted that the institution lacked a well-defined and disseminated policy, including a shared understanding of the relevance of data-protection requirements. Another explained that an integrated access policy existed, but governance continued to be performed manually with limited tools. The contrast between formal policy and operational practice was central: documents could establish intentions without creating stewardship routines, escalation paths, or enforceable standards.

Fragmented accountability produced several observable consequences. Different units maintained parallel versions of the same dataset; data corrections were local rather than propagated to downstream systems; business definitions varied across reports; and managers could not readily identify an authoritative source. These problems slowed decisions because time was spent reconciling numbers before substantive analysis could begin. They also weakened accountability: when no role owned a critical data element end to end, quality failures were treated as technical incidents rather than governance failures.

For DSS, the result was semantic inconsistency. A dashboard can accurately execute a query and still mislead if units disagree about the meaning of an indicator, its time window, exclusions, or source. The findings therefore reinforce the distinction between system availability and information reliability. Formal committees become useful only when they have decision rights, named stewards, a manageable scope of critical data, and a process for resolving contested definitions. The Brazilian institutional context makes this particularly important because data sharing crosses organizational mandates and administrative levels [8].

3.3. Cultural resistance, awareness, and control over information

Resistance was not limited to discomfort with unfamiliar software. Participants connected it to established routines, professional identities, and control over information. One manager described opposition to an analytics project after it reduced privileged access to data; challenges to accuracy and provenance became a means of contesting the

© 2026 ITMA. All rights reserved.

redistribution of informational power. Another participant reported acceptance only when technology reproduced the former paper process exactly. In both cases, the object of resistance was a change in accountability or work design, not the interface itself.

Low awareness amplified this resistance. Where data governance was perceived as an IT responsibility or an additional compliance layer, employees had little reason to invest effort in metadata, quality checks, classification, or access-review routines. Senior leadership behavior was decisive. Participants reported that initiatives lost momentum when leaders endorsed governance rhetorically but did not follow up on decisions, allocate time, resolve interdepartmental disputes, or use governed information in their own meetings. Conversely, digital-governance committees and cross-functional working groups increased visibility and gave non-IT units a place in the decision process. This emphasis on leadership is consistent with evidence that leadership shapes digital-transformation performance [17].

These accounts suggest that promoting a data-driven culture requires more than a general commitment to data use. Culture was produced through repeated practices: which figures leaders requested, whether disputed definitions were resolved, whether quality incidents were recorded, and whether staff were recognized for stewardship work. Training is necessary but insufficient when governance tasks remain unrewarded or conflict with local incentives. Data literacy and governance sponsorship must therefore be linked. Employees need to understand the value and limits of data, while leaders must make the use of agreed definitions and quality evidence part of normal managerial accountability [13].

3.4. Capability gaps, turnover, and the erosion of institutional memory

Participants identified shortages of specialized knowledge spanning data quality, architecture, metadata, security, privacy, integration, and governance design. These are hybrid capabilities: they require technical competence and an understanding of administrative processes, legal mandates, and policy domains. Hiring constraints and dependence on a small number of experienced employees made organizations vulnerable. When these employees changed positions, retired, or left, undocumented knowledge about datasets, interfaces, exceptions, and historical decisions was lost.

Turnover converted an individual capability problem into an institutional continuity problem. Projects stalled while new teams reconstructed decisions; temporary solutions became permanent because their rationale was not documented; and vendors sometimes held more knowledge of integration logic than the contracting institution. Participants' accounts also indicated variation rather than a simple generational divide. Newer staff were often more receptive to governance practices, but receptiveness did not substitute for domain knowledge. Sustainable capability required communities of practice, role-based learning, documentation, and succession arrangements that connect experienced domain specialists with technical teams.

For DSS, the practical consequence is slower diagnosis of problems and more fragile maintenance. When a report changes unexpectedly, managers need people who can trace the

© 2026 ITMA. All rights reserved.

result from a business definition through transformations to a source system. Without lineage documentation and retained expertise, analytical errors are difficult to distinguish from legitimate changes in the underlying phenomenon. Institutional memory should therefore be treated as part of data governance. Code repositories, data catalogs, decision logs, business glossaries, and documented quality rules reduce dependence on individual memory, but only if maintaining them is an assigned responsibility rather than an optional task.

3.5. Legacy systems, interoperability, and resource constraints

Technological heterogeneity constrained governance even when policy and leadership were favorable. Managers described legacy systems with inconsistent identifiers, incompatible formats, limited interfaces, and weak documentation. Budget restrictions delayed modernization, while procurement cycles and vendor dependence reduced flexibility. These conditions increased the amount of manual reconciliation required and made it difficult to implement common controls across the data life cycle. A governance policy that assumes modern interfaces and centralized metadata may therefore remain aspirational in a mixed legacy environment.

The accounts included more mature cases. Some organizations had robust storage, security, cloud arrangements, and experience sharing data projects. These cases are analytically important because they show that infrastructure can reduce, but does not eliminate, governance barriers. Technical capacity created options for integration and monitoring; effective use still depended on ownership, standards, and coordination. The comparison suggests a complementarity relationship: organizational governance without enabling infrastructure becomes manual and fragile, whereas infrastructure without governance accelerates the production and distribution of inconsistencies.

Resource constraints also require prioritization. An institution does not need to modernize every system before improving DSS reliability. It can begin with a limited set of high-value decisions and trace the critical data elements that support them. For these elements, the organization can define owners and stewards, document lineage, establish quality thresholds, and create controlled integration routines. This decision-centered approach concentrates scarce capacity where errors or delays have the greatest administrative and public consequences.

3.6. Security and privacy as operational governance

Managers recognized the LGPD as a clear normative reference, but they reported uncertainty in translating legal principles into everyday classifications, access decisions, retention routines, and monitoring. The barrier was therefore not the absence of law. It was the gap between legal obligation and repeatable operational control. Institutions struggled to identify which datasets required priority protection, who could authorize access, how permissions should be reviewed, and how compliance evidence should be retained.

© 2026 ITMA. All rights reserved.

Security and privacy were sometimes framed as constraints on data sharing, producing a false choice between protection and use. Mature governance instead makes legitimate use possible by documenting purpose, classification, lawful access, and accountability. For DSS, poorly designed restrictions can be as damaging as uncontrolled access: managers may receive delayed, incomplete, or manually transformed data, while analysts create unofficial copies to meet deadlines. Governance should therefore integrate privacy, security, access, and usability rather than assigning them to isolated control functions.

Operational controls are therefore most useful when they are tied to data classes and decision contexts. Critical datasets should have documented purposes, custodians, access criteria, review intervals, and incident procedures. Metadata should identify sensitivity and permitted uses, while logs provide evidence of access and transformation. This approach reduces discretionary, case-by-case decisions and supports both compliance and responsible analysis. It is also essential for trustworthy artificial intelligence, whose outputs depend on the provenance, representativeness, and authorized use of training and operational data [7].

3.7. How barriers interact to weaken DSS reliability

Taken together, the evidence indicates that the barriers formed reinforcing chains rather than isolated obstacles. Fragmented roles allowed inconsistent definitions to persist. Low awareness reduced participation in corrective routines. Turnover removed the tacit knowledge needed to interpret legacy data. Infrastructure constraints encouraged manual workarounds, and uncertainty about privacy encouraged either excessive restriction or uncontrolled copies. Together, these conditions reduced data quality, accessibility, integration, and traceability. Managers then encountered conflicting or delayed DSS outputs and became less willing to rely on the systems, which further weakened incentives to invest in governance.

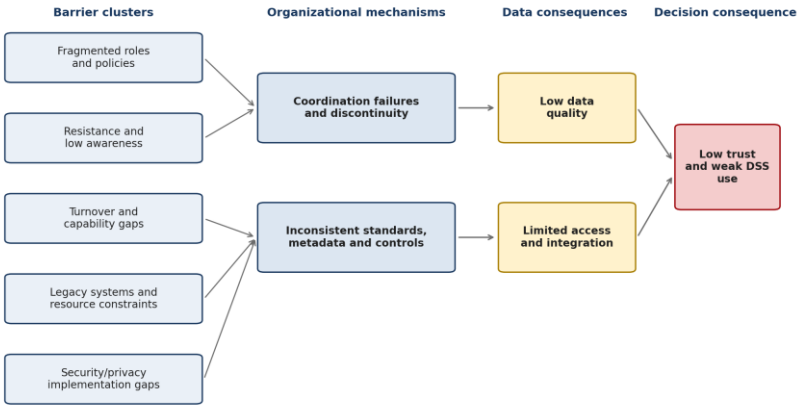


Figure 2. Barrier-interaction model linking institutional conditions to data consequences and reduced trust in Decision Support Systems. Developed from the relational analysis of interview themes.

© 2026 ITMA. All rights reserved.

Figure 2 expresses this mechanism. Barrier clusters influence DSS indirectly through organizational processes and properties of data. This distinction helps explain why replacing a dashboard or database often disappoints: the intervention occurs at the visible end of the chain while leaving decision rights, definitions, expertise, integration, and control routines unchanged. It also identifies leverage points. Clarifying stewardship can reduce fragmentation; documenting lineage can mitigate turnover; common identifiers can reduce integration errors; and leadership use of governed indicators can strengthen awareness and compliance.

The mechanism also explains a negative feedback loop. When DSS outputs are disputed, managers return to spreadsheets, personal contacts, and local data extracts. These workarounds may solve an immediate task but create additional versions, undocumented transformations, and access risks. The next DSS result becomes even harder to reconcile. Breaking the loop requires visible evidence that governance improves decisions: fewer reconciliation cycles, shorter time to obtain a trusted indicator, reduced duplication, or a documented resolution of quality incidents. Such measures make governance performance observable to leaders and users.

Table 2. Cross-theme synthesis of barriers, mechanisms, DSS consequences, and governance responses.

Barrier cluster	Mechanism	Consequence for DSS	Feasible governance response
Low awareness	Governance seen as IT or compliance work	Metadata and quality routines receive low priority	Leaders use governed indicators; role-based data literacy; visible quality metrics
Cultural resistance	New controls alter routines and informational power	Unofficial sources and contested results	Co-design processes; clarify decision rights; manage incentives and change impacts
Capability gaps and turnover	Tacit knowledge leaves with individuals	Weak lineage, delayed diagnosis, fragile maintenance	Communities of practice; succession; catalogs; decision and transformation logs
Fragmented roles and policies	No end-to-end ownership of critical data	Competing definitions and duplicate records	Named owners/stewards; glossary; issue escalation; committee with decision authority
Legacy/infrastructure constraints	Heterogeneous identifiers, formats, and interfaces	Manual reconciliation and delayed integration	Prioritize critical data; canonical identifiers; staged interfaces; quality gates
Security/privacy implementation gaps	Rules are not converted into repeatable controls	Over-restriction, shadow copies, or inappropriate access	Classification, purpose and access metadata; periodic review; logging and incident procedures

3.8. A staged capability roadmap for public organizations

The findings do not support a single, comprehensive transformation launched simultaneously across the institution. They support a staged capability strategy that aligns governance scope with organizational capacity. Stage 1 establishes minimum accountability

© 2026 ITMA. All rights reserved.

around a small set of decision-critical data. Stage 2 standardizes and integrates the practices that have demonstrated value. Stage 3 institutionalizes monitoring, cross-organizational coordination, and advanced analytics governance. Each stage should produce evidence useful to DSS users, not merely new policy documents.

Table 3. Staged roadmap from minimum accountability to institutionalized data governance.

Stage	Priority actions	Core outputs	Expected DSS effect
Stage 1: Stabilize	Select high-value decisions and critical data; name owner and steward; agree definitions; record sources and access; establish a quality-issue log	Authoritative definitions; responsibility matrix; initial lineage; baseline quality measures	Less time reconciling critical indicators
Stage 2: Standardize and integrate	Expand glossary/catalog; implement quality rules; adopt common identifiers; formalize access reviews; document interfaces and transformations	Reusable metadata; quality dashboards; controlled integration; auditable access	More consistent and timely DSS outputs
Stage 3: Institutionalize and scale	Embed governance in planning and performance; maintain communities of practice; monitor value and risk; coordinate across organizations; govern AI-ready data	Sustained stewardship network; cross-government agreements; continuous assurance	Trusted decision support across programs and transitions

The roadmap operationalizes the OECD emphasis on leadership, rules, architecture, infrastructure, and capabilities while adapting it to the constraints reported by participants [1,6]. The first stage is deliberately narrow: broad governance programs often lose credibility when they attempt to catalog every dataset or define enterprise-wide standards before demonstrating value. A decision-centered pilot makes the relationship between data work and managerial outcomes visible. Subsequent scaling should reuse standards and learning from the pilot while allowing domain-specific variation. This staged logic is consistent with information-management roadmaps that progressively build governance capabilities [18].

Governance performance should be evaluated with measures that connect operational practice to information use. Examples include the percentage of critical elements with named stewards, time to resolve quality incidents, proportion of DSS indicators with documented definitions and lineage, time required to approve legitimate access, number of competing versions retired, and user confidence in authoritative sources. These measures do not replace evaluation of policy or service outcomes, but they provide early evidence that the institutional conditions for trustworthy decisions are improving.

3.9. Implications for information-systems research and public management

From an information-systems perspective, the findings suggest that DSS success models should treat governed data as an organizational accomplishment rather than as a fixed input. Conventional evaluations often measure information quality, system quality, use, satisfaction, or decision impact at one point in time. The interviews indicate that information

© 2026 ITMA. All rights reserved.

quality is continuously produced through stewardship, interpretation, correction, access negotiation, documentation, and maintenance. These activities are distributed across technical and business units and are vulnerable to turnover and changes in leadership. A DSS may therefore remain technically unchanged while its reliability deteriorates because the governance arrangements surrounding its data have weakened.

The barrier-interaction model also provides propositions for subsequent testing. Clear ownership should be positively associated with agreement on indicator definitions and shorter quality-incident resolution times. Lineage completeness should weaken the negative effect of staff turnover on DSS reliability. Data literacy should strengthen the relationship between formal governance mechanisms and the actual use of governed information. Legacy complexity should intensify the effect of fragmented responsibility on reconciliation effort, while leadership use of agreed indicators should reduce reliance on shadow datasets. These propositions translate qualitative mechanisms into variables that can be examined across organizations without reducing governance to a single maturity score.

For public management, an important distinction is between compliance and institutionalization. Compliance concerns whether a policy, committee, or control exists, whereas institutionalization concerns whether that arrangement repeatedly shapes decisions, survives personnel changes, and resolves conflicts among units. This distinction is important in settings where organizations can produce formal governance artifacts but lack the capacity or incentives to maintain them. Oversight should therefore examine evidence of use: stewardship decisions, resolved definition disputes, access-review records, data-quality remediation, lineage coverage, and the incorporation of governed indicators into planning and performance meetings.

Interorganizational coordination is another implication. Many public decisions depend on data created outside the unit that analyzes them. An organization can improve internal controls and still receive ambiguous, delayed, or inconsistent inputs. Bilateral exchanges based on personal relationships are especially vulnerable to turnover. Where feasible, agencies should formalize shared definitions, responsibilities, service expectations, change-notification procedures, and lawful-use conditions. Common metadata and identifiers should be governed as shared institutional infrastructure. This does not require eliminating local autonomy; it requires making variation explicit and preventing unrecorded differences from appearing as comparable data.

Governance is also better understood as a public-value capability. The immediate benefits may appear operational—less duplication, faster reconciliation, controlled access, and more stable reporting—but these improvements affect policy design, service delivery, accountability, and trust. A governance initiative is more likely to retain leadership support when it demonstrates this chain of value. Business cases should connect a critical decision to its data dependencies, current failure costs, proposed controls, expected improvement, and responsible roles. Such cases make governance choices contestable and transparent, while avoiding claims that all data have equal value or require the same level of control.

© 2026 ITMA. All rights reserved.

4. Conclusion

This study examined how barriers to data governance manifest in Brazilian public organizations and how they affect Decision Support Systems. The evidence shows that the main challenge is not a simple shortage of technology. Governance initiatives weaken when responsibilities are fragmented, leadership support is intermittent, employees do not see data work as strategically relevant, turnover removes institutional memory, legacy environments make controls difficult to apply, and privacy or security rules are not translated into workable routines. These barriers interact through coordination failures and inconsistent standards, reducing data quality, accessibility, integration, and traceability.

The theoretical contribution is a sociotechnical account of DSS reliability. Trust in decision support is not produced solely by model accuracy, system availability, or interface quality. It is produced upstream through decisions about ownership, meaning, provenance, access, quality, and accountability. The barrier-interaction model explains how institutional conditions become data problems and how data problems become hesitation, underuse, and reliance on unofficial workarounds. It therefore connects the data-governance literature to information-systems concerns with the credibility and practical use of decision artifacts.

The empirical contribution lies in situated evidence from 18 experienced managers and coordinators working across Brazilian federal and state contexts. Their accounts reveal a recurrent gap between formal governance and daily practice. They also show variation: organizations with stronger infrastructure and collaborative mechanisms had more favorable conditions, but technical maturity did not remove the need for stewardship and leadership. The analysis cautions against treating the public sector as homogeneous while identifying mechanisms that may be transferable to other multi-level administrative systems.

For practice, the study recommends beginning with a small set of high-value decisions and the critical data that support them. Public organizations should assign owners and stewards, agree on definitions, document lineage, establish quality and access routines, and measure whether these changes reduce reconciliation and improve confidence in DSS outputs. Scaling should then integrate metadata, common identifiers, quality controls, access reviews, communities of practice, and cross-organizational agreements. This sequence treats governance as an institutional capability that must survive personnel and political transitions.

The study is limited by its reliance on managerial accounts and by the absence of direct measures of data quality or DSS performance. Coding frequencies indicate thematic salience within the material but do not estimate prevalence. Future research should combine interviews with audits of metadata, lineage, access, and quality incidents; compare managers, frontline users, policy units, privacy officers, and external stakeholders; and follow governance initiatives longitudinally across leadership transitions. Comparative studies could test whether the interaction mechanisms identified here operate similarly in municipal, federal, and cross-national settings. Quantitative work could examine whether stewardship coverage, lineage completeness, or quality-incident resolution predicts DSS use and trust.

© 2026 ITMA. All rights reserved.

Ultimately, trustworthy public-sector decision support depends on the capacity to make governance routine. Policies and platforms are necessary, but they create value only when responsibilities are enacted, knowledge is retained, standards are negotiated, controls are usable, and leaders consistently rely on governed information. Under these conditions, data become more than stored records: they become an accountable institutional resource for decisions and services that citizens can trust.

Funding: This research received no external funding.

Data Availability Statement: Interview transcripts are not publicly available because they contain potentially identifying organizational and professional information. An anonymized codebook or aggregate thematic materials may be made available by the corresponding author upon reasonable request, subject to ethical and legal constraints.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] OECD. The Path to Becoming a Data-Driven Public Sector; OECD Digital Government Studies; OECD Publishing: Paris, France, 2019. https://doi.org/10.1787/059814a7-en.

[2] Abraham, R.; Schneider, J.; vom Brocke, J. Data governance: A conceptual framework, structured review, and research agenda. Int. J. Inf. Manag. 2019, 49, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

[3] Khatri, V.; Brown, C.V. Designing data governance. Commun. ACM 2010, 53, 148–152. https://doi.org/10.1145/1629175.1629210.

[4] Tallon, P.P.; Ramirez, R.V.; Short, J.E. The information artifact in IT governance: Toward a theory of information governance. J. Manag. Inf. Syst. 2013, 30, 141–178. https://doi.org/10.2753/MIS0742-1222300306.

[5] Brous, P.; Janssen, M. Trusted decision-making: Data governance for creating trust in data science decision outcomes. Adm. Sci. 2020, 10, 81. https://doi.org/10.3390/admsci10040081.

[6] OECD. The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government; OECD Public Governance Policy Papers, No. 02; OECD Publishing: Paris, France, 2020. https://doi.org/10.1787/f64fed2a-en.

[7] Janssen, M.; Brous, P.; Estevez, E.; Barbosa, L.S.; Janowski, T. Data governance: Organizing data for trustworthy artificial intelligence. Gov. Inf. Q. 2020, 37, 101493. https://doi.org/10.1016/j.giq.2020.101493.

[8] Filgueiras, F.; Lui, L. Designing data governance in Brazil: An institutional analysis. Policy Des. Pract. 2023, 6, 41–56. https://doi.org/10.1080/25741292.2022.2065065.

[9] Wiedenhöft, G.C.; Alexopoulos, C.; Saxena, S.; Rizun, N.; Matheus, R. Assessing the failure of Open Government Data initiatives in Brazil. Electron. J. Inf. Syst. Dev. Ctries. 2023, 89, e12286. https://doi.org/10.1002/isd2.12286.

[10] Mergel, I.; Edelmann, N.; Haug, N. Defining digital transformation: Results from expert interviews. Gov. Inf. Q. 2019, 36, 101385. https://doi.org/10.1016/j.giq.2019.06.002.

© 2026 ITMA. All rights reserved.

[11] Vial, G. Understanding digital transformation: A review and a research agenda. J. Strateg. Inf. Syst. 2019, 28, 118–144. https://doi.org/10.1016/j.jsis.2019.01.003.

[12] Brazil. Law No. 13,709 of 14 August 2018: General Personal Data Protection Law (LGPD). Available online: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (accessed on 27 August 2026).

[13] Fattah, I.A. The mediating effect of data literacy competence in the relationship between data governance and data-driven culture. Ind. Manag. Data Syst. 2024, 124, 1823–1845. https://doi.org/10.1108/IMDS-11-2023-0812.

[14] Braun, V.; Clarke, V. Using thematic analysis in psychology. Qual. Res. Psychol. 2006, 3, 77–101. https://doi.org/10.1191/1478088706qp063oa.

[15] Gioia, D.A.; Corley, K.G.; Hamilton, A.L. Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organ. Res. Methods 2013, 16, 15–31. https://doi.org/10.1177/1094428112452151.

[16] Lincoln, Y.S.; Guba, E.G. Naturalistic Inquiry; Sage: Beverly Hills, CA, USA, 1985.

[17] Geada, N.; Alturas, B. Performance in digital transformation: Focus group insights. World J. Inf. Syst. 2024, 1, 19–27.

[18] Martins, M.M.S.; Sousa, C.D.P.; Pereira, C.S.G.; Silva, B. A Dynamic Circularity Information Management Roadmap for Small and Medium Enterprises. World J. Inf. Syst. 2024, 1, 61–73. https://doi.org/10.17013/wjis.v1i2.14.

© 2026 ITMA. All rights reserved.