Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

When Does Interoperability Become Governance? Data, Authority, and Collaborative Accountability in Fragmented Public Service Systems

Muhtar (.)

muhtar@lecturer.unpatti.ac.id

Universitas Pattimura

Jusuf Madubun

Universitas Pattimura

Marno Wance

Universitas Pattimura

Research Article

Keywords: data interoperability, collaborative governance, collaborative accountability, digital government, public-service systems, Design Science Research

Posted Date: October 27th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11262587/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

This study investigates the point at which data interoperability transcends mere information exchange to perform governance functions in fragmented public service systems. It adopts theory-elaborating Design Science Research, with an emphasis on Indonesia's Free Nutritious Meal programme in Ambon. Evidence combines semi-structured interviews with three school-based adults and one student beneficiary, official policy and oversight records, process/data-format evidence, and controlled evaluation across 20 prototype scenarios. Rather than revealing an information deficit, the case shows fragmented meanings, differentiated decision rights, weak links between indicators and corrective action, and incomplete closure. Five mechanisms explain governance-bearing interoperability: semantic stabilisation, authority allocation, actionability, traceability, and accountable closure. The study distinguishes this concept from pragmatic interoperability by focusing on institutionally differentiated rights and obligations. It contributes reusable design principles for purpose-sensitive public-service interoperability while treating organisational recognition as the boundary condition separating governance-bearing design from institutionalised interoperability-as-governance. Theoretically, the study specifies a governance threshold: interoperability becomes governance-bearing only when shared meaning, differentiated authority, actionable obligation, reconstructable decision history, and authorised closure operate as a connected configuration. Empirically, the Ambon case shows that the decisive problem is not data scarcity but the institutional conversion of heterogeneous observations into recognised, role-differentiated, evidence-bearing decisions.

1. Introduction

"School feeding has become one of the world's largest public service and social protection infrastructures. School meal programmes are now in place for at least 466 million children globally, and the majority of these programmes are now funded by national governments (WFP, 2025). The scale of these programmes matters analytically because school meals are no longer treated solely as nutritional interventions. They increasingly connect education, health, social protection, food systems, local procurement, and public administration. As programmes expand, the governance problem shifts from whether meals can be delivered to whether multiple organisations can coordinate data, decisions, risks, and corrective actions across a service chain. The institutional demands for monitoring and evaluation have long been recognised in the research on school feeding, and it has been pointed out that responsibility is often divided among education, health, agriculture and other actors and that data systems are geared towards distinct service processes rather than integrated decision-making (Gelli & Espejo, 2013; Bicalho et al., 2021).

This global problem is brought into a rapidly expanding public-service setting by Indonesia's Free Nutritious Meal programme (Makan Bergizi Gratis; MBG). The national technical governance framework for fiscal year 2026 requires implementation to be orderly, effective, efficient, and accountable and assigns responsibilities across multiple organisational units (Badan Gizi Nasional, 2025). In Ambon, the problem is intensified by an island-city service environment in which school distribution, travel time, service radius, food condition, and last-mile coordination matter operationally. Rather than being a peripheral implementation detail, the local setting makes visible a wider question faced by networked public services: how can a programme be governed when operational information, professional expertise, and formal authority are distributed across organisations?

Field evidence from the Ambon study shows that the central difficulty was not the absence of information. Monitoring already occurred through WhatsApp, Microsoft Excel, Google Forms, web links, official administrative data, and direct communication. Schools reported issues concerning beneficiary-data reconciliation, delivery delays, portion variation, repetitive menus, food waste, allergy-related information, complaints, and uneven follow-up. Rather than an information-scarcity problem, the case revealed a coordination problem: data circulated, but the chain connecting data

to shared meaning, shared meaning to authority, authority to responsibility, and responsibility to verifiable corrective action remained incomplete.

This local pattern mirrors a central debate in digital-government research. Interoperability has often been framed as the capacity of heterogeneous systems to exchange and reuse information, yet public-sector integration repeatedly encounters organisational and institutional boundaries (Scholl & Klischewski, 2007). Sharing information across boundaries requires more than technical connectivity as actors are required to negotiate information boundaries, organisational interests, legal constraints and professional interpretations (Dawes et al., 2009). Likewise, empirical research shows that successful inter-organisational information sharing can be explained not only through technical compatibility but also through formally assigned organisational responsibilities and collaborative arrangements (Gil-Garcia & Sayogo, 2016). Recent work has therefore considered digital transformation as the co-evolution of technology, organisations and institutions and not only as digitisation (Luna-Reyes & Gil-Garcia, 2014; Mergel et al., 2019; Margariti et al., 2022).

However, this literature leaves an inverse question less developed. Most studies ask how governance arrangements enable interoperability: which institutional conditions, managerial capacities, standards, and organisational relationships make data integration possible. The reverse relationship is less explicit: under what conditions can interoperable arrangements themselves begin to structure governance? This distinction matters because a common database can increase visibility while leaving decision rights unresolved; a dashboard can display a red indicator without specifying who must respond; an alert can be generated without defining a deadline or escalation pathway; and a corrective action can be recorded without establishing who has authority to verify closure. Integrated information is therefore not equivalent to integrated government.

Collaborative-governance scholarship exposes the complementary side of this problem. Ansell and Gash (2008) emphasise institutional design, participation, trust, shared understanding, and consensus-oriented interaction, while Emerson et al. (2012) highlight the value of principled engagement, shared motivation and capacity for joint action. These frameworks take into account how autonomous actors might collaborate. Collaboration intensifies accountability relations. Lee and Ospina (2022) show that collaborative accountability is multilateral, combining horizontal and vertical relations rather than following a single bureaucratic chain. The issue is therefore not merely whether actors collaborate, but whether collaboration makes it possible to determine who must act, according to what rule, within what time, on the basis of what evidence, and before which actor or forum the response must be justified.

The intersection of these two literatures produces a sharper theoretical tension. In interoperability research, governance is commonly treated as a condition for successful data integration. In collaborative-governance research, data infrastructures are commonly treated as resources that support interaction. Less attention has been given to whether data definitions, validation rules, access permissions, performance thresholds, workflow states, audit trails, and closure rules can themselves become mechanisms through which distributed public authority is operationalised. The more demanding question is whether data can move across organisational boundaries and whether such movement makes that data institutionally consequential.

This article conceptualises that transition as a movement from interoperability for governance to interoperability-as-governance. The argument is conditional rather than technologically deterministic. Software does not create legitimate authority independently of institutions. Yet interoperable arrangements may acquire governance significance when shared definitions determine what counts as an actionable condition; access and validation rules specify who may recognise or alter that condition; thresholds trigger obligations; workflows assign responsible actors and time limits; audit trails preserve answerability; and verification rules determine who may recognise a matter as resolved. At that

point, the infrastructure is no longer merely transporting information. It is helping to structure meaning, authority, obligation, and accountability.

The Ambon case makes this boundary observable. Official beneficiary data did not always map cleanly onto locally observed conditions, requiring reconciliation rather than automatic synchronisation. Allergy-related information was operationally necessary but too sensitive for unrestricted circulation. Complaints could be communicated without equivalent degrees of resolution. These are not only data-quality problems. They are institutional problems because they concern whose information is authoritative, who may validate exceptions, what constitutes a response, and who may declare closure. The study therefore treats the dashboard not primarily as a visualisation artefact but as an experimental governance architecture linking a minimum dataset, data ownership, validation, actionable indicators, role-based access, responsible actors, service-level expectations, escalation, evidence, verification, and closure.

An earlier publication by the same research team established a documentary diagnosis and design specification for an interoperable MBG monitoring dashboard in Ambon using public reports, official guidance, and a research design document; it did not claim completed software development or field usability testing (Muhtar et al., 2026). The present study builds upon that work by providing primary field evidence at the school-service interface, establishing a broader cross-actor institutional evidence base, implementing a working prototype, and conducting a controlled end-to-end evaluation. It also develops a distinct theory-building contribution by specifying governance-bearing interoperability, a governance-threshold proposition, and reusable design principles that were not developed in the earlier article.

The research gap is threefold. First, digital-government research has established that organisational and institutional arrangements are necessary for interoperability but pays less attention to how interoperable arrangements may structure organisational authority and accountability. Second, collaborative-governance research provides strong accounts of joint action and accountability but offers comparatively limited attention to the constitutive role of digital data architectures in allocating decision rights and obligations. Third, school-feeding monitoring research has examined coverage, indicators, service quality, and evaluation capacity but has not sufficiently explained how integrated monitoring can connect a detected deviation to differentiated responsibility, corrective evidence, verification, and closure across organisational boundaries. The theoretical puzzle is therefore not whether governance and interoperability are related; that relationship is already well established. The unresolved issue is where the direction of explanation changes: when arrangements initially designed to support coordination begin to define authoritative meanings, permissible actions, response obligations, and closure conditions. Put differently, the missing explanation is not simply how to build another monitoring application, but how interoperability crosses a governance threshold without collapsing legitimate organisational differences into technical rules. This gap is consequential because the same technical device can support very different institutional arrangements: one may merely aggregate information, while another may determine who can validate a problem, who becomes answerable, and what counts as satisfactory resolution. Explaining that variation requires a theory of the institutional consequences of interoperability, not only a theory of successful integration.

Against this background, the article asks:

When does data interoperability move from being a technical capacity for information exchange to becoming a governance mechanism that structures authority, collaborative accountability, and corrective action across organisational boundaries?

To answer this question, the study uses Design Science Research to make otherwise dispersed governance assumptions explicit in an artefact and then traces five mechanisms through which interoperability becomes governance-bearing: semantic stabilisation, authority allocation, actionability, traceability, and accountable closure. The

contribution lies not in claiming that a dashboard itself governs, but in identifying the institutional conditions under which shared data can become consequential for collective action.

The article makes three linked contributions. First, it reverses the usual explanatory direction by theorising how interoperability arrangements can constitute governance rather than merely depending on them. Second, it identifies a five-mechanism governance threshold and distinguishes governance-bearing capacity from institutionalised interoperability-as-governance. Third, it provides empirical process evidence showing how beneficiary reconciliation, sensitive-condition data, complaints, oversight recommendations, and closure requirements expose the conversion of shared data into differentiated authority and accountable action.

2. Theoretical Background and Conceptual Framework

2.1. From technical interoperability to institutional interoperability

That definition captures an indispensable technical condition but is analytically incomplete in public administration because interoperation occurs across jurisdictions that differ in mandates, professional vocabularies, legal constraints, reporting cycles, and decision authority. Scholl and Klischewski (2007) therefore frame e-government integration as simultaneously technical and organizational, while Margariti et al. (2022) point out organizational interoperability as a specific requirement for digital transformation in the public sector. The implication is that a connection can work technically while failing institutionally. Data may move correctly yet remain unusable for collective action because actors disagree about definitions, ownership, validation, or the consequences attached to a value. For fragmented public services, interoperability is therefore better understood as a layered coordination problem in which technical connectivity is necessary but cannot determine by itself how information becomes authoritative or actionable.

The layered view distinguishes at least three familiar questions. Technical interoperability asks whether systems can connect and exchange data. Semantic interoperability asks whether information retains sufficiently stable meaning across systems and organizations. Organizational interoperability asks whether actors can coordinate processes around that information. These layers are interdependent, but none fully answers a fourth question that becomes central once shared data enter decision processes: who is entitled to validate a condition, determine that it requires intervention, assign responsibility, verify evidence, and declare the matter closed? This study calls the point at which interoperable arrangements begin to structure those institutional consequences the governance threshold of interoperability. The threshold is not a technological maturity level. It is an analytical boundary between interoperability that mainly enables information exchange and interoperability whose rules become consequential for organizational authority and accountability.

Research in Information Systems Frontiers reinforces the need to look beyond connectivity. Guo et al. (2024) proposes an architecture for semantic interoperability that preserves the meaning between heterogeneous information systems. It is not only about interfaces but also shared agreements and governance arrangements which enable the digitally processible exchange in collaborative ecosystems (Kannisto et al. 2020). Klievink et al. (2017) similarly show that public-sector data initiatives depend on organizational readiness and the capacity to handle institutional uncertainty. Together, these studies explain why interoperable infrastructures need governance. The present article takes the inverse step. It asks when the agreements required to make interoperability work—definitions, access rules, ownership, validation, thresholds, and workflow rights—also begin to govern the participating organizations. This reversal matters because it shifts interoperability from a background capability to a possible institutional mechanism. This distinction also clarifies why public-sector interoperability cannot be evaluated only by integration depth. A tightly integrated platform may remain institutionally shallow if actors continue to rely on parallel interpretations and informal workarounds. Conversely, a relatively modest exchange arrangement may be institutionally consequential if shared

definitions, validation rights, and response obligations are settled. The theoretical object is therefore not technological sophistication as such, but the relationship between informational integration and institutional consequence.

Pragmatic interoperability is the nearest neighbor construct. It extends beyond the syntax and semantics of the exchanged data to examine whether it enables the intended actions, the goals of the organization, and the actual outcomes. New research in Information Systems Frontiers shows that pragmatic interoperability is a function of actors' strategic motives and alignment of system-level and business-level purposes (Obayi et al., 2025). Governance-bearing interoperability addresses a different, complementary question. Its analytical focus is not primarily whether exchanged data are useful for intended outcomes, but whether interoperability arrangements allocate institutionally differentiated rights and obligations: who may validate a condition, whose threshold triggers action, who becomes answerable, what evidence must be produced, and who may authorize closure. Pragmatic interoperability therefore concerns alignment between exchange and intended use; governance-bearing interoperability concerns the institutional consequences through which that use becomes authoritative and accountable. The distinction is important because an exchange can be pragmatically useful without redistributing formal decision rights, while a governance-bearing arrangement can constrain or authorize action even when actors disagree about its strategic desirability.

2.2. Collaborative governance and distributed authority

Collaborative governance is the second theoretical anchor, as fragmented public services seldom operate under a unitary, hierarchical authority. Ansell and Gash (2008) stress aspects of institutional design, trust, shared understanding and consensus oriented interaction, and Emerson et al. (2012) refer to principled engagement, shared motivation and capacity for joint action. Provan & Kenis (2008) further add that inter-organizational networks require governance structures even when the participating organizations retain formal autonomy. These perspectives challenge the notion that coordination is just a matter of creating better links between organizations. Collaboration must preserve differentiated mandates while creating enough common structure to support collective action. This makes public-service networks a useful setting for studying interoperability: the central problem is not how to eliminate organizational boundaries, but how to coordinate across them without erasing legitimate differences in authority.

Authority therefore remains present inside collaboration; it is redistributed, negotiated, and sometimes contested. Purdy (2012) identifies formal authority, resources, and discursive legitimacy as different sources of power in collaborative processes. Digitally mediated coordination adds another layer because elements that appear technical can materialize those power relations. Permission to view a record is different from permission to alter it; the right to validate an exception is different from the ability to report it; a threshold can determine when an observation becomes an organizational problem; and closure rights can determine whose judgment counts as sufficient evidence of resolution. Rather than treating these features as neutral system administration, the framework treats them as possible expressions of institutional design. The relevant question is not whether technology replaces authority, but whether information architectures make the distribution of authority more explicit, durable, and executable. This perspective also complicates the familiar distinction between formal and informal governance. Digital rules may codify some relationships but leave others to negotiation, professional judgment, or trust. The workflow may define who should respond, but the actors may dispute the classification that triggered it. The importance of interoperability for governance is therefore in part its redistribution of points of discretion: some judgments become standardized and visible, while others remain subject to interpretation and contestation.

2.3. From shared information to collaborative accountability

Accountability becomes more difficult when public outcomes are produced by many hands. Bovens (2007) defines accountability as a relationship in which an actor has an obligation to explain and justify his or her actions to a forum that is empowered to question, judge, and possibly impose sanctions. However, in collaborative environments the

actor-forum relation is rarely one-to-one. Multiple organizations may share responsibilities, report to different authorities, and depend on each other's actions. Thus, Lee and Ospina (2022) show that collaborative accountability is multilateral, creating vertical and horizontal relationships and encompassing information, discussion, and consequences. Their account is important for interoperability, as shared data can improve visibility without clarifying who is responsible for what. More information may even intensify ambiguity if responsibility is distributed but the sequence of obligations remains unspecified.

This study consequently distinguishes shared responsibility from collaborative accountability. Shared responsibility means that several actors contribute to a common outcome. Collaborative accountability requires those differentiated responsibilities to be connected through a traceable process: a condition is recognized, a responsible actor is identified, a time-bounded response is expected, evidence is produced, another authorized actor may review that evidence, and closure is recorded. This distinction fits with Lee and Ospina's (2022) focus on process rather than accountability as a static attribute. It also speaks to Purdy's (2012) insight that power shapes who participates, who can negotiate, and whose interpretation gets into the collaborative process. Interoperability becomes theoretically relevant to accountability when it connects otherwise distributed obligations without assuming that every actor holds the same authority. Collaborative accountability is thus not synonymous with collective responsibility. Describing every actor as jointly responsible may dilute answerability in practice, as no actor is clearly obligated to act. The framework instead emphasizes differentiated but connected responsibility. Interoperability can contribute by making those connections inspectable: the producer of information, the validator, the responsible operational actor, the verifier, and the forum that receives the account may occupy different organizational positions while remaining linked through one traceable process.

2.4. Five mechanisms of interoperability-as-governance

The conceptual framework proposes five mechanisms through which interoperability can become governance-bearing. Semantic stabilisation establishes sufficiently shared meanings for conditions that may trigger collective action. Authority allocation links information rights to recognised organisational roles rather than treating access as institutionally neutral. Actionability connects indicators and deviations with responsible actors, time expectations and conditions for escalation. Traceability preserves the provenance and sequence of decisions across organisational boundaries so that disagreement, correction, and responsibility remain inspectable. Accountable closure requires corrective evidence and authorised verification before a matter is treated as resolved. The mechanisms are analytically distinct but interdependent: semantic agreement without authority leaves ownership unresolved; authority without actionability can produce nominal responsibility; action without traceability weakens answerability; and traceability without closure can document activity without establishing resolution. The framework therefore treats interoperability-as-governance as a relational configuration rather than as a feature list or a linear technological stage. Table 1 summarizes these five mechanisms by linking each mechanism to its principal technical expression and governance function.

Table 1
Five mechanisms of governance-bearing interoperability: technical expressions and governance functions

Mechanism	Technical expression	Governance function
Semantic stabilization	Data dictionary, reference codes, reconciliation	Determines what a condition means and whether it is institutionally recognizable
Authority allocation	RBAC, ownership, validation and approval rights	Specifies who may know, change, validate, decide, or close
Actionability	KPI, threshold, alert, PIC, SLA, escalation	Converts deviation into an obligation to act
Traceability	Audit trail, timestamps, provenance, status history	Makes distributed decisions and responsibilities reconstructable
Accountable closure	Evidence, verifier, closure status	Separates claimed correction from authorized recognition of resolution

2.5. The governance-threshold proposition

The framework does not imply that data integration automatically produces governance. For the purposes of this study, the five mechanisms are treated as constitutive conditions of a complete governance-bearing decision cycle rather than as interchangeable maturity indicators. Semantic stabilization is required so that an actionable condition has a sufficiently shared meaning; authority allocation is required so that the right to recognize or alter that condition is institutionally differentiated; actionability is required to convert deviation into an obligation; traceability is required to preserve the decision history; and accountable closure is required to distinguish activity from authorized resolution. The absence of any one mechanism yields only partial governance-bearing capacity. For example, an alert without an accepted responsible actor produces visibility without obligation, while a corrective action without verification produces activity without accountable closure.

A second boundary separates governance-bearing design from institutionalized interoperability-as-governance. Governance-bearing interoperability exists when the architecture encodes all five conditions coherently and can execute them across a decision cycle. Institutionalized interoperability-as-governance is the stronger state in which organizations recognize those definitions, roles, thresholds, and verification rights as legitimate and routinely enact them in actual decisions. This boundary makes the proposition falsifiable: technical execution can demonstrate governance-bearing capacity, but evidence of routine recognition, compliance, contestation, and negotiated change is required to claim institutionalization. A system therefore fails to cross the institutional governance threshold if actors bypass its definitions, reject assigned authority, ignore its escalation rules, or refuse the legitimacy of closure decisions, even when the software operates correctly.

Proposition 1

(governance-bearing threshold). An interoperable arrangement has governance-bearing capacity when the five mechanisms jointly structure a complete decision cycle from a recognized condition to authorized closure. It crosses the institutional governance threshold only when participating organizations recognize those encoded definitions, rights, obligations, traces, and closure decisions as legitimate and routinely consequential.

3. Research Design and Methods

3.1. Research design and epistemic purpose

This study uses theory-elaborating Design Science Research (DSR) within a bounded single-case public-service setting. It is not treated as a mixed-methods design: interviews, documents, process materials, and prototype test data serve complementary functions inside one DSR logic rather than forming separate qualitative and quantitative strands. The objective is explanatory and design-theoretical—to identify the conditions under which interoperability moves beyond information exchange and begins to structure authority, responsibility, and collaborative accountability.

DSR is appropriate because knowledge is generated through disciplined artefact construction and evaluation (Hevner et al., 2004; Peffers et al., 2007). Consistent with Gregor and Hevner (2013), the artefact is not treated as a final scholarly contribution. Its design is used to expose and test higher-order relationships among semantic rules, access rights, thresholds, workflows, evidence requirements, and closure authority.

The study is therefore a substantive empirical and theoretical extension of the team's earlier documentary design paper (Muhtar et al., 2026), rather than a replication of that design specification. The earlier work informed the starting design space; the present analysis adds primary interviews, institutional monitoring evidence, prototype enactment, evaluation, and theory elaboration.

The bounded context provides analytical leverage rather than statistical representativeness. Case-based theorizing is useful when a setting makes mechanisms unusually visible (Siggelkow, 2007; Eisenhardt & Graebner, 2007). Ambon is therefore used to elaborate a mechanism linking interoperability to governance, not to estimate the prevalence of operational problems across Indonesia.

3.2. Case context, unit of analysis, and empirical boundaries

The empirical setting is the monitoring and evaluation of Indonesia's Free Nutritious Meal (MBG) programme in Ambon City. The theoretical unit of analysis is the cross-organisational service chain through which beneficiaries are identified, meals are produced and distributed, schools receive deliveries, food-safety risks and complaints are monitored, recommendations are issued, and corrective actions taken. This unit is analytically appropriate because the phenomenon of interest occurs at organisational interfaces where information and authority are distributed rather than within a single agency.

The empirical observation level is deliberately narrower than the theoretical unit. Primary interviews are concentrated at the school-facing boundary of the chain, but the wider governance structure is reconstructed from official programme, monitoring, inspection, and oversight records. These materials identify five recurring actor layers: BGN/KPPG and SPPG for production, distribution, operational status, suspension and reactivation; municipal government, education authorities and schools for targeting, reception, complaints and coordination; health services and BPOM for hygiene, sanitation, certification, sampling and testing; BPKP for effectiveness, compliance, infrastructure, finance, risk and recommendations; and DPRD/DPD/Ombudsman for public-service and external accountability. Authority claims in the analysis are therefore grounded in formal or public institutional evidence, whereas actor experiences and last-mile practices are grounded primarily in school interviews.

The case is used for analytic rather than statistical generalisation. Ambon's island-city service environment makes distribution time, service radius, last-mile reception, and cross-agency monitoring especially visible, while the rapid expansion of SPPG and recipient coverage creates a setting in which source definitions and monitoring responsibilities changed over time. Evidence with different geographic scopes was retained with its source, date, and institutional boundary rather than silently aggregated. Table 1 summarises the empirical materials, their analytic roles, and the reporting boundaries used to prevent evidence classes from being conflated.

Table 1
Empirical material and analytic role

Evidence source	Coverage	Role in the study	Analytic use	Reporting boundary
Semi-structured interviews	3 school-based adult informants + 1 secondary-school beneficiary	Primary qualitative evidence	Last-mile practices, beneficiary exceptions, allergies, distribution, portions/menu, complaints, reporting channels and decision needs	Primary experience evidence is concentrated at the school interface
Policy and programme documents	National/local regulations, BGN guidance, local programme records	Formal institutional evidence	Mandates, standards, authoritative data, variables, decision rights and compliance requirements	Used to reconstruct formal roles; not treated as evidence of actors' subjective acceptance
Monitoring, oversight and safety records	2025–2026 records involving KPPG/BGN, Pemkot/Disdik, Dinkes/BPOM, BPKP, DPRD/DPD/Ombudsman, plus incident material	Cross-actor institutional evidence	Five-layer actor map, inspection priorities, suspension/reactivation, recommendations, escalation and follow-up requirements	Evidence is documentary/public unless explicitly identified as a primary interview
Existing formats/process evidence	Spreadsheets, forms, links and reported WhatsApp/direct communication	Process/data evidence	Semantic differences, handoffs, provenance gaps, reconciliation and traceability requirements	Used to understand information practices, not to estimate prevalence
Demonstration dataset	1 SPPG, 3 schools, 5 days, 15 distribution records	Artefact demonstration evidence	Validation, KPI, alerts, role restrictions, workflow, evidence and closure	Controlled data; not routine organizational adoption
Functional test log	20 predefined scenarios	Evaluation evidence	Technical efficacy across validation, distribution/KPI, safety/incidents, RBAC/audit, responsiveness/export	Does not establish institutional recognition or real-world programme effects

3.3. Participants and data collection procedures

Primary interviews involved four roles at the school-service interface: a primary-school principal (KS-SD1), a junior-secondary MBG manager (PG-SMP15), a senior-secondary vice-principal/programme coordinator (PIC-SMA11), and one student beneficiary (SW-SMA11). Role-based codes are used in the manuscript. A public interview with the regional KPPG head was treated only as secondary triangulation. Exact interview dates and durations are absent from the archive and are therefore not reconstructed.

Interviews were semi-structured and role-adapted, covering beneficiary identification, reception and distribution, menus and portions, allergies or special conditions, food safety, complaints, reporting channels, monitoring practices, perceived benefits, and dashboard needs. This format balanced comparability with the ability to capture role-specific exceptions; Kallio et al. (2016) provide the methodological basis for linking semi-structured guides to prior knowledge and transparent topic design. The interview guide was therefore organised around decisions and exceptions rather than perceptions of the software alone. Participants were asked to describe what happened when routine delivery diverged from expectations, how discrepancies were communicated, and what evidence they used to decide that a

problem had been addressed. This orientation was chosen because the research question concerns governance consequences rather than technology acceptance in the abstract.

Document collection was purposive and treated as an empirical stream rather than background context. Materials were retained when they clarified formal mandates, monitoring events, inspection findings, safety controls, public accountability, or data/reporting requirements. The corpus included national and local programme guidance and public records of monitoring by BGN/KPPG, municipal/education actors, health and food-safety bodies, BPKP, legislative oversight, and Ombudsman-related monitoring. Each item was read substantively for what condition or risk it documented and procedurally for who generated the information, who possessed decision authority, what response was expected, and whether closure or reactivation required further evidence. Dates, geographic scope, terminology, and denominators were retained so that apparent inconsistencies remained analytically visible rather than normalised.

A process-analysis stream examined spreadsheets, forms, official data, web links, reported WhatsApp coordination, and direct communication to identify points where information changed meaning, ownership, verification status, or responsible actor. The monitoring chronology for 2025–2026 was also used to trace how oversight priorities expanded from coverage and delivery to hygiene, certification, testing, risk, corrective action, and external accountability. These observations informed as-is/to-be workflows, the minimum dataset, escalation routes, and provenance requirements.

A controlled demonstration dataset representing one SPPG, three schools, five operational days, and 15 distribution records was kept separate from empirical problem evidence. It provided a reproducible environment for testing validation, KPI calculations, alerts, role restrictions, auditability, corrective-action workflows, and export functions.

COREQ items (Tong et al., 2007) were used as a reporting audit, not as a retrospective claim of prospective protocol compliance. Where the archive is silent—for example, on interview duration, prior interviewer relationships, or transcript-return procedures—the manuscript states that boundary explicitly.

3.4. Data processing, coding, and analytic strategy

Analysis followed five linked stages. First, evidence classes were preserved: interviews, official documents, public statements, programme information, and demonstration records were kept distinguishable, with source, period, scope, and verification status retained where available. This process was necessary because disagreement over meaning and authority is part of the phenomenon rather than noise to be removed.

Second, first-cycle thematic coding followed Braun and Clarke's (2006) flexible thematic-analysis logic. Coding remained close to operational problems and covered eight archived domains: data/interoperability; menu, quality and portions; food safety/allergies; distribution; complaints/follow-up; benefits/student acceptance; monitoring; and dashboard requirements. Coding was not organised around the five theoretical mechanisms at the outset. Keeping first-cycle codes closer to field problems reduced the risk of forcing evidence prematurely into the conceptual framework. The five mechanisms were applied only during second-order abstraction after recurrent empirical problems and design requirements had been identified.

Third, empirical observations were translated into design requirements through a traceability chain. Delays became departure/arrival fields and deviation reasons; beneficiary discrepancies became exception and reconciliation workflows; allergy concerns became restricted condition/substitution fields; repeated complaints became response-evidence-verification-closure records; and fragmented channels became a semantic and process-interoperability requirement. This step tied each major feature to an observed or normative problem.

Empirical observation → governance problem → information requirement → decision rule → artefact feature → evaluative test

Fourth, second-order abstraction grouped requirements into the five theoretical mechanisms: semantic stabilisation, authority allocation, actionability, traceability, and accountable closure. The reasoning was abductive rather than purely inductive: empirical anomalies refined theory, prior concepts sensitised attention, and artefact construction exposed relationships that were difficult to see when interoperability was treated only as connectivity (Gioia et al., 2013).

Fifth, interpretations were challenged through cross-school comparison and triangulation with official guidance, oversight material, and public statements. Discrepant terminology or figures were retained with source boundaries. The archive does not document independent double coding; credibility instead rests on source triangulation, explicit traceability, preserved contradictions, and separation of evidence from inference (Nowell et al., 2017; Tracy, 2010). Validation therefore operated through convergence and disciplined disagreement rather than simple source counting. A theme was treated as stronger when it appeared across independent evidence classes or when documentary rules and field accounts pointed to the same design problem. Where sources conflicted, the conflict was retained as evidence of fragmentation and became a prompt for reconciliation or authority rules in the artefact. The overall research design and theory-building sequence are summarised in Fig. 1.

3.5. Artefact construction as a theory-building intervention

Artefact construction iteratively translated problems into requirements, specifications, functions, and a revision backlog. The architecture connected a minimum dataset and data dictionary to validation, reconciliation, RBAC, audit trails, actionable KPIs, alerts, responsible actors, time expectations, escalation, corrective evidence, verification, and closure.

Four layers were distinguished: a data layer for definitions, sources, ownership and validation; a decision layer for indicators and deviations; a governance-workflow layer for responsibilities, deadlines, escalation, evidence and closure; and an interaction layer implemented through six responsive modules. API integration was intentionally deferred until semantic and governance arrangements were stable.

This sequencing made artefact construction a theory-building intervention: technical connection was not allowed to substitute for agreement on meaning, provenance, authority, and action.

3.6. Evaluation logic and acceptance criteria

Evaluation was embedded in the design cycle and is best characterized as formative, controlled, and context-relevant. Following FEDS (Venable et al., 2016), the study prioritizes technical efficacy and design coherence; it does not claim naturalistic evidence of sustained organizational adoption.

Three levels were examined: functional behavior (calculations, validation, workflow transitions, alerts, RBAC, audit logs, and exports); data quality (mandatory fields, codes, duplicates, and reconciliation); and governance-oriented design coherence (whether deviations were connected to responsible actors, time expectations, escalation, evidence, verification, and closure).

Acceptance criteria were specified before demonstration. Twenty predefined scenarios covered master data/validation (4), distribution/KPIs (6), food safety/incidents (5), RBAC/audit (3), and responsive display/export (2). All passed the technical test. KPI calculations were checked manually, alerts against defined thresholds, and status changes through the audit trail; failures, had they occurred, were to remain in the backlog. The scenarios were selected to cover both routine and deviant conditions so that the test would not reward a system that performed only under normal input. Tests included missing mandatory values, inconsistent codes, timing and portion deviations, safety-related states, access restrictions, status transitions, and evidence-linked closure. This provided a structured check that the governance logic survived exception handling as well as ordinary workflow execution.

Interpretation remained conservative: a 20/20 pass shows that the encoded workflow can execute under controlled conditions, not that agencies accept the allocation of authority, that thresholds possess normative legitimacy, or that programme outcomes improve. Those claims require subsequent naturalistic evaluation. Table 2 summarizes the principal analytic risks and the controls used to limit them.

Table 2
Analysis, validation, and bias-control chain

Stage	Primary risk	Control used	Contribution to inference
Evidence assembly	Conflating sources with different authority/scope	Source classes preserved; public statements separated from primary interviews	Clarifies provenance and prevents silent normalization
Thematic coding	Forcing evidence into preselected technical features	First-cycle problem coding before design translation	Maintains empirical grounding
Design translation	Technological solutionism	Observation-to-requirement traceability	Makes assumptions inspectable
Theoretical abstraction	Confirmation bias toward interoperability-as-governance	Cross-source comparison and retention of contradictions	Allows theory to be challenged by discordant evidence
Artefact evaluation	Defining success after seeing results	Predefined acceptance criteria and retained backlog	Reduces post hoc success claims
Inference	Equating technical success with institutional effectiveness	Explicit separation of technical efficacy, design validity, and institutional effectiveness	Prevents overclaiming

3.7. Researcher positionality, reflexivity, and bias mitigation

and with a project mandate to develop a monitoring artefact. Local familiarity strengthened contextual interpretation but created risks of technological solutionism and over-reading successful tests.

Reflexivity was therefore treated as quality control (Berger, 2015; Tracy, 2010). Primary interviews, public statements, documents, and demonstration data were kept distinct; discrepancies were preserved; major features required empirical or normative traceability; and technical evaluation was separated explicitly from organisational validation. A simple reflexive question was applied during analysis: would the same empirical observation still matter if no dashboard were built? If the answer was no, the proposed feature was reconsidered as potentially technology-driven rather than problem-driven. This check helped separate substantive coordination requirements from preferences created by the development mandate itself.

Primary interviews are concentrated on the school side of the service chain, the archive lacks a documented pilot interview and independent double-coding protocol, and not all organisations are represented directly. These limitations constrain inference but are consistent with the study's purpose of mechanism elaboration rather than comprehensive representation.

3.8. Ethics and participant protection

Project documentation records informed participation, anonymization, the right to withdraw, and explanation of intended data use. The manuscript uses role-based codes for primary participants and minimizes identifiable detail, particularly for the student participant (Kaiser, 2009). Because deductive identification is possible in small service settings, contextual detail is reported only when analytically necessary, and the findings privilege role and process over personal biography.

The research report further specifies that the dashboard is not intended to evaluate individual teachers, students, or food-service workers; analysis is directed at processes and service units. Findings are to be reported proportionately, with room for correction, and causal claims about food-safety incidents are withheld until laboratory or investigative evidence is available. These safeguards are consistent with the study's distinction between institutional accountability and individual surveillance.

Data-protection principles were also embedded in the artifact: public and managerial views use aggregation where appropriate, sensitive condition/allergy data are role-restricted, changes are logged, and data entry is separated from authorization to close a case. These design choices reduce unnecessary exposure while preserving the information required for operational response and auditability.

The available project documentation does not contain a separate research-ethics committee approval or exemption identifier. Accordingly, the study reports the documented participant-protection procedures transparently rather than attributing an approval number that is not present in the project record.

3.9. Scope of inference and reproducibility

The design supports analytic rather than statistical generalization. Reproducibility means that another team can reconstruct the chain from evidence to codes, design requirements, artifact rules, and tests, not that another case would reproduce identical qualitative statements.

Three claims are kept separate: technical feasibility (the logic can execute), design validity (the artefact is traceable to defensible requirements), and institutional effectiveness (organizations recognize and sustain the rules in practice). The study directly evaluates the first two and leaves the third to subsequent naturalistic research.

4. Findings and Discussion: From Fragmented Information to Governance-Bearing Interoperability

The findings answer the research question conditionally: interoperability became governance-bearing in the artefact when shared information was connected to rules about meaning, authority, obligation, traceability, and closure. Rather than an information deficit, the case revealed an institutional coordination deficit. School interviews documented fragmented last-mile practices, while programme and oversight records showed that production, targeting, food safety, financial/administrative oversight, and public accountability were distributed across different layers of actors. The controlled 20-scenario evaluation is therefore used only to establish that the resulting governance logic could be executed technically; it does not establish that every participating organisation has institutionalised those rules.

The analysis is organised around five mechanisms that together constitute a complete governance-bearing decision cycle. For each mechanism, the discussion separates observed field problems, documentary or institutional evidence, the design response, and the theoretical inference. This separation is important because an artefact's feature is not itself evidence that the corresponding governance relation already operates in routine practice. Table 3 summarises how the evidence streams support each mechanism and where the inference remains bounded.

Table 3
Evidence-to-mechanism chain and bounded inference for governance-bearing interoperability

Mechanism	Interview/field evidence	Document/artefact evidence	Interpretive key
Semantic stabilization	Dapodik was used as the beneficiary reference, yet locally observed students could remain unrecorded; allergy information was operationally necessary but sensitive.	Public coverage snapshots used different recipient definitions; the design retained provenance, exception status, verification and versioned definitions.	Rather than moving data faster, interoperability first had to stabilize what a value meant and which source could make it authoritative.
Authority allocation	Schools observed reception conditions and complaints but did not hold all formal rights over eligibility, safety, suspension or oversight.	Actor mapping assigns production/suspend-reactivate to BGN/KPPG-SPPG, hygiene/testing to Dinkes/BPOM, effectiveness/recommendations to BPKP, and external accountability to DPRD/DPD/Ombudsman; RBAC operationalizes differentiated rights.	Rather than flattening boundaries, governance-bearing integration connects actors while preserving legitimate differences in decision authority.
Actionability	Delays, menu/portion concerns, allergies and complaint outcomes varied across schools; one complaint was corrected quickly while another issue recurred.	Thirteen KPI groups connect definitions and deviations to threshold, risk, PIC, SLA, escalation and corrective-action fields; unsupported demo thresholds are not treated as official standards.	Rather than adding indicators, the design converts recognized deviations into time-bounded obligations whose legitimacy depends on institutional agreement.
Traceability	Problems and responses could move across WhatsApp, forms, spreadsheets and direct communication without one reconstructable history.	2025–2026 monitoring involved multiple oversight bodies; the architecture preserves provenance, old/new values, timestamps, recommendation source, status history and evidence.	Rather than showing only current state, interoperability preserves how a condition became accepted, corrected or contested across organizational boundaries.
Accountable closure	Complaint response and resolution differed across schools; safety responses could remain open pending investigation or authorization.	Incident records document temporary closure/suspension and the need for investigation/reactivation; recommendations require PIC, deadline, evidence, verifier and closure status.	Rather than treating communication or activity as completion, closure requires evidence and authorized recognition.

4.1. Semantic stabilization: from data abundance to governable meaning

The first finding is that fragmentation was semantic before it was technical. At the school interface, official education data were treated as the beneficiary reference, yet one school reported students who were locally present but not yet recorded in that source. Allergy information created a second tension because it was necessary for substitution decisions but inappropriate for unrestricted circulation. The school-level pattern was mirrored in public programme data: successive coverage snapshots referred to students, active recipients, and broader recipient groups using different denominators. The issue was therefore not simply inconsistent formatting. It was whether a value represented

the same institutional object across time and organisations and which source had authority when locally observed conditions diverged from an official record.

The field material makes this problem visible in ordinary work. One school leader described coordination as still relying on a WhatsApp group and linked forms, while the beneficiary record remained anchored to Dapodik. Rather than allowing the artefact to resolve discrepancies by overwriting one source, the design retained source values, verification status, exception states, and reasons for correction. The data dictionary specified definitions, reference codes, owners, update frequencies, validation rules, access classifications, and effective dates. A locally observed student could therefore be recorded as an exception awaiting verification without the system unilaterally redefining eligibility; sensitive allergy data could support operational action while remaining role-restricted.

This pattern matters theoretically because semantic interoperability is often framed as preserving machine-readable meaning across heterogeneous systems. Guo et al. (2024), for example, show in Information Systems Frontiers that semantic interoperability depends on architectures that stabilise meaning across information environments. The Ambon evidence extends this concern to governance. Once a definition determines eligibility, compliance, risk, or the need for intervention, standardising meaning also structures what organisations may legitimately recognise and act upon. Rather than a preliminary technical task, semantic stabilisation became an institutional mechanism: it defined the boundary between an observation, a disputed record, and an actionable condition. This helps explain why technical integration undertaken before semantic agreement can reproduce disagreement within a more sophisticated application.

The implication is that shared meaning is neither neutral nor automatically consensual. It can redistribute authority by privileging particular classifications, sources, or validation procedures. In this case, the design mitigated this risk by preserving provenance and requiring verification rather than treating integration as automatic harmonisation. Semantic stabilisation, therefore, represents the first movement towards the governance threshold: data become governance-relevant when shared definitions determine which conditions are institutionally recognisable, which remain exceptions, and what organisational actions can legitimately follow. Action could not be assigned reliably until actors sufficiently agreed on the status of the condition to which that action referred.

4.2. Authority allocation: integration without flattening organizational boundaries

access. The conclusion was not inferred only from the RBAC design. The empirical actor map reconstructed five layers of monitoring the right to perform corrective action, which was separate from the right to validate it, and the right to perform corrective action did not include decision-making authority. BGN/KPPG and SPPG were linked to production, portions, distribution, operating status, and suspension and reactivation; municipal, education, and school actors to targeting, reception, complaints, and coordination; Dinkes, puskesmas, and BPOM to hygiene, sanitation, certification, sampling, and testing; BPKP to effectiveness, compliance, infrastructure, finance, risk, and recommendations; and DPRD/DPD/Ombudsman to public service and external accountability. No single actor therefore controlled the whole service-risk chain.

The design response translated this differentiated authority into data ownership, input roles, access classifications, validation and approval rights, segregation of duties, and routing rules. This distinction mattered because the right to report a condition was separate from the right to validate it, and the right to perform corrective action was separate from the right to validate it, and the right to perform corrective action did not imply the right to verify closure. For example, schools could report reception problems or beneficiary exceptions, but the system was not allowed to redefine program eligibility; food-safety observations could trigger escalation without displacing the formal authority of

health and program bodies to investigate, suspend, or reactivate operations. RBAC therefore operationalized an empirically documented distribution of authority rather than inventing a new hierarchy.

This finding aligns with work showing that governance cannot be reduced to system implementation. Papazafeiropoulou and Spanaki (2016) emphasize stakeholder, control, risk and compliance arrangements in governance-related information systems, and Klievink et al. (2017) show that data exploitation in the public-sector depends on organizational readiness and governance conditions. Purdy's (2012) account of power in collaborative governance provides the complementary insight that formal authority, resources, and discursive legitimacy shape who can influence process and content. The present case connects these literatures: technical permissions can operationalize institutional authority when they determine whose interpretation can be validated, whose action can change status, and whose judgment can authorize closure.

The result is a paradox of integration. Interoperability had to connect organizations without flattening the boundaries that made their mandates legitimate in the first place. Maximum access would have produced technical openness but potentially weaker governance by obscuring differentiated responsibility. Conversely, excessive restriction would have preserved jurisdictional boundaries while preventing coordinated action. The case therefore suggests that governance-bearing interoperability depends on calibrated rather than universal integration: enough common structure to make cross-boundary action possible, but enough differentiation to preserve legitimate decision rights. Where authority remained contested, the software could expose the contest and record its implications but could not legitimately settle it on its own.

4.3. Actionability: from indicators to time-bounded obligations

The third finding is that visibility was insufficient unless deviations were converted into obligations. School experiences were heterogeneous: one site reported punctual delivery but repeated concerns over menu variation and uneven portions; another reported delays, menu repetition, and food waste; a third described a multi-day meal-package issue that was corrected after a complaint. These contrasts show why a single composite performance score would obscure the decision problem. The relevant question was not whether the dashboard could display a negative value, but whether a recognized deviation had an agreed response path.

Complaint evidence further separated communication from responsiveness. At one school a complaint was described as corrected promptly, while at another a recurring menu concern had been communicated repeatedly without complete resolution. The design therefore distinguished report date, category, risk, initial response, corrective action, responsible actor, evidence, verification, and closure status. The same logic structured the KPI layer: an indicator was actionable only when it had a definition, source, threshold, risk level, responsible actor, time expectation, and corrective-action rule. Importantly, the research report explicitly states that demonstration thresholds without a normative basis are not official standards; operational thresholds must be agreed with relevant partners and tied to their approving authority.

This pattern qualifies the common assumption that dashboards improve governance by increasing visibility. Matheus et al. Dashboards may encourage transparent, accountable decision making (2020). But poor quality data, and interpretation and institutional arrangements can lead to confusion or false transparency. Pereira et al. (2017), in Information Systems Frontiers, likewise connect public-sector data initiatives to public value through organizational coordination and stakeholder use rather than availability alone. The Ambon evidence adds a governance condition: information becomes consequential when a deviation triggers a recognizable obligation. Visibility tells actors that something happened; actionability specifies who must do what, by when, and under what escalation logic if the issue persists.

Actionability can therefore be represented as a chain: data → indicator → threshold → deviation → responsible actor → temporal obligation → corrective action. Yet the chain is not purely technical. A threshold has governance force only when actors recognize its basis; an assigned PIC matters only when the role is institutionally accepted; an SLA is consequential only when non-response has an understood escalation path. Rather than equating a red dashboard status with governance, the findings show that governing effects arise from the institutional consequences attached to the indicator. This is where measurement shifts into coordination: the system does not merely describe performance but connects a recognized condition to a differentiated duty to respond.

4.4. Traceability: from current-state integration to institutional memory

The fourth finding is that fragmentation was temporal as well as organizational. The 2025–2026 monitoring chronology shows that the same service network was examined by different bodies for different purposes: education actors focused on reception and delivery, BPOM and health bodies on hygiene, sanitation, and testing, BPKP on effectiveness, infrastructure, risk, and compliance, and Ombudsman-related monitoring on service quality and maladministration. “BPKP, BPOM, and Dinas Kesehatan might give different recommendations on the same SPPG in 2026,” the report reads. Without a shared history, a current 'compliant' status could conceal which recommendation was addressed, which remained open, or which evidence supported a change.

The architecture therefore preserved unique identifiers, source institution, verification state, timestamps, previous and revised values, reasons for correction, users responsible for changes, supporting evidence, recommendation category, deadline, and status history. Discrepant values were not silently replaced, and recommendations from different oversight sources remained distinguishable. This turned the audit trail from a technical log into an institutional record capable of showing how a condition moved from observation to correction and who accepted each transition.

The interpretation is consistent with collaborative information-exchange research. Kannisto et al. (2020) Information Systems Frontiers 1 3 For collaborative digital exchange, it is not only connectivity that matters, but also common agreements and continuous governance. Lee and Ospina (2022) explain collaborative accountability as the result of the interaction of vertical and horizontal relationships and is a function of information, discussion, and consequences. Traceability provides an infrastructural bridge between these perspectives because it makes distributed accountability reconstructable. It enables actors and reviewers to follow how a problem moved across organizational boundaries rather than relying on isolated communications or retrospective recollection.

Traceability therefore did more than increase transparency. It preserved institutional memory, including disagreement, correction, and changes in responsibility. This matters because accountability can weaken when integration erases the evidence needed to reconstruct how an accepted state was reached. The case suggests that governance-bearing interoperability should preserve not only accurate current values but also the provenance and sequence through which those values became authoritative. Rather than rewarding a clean dataset at any cost, the design treated an inspectable decision history as part of data quality itself. Interoperability became more consequential when it enabled actors to answer not only "what is the current status?" but also "how did this status become legitimate?" and what is the current position? but also, “how did this status become legitimate?

4.5. Accountable closure: from response to verified resolution

Fifth, response and resolution differed empirically. There were already different degrees of completion of school complaints, but proof of safety and oversight was what made the difference much more important. In 2025, a publicly reported incident at SD Inpres 35 Passo resulted in the closure of the kitchen until an investigation was completed. The research archive intentionally did not confirm the suspected cause, as the official laboratory never provided a final

determination. KPPG's public statement in 2026 also noted the temporary suspension of SPPG in Maluku for deficiencies in SOPs, sanitation/IPAL, SLHS, and food-safety standards. Such cases show that immediate response can be appropriate where institutional closure is still awaiting evidence, investigation or authorization to re-activate.

The artifact formalized that distinction by linking findings and recommendations to risk level, responsible actor, deadline, corrective evidence, verifier, escalation, and closure status. The workflow distinguished between the execution of a corrective action and the authority to deem that action sufficient. For safety-related cases, the design could represent hold, investigation, suspension, correction, and reactivation as different states rather than compressing them into a binary open/closed field. For routine complaints, the same principle required evidence of correction before an issue could be treated as resolved.

This finding connects directly to accountability theory. Accountability is more about explaining and justifying actions to a proper forum than just disclosure (Bovens, 2007). Lee and Ospina (2022) show that collaborative accountability extends this logic into multilateral settings where several horizontal and vertical relationships coexist. In the present case, evidence and verification translated that abstract relationship into an operational sequence. Corrective claims remained open until evidence could be reviewed by an authorized role. This does not eliminate discretion or conflict, but it makes the point of judgment explicit and therefore contestable rather than hidden in informal communication.

Accountable closure consequently provides the clearest empirical marker of the governance threshold. Interoperability was no longer only moving information among organizations; it was specifying who could legitimately recognize an institutional obligation as fulfilled. Yet closure also exposes the limit of technical design. A workflow can encode a verifier role, but institutionalization requires organizations to accept that role and its judgment. The case therefore supports a conditional interpretation: accountable closure is governance-bearing in architecture, but it becomes interoperability-as-governance only when the encoded verification relationship is treated as legitimate in routine practice.

4.6. Integrative interpretation: when interoperability becomes governance-bearing

ladder. Semantic stabilization establishes what condition is being governed; authority allocation establishes who may recognize or change its status; actionability specifies the obligation generated by deviation; traceability preserves the sequence through which responsibility is exercised; and accountable closure determines what evidence and authorization are required for resolution. All five are necessary for the complete governance-bearing cycle proposed here, although they may be revisited iteratively in practice. A dispute over closure can reopen authority questions, while repeated exceptions can force revisions to data definitions. Figure 2 summarizes the empirically derived pathway from fragmented information to governance-bearing interoperability.

Figure 2 Empirically derived pathway from fragmented information to governance-bearing interoperability

The technical evaluation provides a bounded entry point for this interpretation. Twenty predefined scenarios covering validation, distribution and KPIs, safety and incidents, role-based access and audit, responsive display, and export passed the controlled test. This result demonstrates that the encoded governance logic can execute under the demonstration conditions. It does not show that participating organizations accept the assigned roles, that simulated service-level expectations are binding, or that one organization recognizes another actor's authority to verify closure. The quantitative result is thus a feasibility assessment rather than the main empirical claim. Its value lies in showing that the five mechanisms can be instantiated together without treating technical success as evidence of institutionalization.

This boundary matters theoretically. Information Systems Frontiers research on public-sector data repeatedly shows that technological capacity must be read together with organizational readiness, governance, and stakeholder arrangements (Klievink et al., 2017; Pereira et al., 2017). The present case extends that position by distinguishing two states. Governance-bearing interoperability exists when an information architecture contains mechanisms capable of structuring meaning, authority, obligation, traceability, and closure. Institutionalized interoperability-as-governance requires those mechanisms to be recognized, routinely enacted, and consequential in actual organizational decisions. The distinction explains how a system can be technically coherent yet institutionally weak, or conversely, how relatively simple exchange formats can support strong coordination when roles and obligations are well settled. This distinction also changes how the five mechanisms should be interpreted comparatively. They are not five independent benefits that can simply be added together. Their effects are conditional on one another: strong traceability cannot compensate for contested semantic definitions, and carefully assigned authority cannot produce accountability if closure is unverifiable. The configuration, rather than any single feature, is what gives interoperability its governance-bearing capacity.

Empirically, the configuration is visible because the same service chain produced recurrent mismatches across distinct governance moments: authoritative beneficiary records required local exception handling; schools could observe conditions without holding all validation or suspension rights; complaints generated unequal degrees of follow-up; multiple oversight bodies produced recommendations that needed provenance; and safety-related correction did not equal authorized reactivation. Taken together, these observations provide process evidence for the five mechanisms rather than treating them as features inferred from the prototype alone.

The research question can therefore be answered conditionally. Interoperability becomes governance-bearing when all five mechanisms are attached to a shared decision cycle so that data no longer merely describe activity but carry differentiated institutional consequences. It becomes institutionalized interoperability-as-governance only when the participating organizations recognize and routinely enact those consequences. This distinction preserves the empirical contribution of the current study—showing how governance can be encoded and technically executed—without treating prototype success as evidence that every organizational relationship has already been institutionalized.

Rather than confirming the common assumption that better data sharing automatically produces better collaboration, the findings show that data sharing becomes consequential only when it is coupled to institutionally differentiated rights and obligations. The five mechanisms also complicate a simple technical-versus-organizational binary. Their operation is simultaneously informational and institutional: definitions are data structures and rules of recognition; permissions are security controls and allocations of authority; thresholds are analytic parameters and triggers of obligation; audit trails are logs and accountability records; closure states are workflow values and judgments about fulfilled responsibility. Theoretical attention should therefore shift from interoperability as a property of connected systems to interoperability as a potentially governance-bearing arrangement whose consequences depend on institutional recognition, contestation, and use. This interpretation also leaves room for failure and resistance. Organizations may comply with data standards while bypassing formal workflows, accept a dashboard's indicators while disputing its thresholds, or supply evidence while rejecting another actor's authority to verify it. Such divergence is not merely implementation failure; it is empirical evidence about where the governance threshold has not yet been crossed.

4.7. Design principles for governance-bearing interoperability

The DSR contribution can be expressed as reusable design knowledge rather than as a list of prototype features. The five mechanisms yield the following principles for public-service settings in which data and authority cross organizational boundaries. Table 4 translates the five mechanisms into reusable design principles.

Table 4
Design principles derived from the empirical mechanisms

Design principle	Observed problem	Design prescription	Mechanism
DP1 Preserve semantic contestability	Authoritative records and local observations can diverge.	Retain provenance, source values, exception status and verification rather than silently overwriting discrepancies.	Semantic stabilization
DP2 Separate access from decision authority	Actors can observe a condition without holding the right to validate, suspend, approve or close it.	Model viewing, editing, validation, response, verification and closure as distinct role-based rights tied to institutional mandates.	Authority allocation
DP3 Couple deviation to obligation	Indicators and complaints can remain visible without producing action.	Link each actionable deviation to an agreed threshold, responsible actor, time expectation, escalation route and corrective-action requirement.	Actionability
DP4 Preserve institutional memory	Multi-channel corrections can erase how an accepted state was produced.	Maintain auditable provenance, old/new values, timestamps, recommendation source, evidence and status history across organizations.	Traceability
DP5 Make closure evidence-bearing	Communication or self-reported correction can be mistaken for resolution.	Require corrective evidence and an authorized verifier before an obligation is closed; distinguish hold, investigation, correction and reactivation where risk warrants.	Accountable closure

These principles are intentionally purpose-sensitive. They do not prescribe one centralized platform or universal workflow. Instead, they specify how an interoperability arrangement should change when the governed task activates different meanings, risks, mandates, or accountability relationships. Their institutional effectiveness remains contingent on organizational recognition and negotiated legitimacy.

5. Conclusion

This study set out to examine when data interoperability moves beyond technical information exchange and begins to operate as a governance mechanism in fragmented public service systems. Drawing on three domains—digital government and organizational interoperability, collaborative governance and accountability, and multi-actor public-service monitoring—the study used Indonesia's Free Nutritious Meal program in Ambon as an analytically bounded case. The aim was not to test whether a dashboard could aggregate heterogeneous data but to explain how shared information becomes consequential for authority, responsibility, corrective action, and accountability.

First, rather than restating interoperability as the ability to exchange information, the findings show that it must stabilize meanings with organizational consequences. Discrepancies between authoritative records and local observations required provenance, exception states, and verification rather than automatic synchronization. Shared meaning, therefore, matters not only for compatibility but also for determining what conditions organizations may legitimately recognize and act upon.

Second, rather than mitigating fragmentation through unrestricted data sharing, the case shows that interoperability depends on differentiated authority. Viewing, editing, validating, responding, verifying, and closing are not equivalent rights. Effective integration required a shared environment that preserved legitimate differences in decision authority instead of flattening them into universal access.

Third, rather than evaluating monitoring by the number of indicators displayed, the study found that information became consequential when deviations were translated into time-bounded obligations. An indicator acquires governance force only when it is connected to an agreed-upon threshold, a responsible actor, a response expectation, an escalation path, evidence, and a verification process. Visibility without responsibility may increase awareness without increasing governability.

Most importantly, rather than treating interoperability and governance as separate domains, the study shows how interoperability can become governance-bearing when data infrastructures organize the relationship among meaning, authority, obligation, traceability, and closure. The five mechanisms operate as a connected configuration: weaknesses in one limit the governing capacity of the others. The contribution, therefore, lies not in the existence of an integrated dashboard but in identifying the institutional sequence through which shared data can become consequential across organizational boundaries.

The empirical contribution is therefore a mechanism-based account of how fragmented public-service information becomes governable: the study links concrete boundary problems—record discrepancies, sensitive allergy data, uneven complaint resolution, multi-actor oversight, and suspension/reactivation requirements—to the institutional rules needed to recognize, assign, trace, and close action. The 20-scenario prototype test then demonstrates the technical enactability of that mechanism configuration without being used as evidence of institutional adoption.

5.1. Theoretical contribution: shifting from whether interoperability matters to how it governs

The theoretical contribution is to shift from the question of whether interoperability supports governance toward the question of how interoperability takes part in organizing governance. Studies have shown that integration depends on organizational and institutional factors (Scholl & Klischewski, 2007; Luna-Reyes & Gil-Garcia, 2014; Margariti et al., 2022). Pragmatic interoperability also determines the consistency of the exchange with actors' intentions, organizational goals, and actual outcomes (Obayi et al., 2025). Governance-bearing interoperability adds a distinct institutional layer: it explains when exchange arrangements specify differentiated rights to validate, require action, preserve answerability, verify evidence, and authorize closure. The contribution is therefore not a replacement for pragmatic interoperability but an extension into the allocation of public authority and accountability.

This perspective complicates binary framings of technology versus governance. Technology is neither an autonomous institutional force nor a neutral instrument governed entirely from outside. The study therefore distinguishes governance-bearing interoperability—an architecture capable of structuring meaning, authority, obligation, traceability, and closure—from institutionalized interoperability-as-governance, in which those encoded relationships are recognized and routinely enacted by organizations. The distinction preserves institutional recognition as a boundary condition and avoids equating technical execution with legitimate authority.

It also complicates centralized-control versus decentralized-collaboration framings. Collaborative accountability can serve to bridge vertical and horizontal relationships and differentiated responsibilities (Lee & Ospina, 2022). Governance-bearing interoperability can make those relationships more explicit without requiring identical authority or a single central decision maker.

This yields three theoretical advances. First, it reverses the usual causal emphasis by treating interoperability as a medium for operationalizing governance, not just as a governance outcome. Second, it specifies the governance threshold as a configurational mechanism, so the explanatory unit is the linked decision cycle rather than isolated technical features. Third, it introduces institutional recognition as the boundary condition that separates governance-

bearing design from legitimate, routinized interoperability-as-governance, thereby making resistance, bypass, and contested closure theoretically meaningful rather than mere implementation noise.

5.2. Implications for public-service design

The practical implication is not that fragmented public services should replace existing systems with one centralized platform. Rather than enforcing comprehensive integration before institutional arrangements are agreed, organizations may benefit from flexible, purpose-driven interoperability. The appropriate architecture should depend on what information is expected to accomplish, who requires access, what authority it activates, the sensitivity and risk involved, and what form of accountability is required.

Standardized formats can be used for low-risk operational exchange, but eligibility, safety intervention, suspension, or formal closure require stronger validation and authorization. Aggregate signals may be created from sensitive information that is restricted in access. Corrective-action data require traceability because accountability depends on reconstructing how a status was reached, not only displaying the current state. The design principle is therefore fit between interoperability arrangements and governance consequences, not maximum integration.

For school-meal monitoring, beneficiary reconciliation, menu feedback, distribution delays, safety incidents, and oversight recommendations should not necessarily use identical workflows. Their risk, sensitivity, institutional authority, expected response, and closure requirements differ. Purpose-driven interoperability should preserve those differences while making cross-organizational dependencies visible and answerable.

5.3. Limitations and future research

The study has clear limits. It is a single embedded case and makes no claim of statistical generalization. Its contribution is analytical: the case provides leverage for identifying mechanisms through which shared data can become institutionally consequential. Comparative research is needed to examine whether the mechanisms combine differently under other institutional arrangements.

Primary interviews are concentrated at the school interface, while the wider distribution of authority is reconstructed from formal programs, monitoring, oversight, inspection, and public institutional evidence. This supports analysis of documented mandates and cross-actor decision pathways, but it does not substitute for first-person evidence about how all organizations interpret or contest those mandates. Future naturalistic evaluation should therefore include SPPG/KPPG, municipal and education authorities, health/BPOM actors, BPKP, and external accountability bodies to examine whether the encoded authority and closure relations are recognized consistently across positions.

The study also evaluates design feasibility rather than full institutionalization. Technical execution does not establish that organizations regard encoded roles as legitimate or sustain them in contested situations. Longitudinal research should therefore examine the transition from governance-bearing interoperability to institutionalized interoperability-as-governance, including moments when rules are accepted, bypassed, resisted, or renegotiated.

These limitations open a wider agenda. Comparative work could test the five mechanisms in health surveillance, disaster response, social protection, education, or food-safety regulation, and examine whether traceability strengthens accountability or creates surveillance burdens, whether formalized closure improves problem resolution or encourages procedural compliance, and how conflicting authorities are negotiated when organizations disagree over shared data.

The broader implication is not that interoperable systems inevitably govern. Interoperability creates an institutional possibility whose effects depend on purpose, rules, actors, and accountability relationships. Governance-bearing interoperability is therefore best understood as a purpose-sensitive institutional resource: its governing capacity depends on the task it supports, the authority it activates, the risk it addresses, and the accountability relationship it

makes possible. This formulation shifts future debate from whether systems can interoperate to how different forms of interoperability become differently consequential for governance—and how those consequences are organized, negotiated, and contested in practice. Future work should therefore treat governance-bearing interoperability as a variable institutional accomplishment rather than an endpoint. The concept invites comparison of which tasks require strong formalization, which depend on negotiated discretion, and when attempts to encode accountability improve coordination versus generate new conflict, burden, or strategic compliance.

Declarations

Funding. This study was funded by Universitas Pattimura through the Penelitian Dasar Unggulan Unpatti (PDUU) / Program Penelitian Unggulan Fakultas (PUF) scheme, Faculty of Social and Political Sciences, 2026. The available project report does not list a grant number.

Author Contributions. Muhtar led the research project, coordinated the study design and analysis, and led preparation of the manuscript. Jusuf Madubun and Marno Wance contributed to the research design, interpretation of findings,. All authors contributed to the research and manuscript development.

Competing Interests. The authors have no relevant financial or non-financial interests to disclose.

Ethics Approval and Consent to Participate. This non-clinical social-research study was conducted within the Universitas Pattimura PDUU/PUF research scheme. Project documentation records participant consent, anonymization, the right to withdraw, and explanation of the intended use of the data. The available project documentation does not contain a separate research-ethics committee approval or exemption identifier. Only de-identified, role-based evidence is reported in the manuscript.

Consent for Publication. Not applicable. The manuscript does not contain identifiable personal data, images, or other participant material requiring consent for publication.

Data Availability. The qualitative interview data are not publicly available because they contain potentially identifiable contextual information and are subject to participant confidentiality. De-identified artefact specifications, test scenarios, and non-sensitive materials supporting the findings may be available from the corresponding author upon reasonable request, subject to institutional and ethical restrictions. Public documentary sources used in the study are cited in the manuscript.

Related Publication Disclosure. A related earlier article by the same research team reported a documentary diagnosis and design specification for the Ambon MBG dashboard (Muhtar et al., 2026). The present manuscript extends that work with primary field evidence, cross-actor institutional records, prototype implementation and controlled evaluation, and develops the distinct theoretical constructs of governance-bearing interoperability, the governance threshold, and reusable design principles.

References

1. Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571. https://doi.org/10.1093/jopart/mum032
2. Badan Gizi Nasional. (2025). Keputusan Kepala Badan Gizi Nasional Republik Indonesia Nomor 401.1 Tahun 2025 tentang Petunjuk Teknis Tata Kelola Penyelenggaraan Program Makan Bergizi Gratis Tahun Anggaran 2026.
3. Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research*, *15*(2), 219–234. https://doi.org/10.1177/1468794112468475

4. Bicalho, D., Santos, T. S. S., Slater, B., & Lima, T. M. (2021). Evaluation of quality indicators for management of the National School Feeding Program in Brazil: A systematic review. *Ciência & Saúde Coletiva*, *26*(8), 3099–3110. https://doi.org/10.1590/1413-81232021268.03802020
5. Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, *13*(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x
6. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
7. Dawes, S. S., Cresswell, A. M., & Pardo, T. A. (2009). From 'need to know' to 'need to share': Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review*, *69*(3), 392–402. https://doi.org/10.1111/j.1540-6210.2009.01987_2.x
8. Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/AMJ.2007.24160888
9. Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory*, *22*(1), 1–29. https://doi.org/10.1093/jopart/mur011
10. Gelli, A., & Espejo, F. (2013). School feeding, moving from practice to policy: Reflections on building sustainable monitoring and evaluation systems. *Public Health Nutrition*, *16*(6), 995–999. https://doi.org/10.1017/S1368980012003989
11. Gil-Garcia, J. R., & Sayogo, D. S. (2016). Government inter-organizational information sharing initiatives: Understanding the main determinants of success. *Government Information Quarterly*, *33*(3), 572–582. https://doi.org/10.1016/j.giq.2016.01.006
12. Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151
13. Gregor, S., & Hevner, A. R. (2013). Positioning and presenting Design Science Research for maximum impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01
14. Guo, H., Scriney, M., & Liu, K. (2024). An ostensive information architecture to enhance semantic interoperability for healthcare information systems. *Information Systems Frontiers*, *26*, 277–300. https://doi.org/10.1007/s10796-023-10379-5
15. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625
16. Kaiser, K. (2009). Protecting respondent confidentiality in qualitative research. *Qualitative Health Research*, *19*(11), 1632–1641. https://doi.org/10.1177/1049732309350879
17. Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031
18. Kannisto, P., Hästbacka, D., & Marttinen, A. (2020). Information exchange architecture for collaborative industrial ecosystem. *Information Systems Frontiers*, *22*, 655–670. https://doi.org/10.1007/s10796-018-9877-0
19. Klievink, B., Romijn, B. J., Cunningham, S., & de Bruijn, H. (2017). Big data in the public sector: Uncertainties and readiness. *Information Systems Frontiers*, *19*, 267–283. https://doi.org/10.1007/s10796-016-9686-2
20. Lee, S., & Ospina, S. M. (2022). A framework for assessing accountability in collaborative governance: A process-based approach. *Perspectives on Public Management and Governance*, *5*(1), 63–75. https://doi.org/10.1093/ppmgov/gvab031
21. Luna-Reyes, L. F., & Gil-Garcia, J. R. (2014). Digital government transformation and internet portals: The co-evolution of technology, organizations, and institutions. *Government Information Quarterly*, *31*(4), 545–555.

https://doi.org/10.1016/j.giq.2014.08.001

22. Margariti, V., Stamati, T., Anagnostopoulos, D., Nikolaidou, M., & Papastilianou, A. (2022). A holistic model for assessing organizational interoperability in public administration. *Government Information Quarterly*, *39*(3), 101712. https://doi.org/10.1016/j.giq.2022.101712
23. Matheus, R., Janssen, M., & Maheshwari, D. (2020). Data science empowering the public: Data-driven dashboards for transparent and accountable decision-making in smart cities. *Government Information Quarterly*, *37*(3), 101284. https://doi.org/10.1016/j.giq.2018.01.006
24. Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4), 101385. https://doi.org/10.1016/j.giq.2019.06.002
25. Muhtar, Madubun, J., Rolobessy, M. J., Marsaolly, S. P. H., & Kabakoran, A. N. (2026). Data-interoperable collaborative governance for monitoring Indonesia's Free Nutritious Meal Program in Ambon. *International Journal of Applied and Scientific Research*, *4*(7), 457–476. https://doi.org/10.59890/ijasr.v4i7.265
26. Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*, 1–13. https://doi.org/10.1177/1609406917733847
27. Obayi, R., Choudhary, S., Nayak, R., & Ramanjaneyulu, G. V. (2025). Pragmatic interoperability for human–machine value creation in agri-food supply chains. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-024-10567-x
28. Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*, 1251–1263. https://doi.org/10.1007/s10796-015-9572-3
29. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302
30. Pereira, G. V., Macadar, M. A., Luciano, E. M., & Testa, M. G. (2017). Delivering public value through open government data initiatives in a Smart City context. *Information Systems Frontiers*, *19*, 213–229. https://doi.org/10.1007/s10796-016-9673-7
31. Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229–252. https://doi.org/10.1093/jopart/mum015
32. Purdy, J. M. (2012). A framework for assessing power in collaborative governance processes. *Public Administration Review*, *72*(3), 409–417. https://doi.org/10.1111/j.1540-6210.2011.02525.x
33. Scholl, H. J., & Klischewski, R. (2007). E-Government integration and interoperability: Framing the research agenda. *International Journal of Public Administration*, *30*(8–9), 889–920. https://doi.org/10.1080/01900690701402668
34. Siggelkow, N. (2007). Persuasion with case studies. *Academy of Management Journal*, *50*(1), 20–24. https://doi.org/10.5465/AMJ.2007.24160882
35. Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): A 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care*, *19*(6), 349–357. https://doi.org/10.1093/intqhc/mzm042
36. Tracy, S. J. (2010). Qualitative quality: Eight 'Big-Tent' criteria for excellent qualitative research. *Qualitative Inquiry*, *16*(10), 837–851. https://doi.org/10.1177/1077800410383121
37. Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A framework for evaluation in Design Science Research. *European Journal of Information Systems*, *25*(1), 77–89. https://doi.org/10.1057/ejis.2014.36

38. World Food Programme. (2025). *State of School Feeding Worldwide 2024*. Rome: WFP. https://doi.org/10.71958/wfp130772

Figures

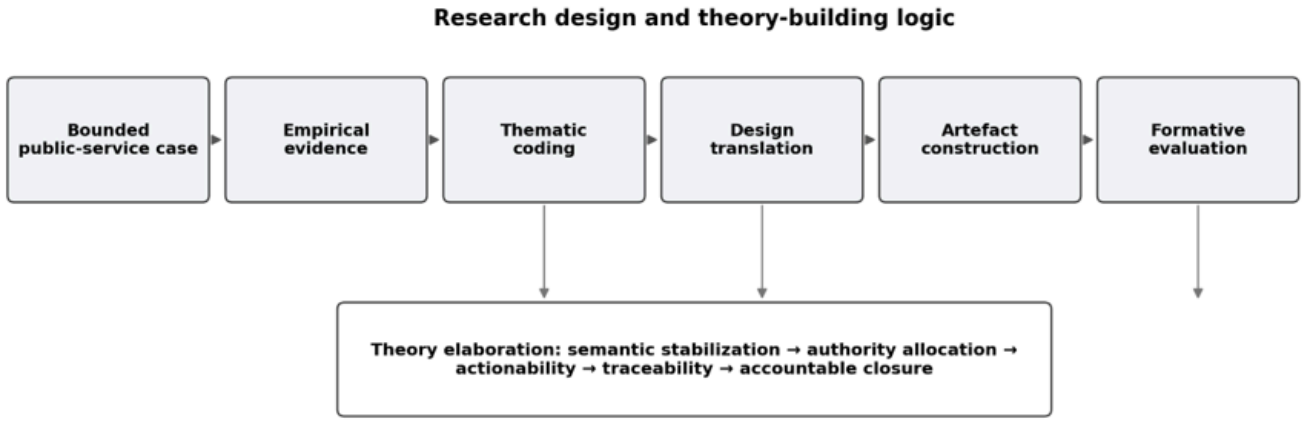


Figure 1

Research design and theory-building logic

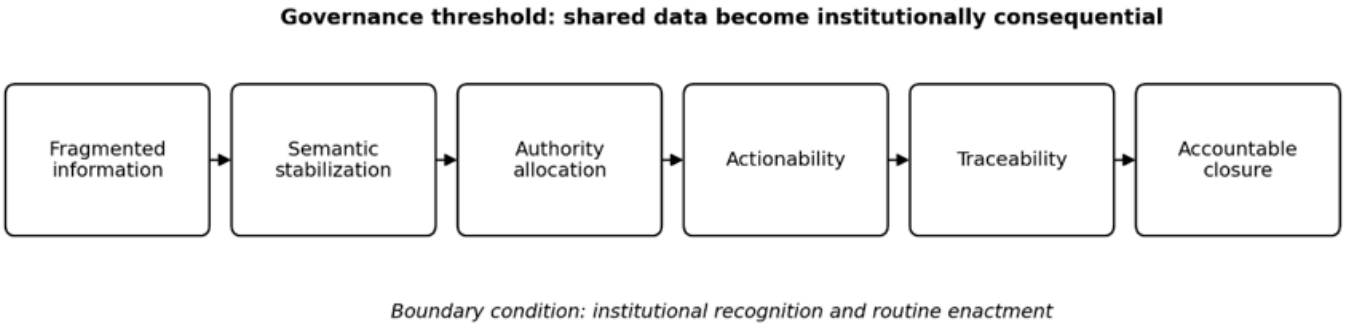


Figure 2

Empirically derived pathway from fragmented information to governance-bearing interoperability