Journal Governance Society
e-ISSN: 3064-2337 p-ISSN: 3064-2329

Vol 3, No 1, May (2026): Page no: 19-41
Available online at
https://journal.austrodemika.org/index.php/jgs

Analysis Risk-Based Digital Governance in an Archipelagic Local Government: A Document-Based Study of the Lingga Regency Fisheries Office, Indonesia

Kurnia Ananda Putri[1], Kamaruddin Kamaruddin[2]

[1,2]Universitas Maritim Raja Ali Haji. Tanjungpinang City. Indonesia

Correspondence: kurniaanandaputri5@gmail.com[1]

Received: November 19, 2025 | Revised: April 10, 2025 | Accepted: May 29, 2026

https://doi.org/10.69812/jgs.v3i1.201

ABSTRACT

Digital transformation has become an institutional requirement for local governments, yet the expansion of digital reporting, licensing, supervision, and public-service systems also creates operational, informational, organizational, and accountability risks. This study examines how risk management is embedded in the digital governance of the Lingga Regency Fisheries Office, an agency operating in an archipelagic jurisdiction where dispersed settlements, uneven connectivity, and cross-agency dependence intensify the consequences of digital disruption. A qualitative document-analysis design was employed. The evidence corpus comprised the agency's 2024 Government Agency Performance Report, applicable national and regional regulations, organizational documents, statistical publications, and peer-reviewed studies on digital government, data governance, information security, and enterprise risk management. Data were reduced, coded, compared, and synthesized into a risk register, an indicative maturity profile, and a phased governance roadmap. The findings reveal a performance–risk paradox. The agency reported aggregate programme achievement of 99.71%, with several output indicators reaching or exceeding their targets, but the available documentation does not demonstrate a fully institutionalized digital-risk management cycle. Risk identification and operational control are visible in fragmented forms, whereas continuous monitoring, incident response, tested recovery, explicit risk ownership, interoperability governance, and systematic workforce development remain underdeveloped or insufficiently documented. The study argues that high output achievement should not be treated as evidence of digital resilience. It proposes a risk-based digital governance model that connects Indonesia's Electronic-Based Government System, performance accountability, One Data principles, information-security controls, and inter-agency coordination.

Keyword: Digital Governance, Risk Management, Public-Sector Digital

INTRODUCTION

Digital transformation in government is no longer confined to converting paper records into electronic files or adding online interfaces to established

administrative routines. It increasingly involves the redesign of organizational processes, decision rights, service relationships, and data flows across institutional boundaries. Mergel et al. (2019) describe public-sector digital transformation as a holistic process that changes services, processes, and organizational culture, while Vial (2019) emphasizes that digital technologies alter value-creation pathways and require coordinated strategic responses. For local governments, this broader transformation creates opportunities to shorten service chains, standardize reporting, improve traceability, and provide decision makers with more timely information. At the same time, it produces new dependencies on infrastructure, software, data quality, external providers, and staff competence. The central governance challenge is therefore not whether technology should be adopted, but whether digital change can be governed in a way that remains reliable, accountable, lawful, and responsive when systems fail or operating conditions change.

The risk dimension is particularly important in public organizations because digital disruption can affect statutory duties, public resources, citizens' rights, regulatory enforcement, and institutional legitimacy. Information-security scholarship shows that public administration must protect confidentiality, integrity, and availability while also preserving transparency and accessibility, objectives that can conflict when control systems are poorly designed (Szczepaniuk et al., 2020). Data governance research similarly demonstrates that trustworthy digital systems require clear authority over data definitions, quality, access, sharing, retention, and accountability throughout the data life cycle (Janssen et al., 2020; Bernardo et al., 2024). Consequently, digital risk cannot be reduced to cyberattack prevention. It includes inaccurate input, incomplete records, network interruption, duplicated procedures, unauthorized disclosure, weak recovery arrangements, incompatible databases, unclear ownership, vendor dependence, and decisions made from data that are timely in appearance but unreliable in substance.

These concerns have become more visible since the COVID-19 pandemic accelerated the use of remote work, online services, and digital coordination. Comparative research indicates that the pandemic acted as an organizational shock that compelled public agencies to improvise digital solutions, but the durability of those solutions depended on leadership, institutional capacity, and the ability to integrate temporary innovations into stable governance arrangements (Eom & Lee, 2022; Moser-Plautz & Schmidthuber, 2023). This experience is relevant beyond emergency response. When agencies expand digital practices without simultaneously strengthening risk ownership, business continuity, information assurance, and learning mechanisms, they may achieve short-term output gains while accumulating hidden vulnerabilities. Adaptive governance therefore requires stability in core values and accountability arrangements together with flexibility in operational decisions, technologies, and partnerships (Janssen & van der Voort, 2016; Wang et al., 2018).

Indonesia has developed a substantial regulatory architecture for this transition. Presidential Regulation No. 95 of 2018 established the Electronic-Based Government System, commonly known as SPBE, as a framework for integrated, effective, transparent, and accountable digital government. Presidential Regulation No. 39 of 2019 introduced the One Data Indonesia principles of data standards, metadata, interoperability, and reference codes, while the Ministry of Administrative and Bureaucratic Reform Regulation No. 5 of 2020 provided specific guidance for SPBE risk management. The National SPBE Architecture under

Presidential Regulation No. 132 of 2022 and the acceleration of integrated national digital services under Presidential Regulation No. 82 of 2023 further reinforce the expectation that digital systems should be coordinated rather than developed as isolated applications. These instruments sit alongside the Government Agency Performance Accountability System under Presidential Regulation No. 29 of 2014, which requires agencies to connect planning, measurement, reporting, and performance evaluation. Together, the regulations imply that digitalization, data governance, risk management, and performance accountability should function as one institutional system rather than as separate compliance projects.

The Lingga Regency Fisheries Office provides a strategically relevant setting in which to examine this problem. Lingga Regency is an island jurisdiction in the Riau Islands Province, and its territorial dispersion creates practical difficulties for service access, supervision, data collection, coordination, and network reliability. The source manuscript reports an area of approximately 2,204 square kilometres, a population increase from 98,633 people in 2020 to about 102,474 in 2023, and an administrative structure comprising 13 subdistricts, 7 urban villages, and 82 villages. The official statistical profile also portrays a population structure with substantial younger age cohorts, indicating sustained demand for responsive public administration and reliable data services (Badan Pusat Statistik Kabupaten Lingga, 2024). In this setting, digital systems may reduce the cost of distance, but the same distance can magnify the effects of unstable connectivity, delayed synchronization, limited technical support, and inconsistent operating practices across locations.

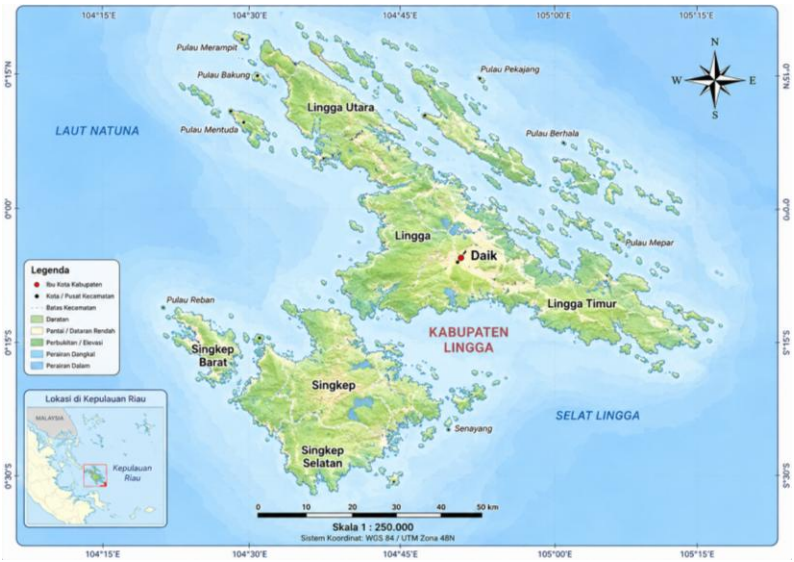

Figure 1. Geospatial map of Lingga Regency
Source: User-provided geospatial map of Kabupaten Lingga

The Fisheries Office carries responsibilities that combine economic development, resource governance, regulatory compliance, and public-service delivery. Its functions include fisheries-resource supervision, aquaculture development, product-quality improvement, facilitation of micro and small businesses, and performance reporting under the regional administrative structure (Lingga Regency Government, 2022). The source material also describes rapid growth in vannamei shrimp-pond activity, including approximately 70 permit applications, nearly 40 operating ponds, and investment approaching IDR 60 billion. These figures are treated in this study as contextual claims reported in the

reviewed manuscript rather than independently audited statistics. Nevertheless, they illustrate why licensing records, environmental monitoring, business data, and cross-agency coordination with environmental, investment, and fisheries-control institutions require dependable digital governance. Data errors or delays in this domain can affect not only administrative efficiency but also compliance, environmental safeguards, investment certainty, and the legitimacy of government oversight.

The agency's 2024 performance report presents a second reason for selecting the case. The document reports aggregate programme achievement of 99.71%, several output indicators at 100%, and production of processed and marketed fishery products of 115.4 tons against a 105-ton target (Lingga Regency Government, 2024). Such performance is significant, but it does not automatically establish that the underlying digital system is resilient. Output indicators usually show whether planned products or activities were delivered; they do not necessarily show whether critical data assets are inventoried, access rights are reviewed, backups are recoverable, incidents are recorded, cross-agency datasets are interoperable, or staff can sustain operations during disruption. Treating performance achievement as a proxy for digital-risk maturity may therefore conceal a gap between visible administrative success and the institutional safeguards required to maintain that success.

Conceptually, the present study is grounded in the view that digital governance should be understood as an institutional transformation rather than a narrowly technical upgrade. Digital systems alter how authority is exercised, how data are governed, and how accountability is demonstrated across organizational routines. This perspective draws on research showing that digital government emerges from the interaction of administrative structures, technological infrastructures, data arrangements, and public-value expectations rather than from technology adoption alone (Cordella & Tempini, 2015; Dawes, 2009; Janowski, 2015; Janssen et al., 2020; Mergel et al., 2019; Meijer & Bolívar, 2016; Vial, 2019). In this sense, risk management is not an external compliance device but an internal governance mechanism that helps public organizations maintain continuity, legitimacy, and service quality while operating under conditions of uncertainty.

The analytical emphasis on risk is further supported by studies demonstrating that sustainable digital transformation depends on organizational readiness, adaptive governance, reliable information stewardship, and clear institutional design. Adaptive and data-driven government requires not only interoperable systems but also explicit arrangements for ownership, monitoring, learning, and control (Bannister & Connolly, 2014; Gil-Garcia et al., 2018; Janssen & van der Voort, 2016; Klievink et al., 2017; Luna-Reyes & Gil-Garcia, 2014; Scholta et al., 2019; Tangi et al., 2021; Wang et al., 2018; Wirtz et al., 2019). For public organizations operating in dispersed territories, these issues are intensified because network instability, uneven digital capacity, and fragmented workflows can quickly translate into accountability problems, service interruption, or data-quality failures.

Previous studies offer important insights but leave a contextual and analytical gap. Digital-government research has explained organizational transformation, institutional co-evolution, adaptive governance, transparency, and data governance (Cordella & Tempini, 2015; Janowski, 2015; Luna-Reyes & Gil-Garcia, 2014; Saldanha et al., 2022), while risk-management studies have developed systematic approaches to identifying, assessing, treating, and

monitoring uncertainty (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017; International Organization for Standardization [ISO], 2018). However, less attention has been paid to how these bodies of knowledge intersect in a small or medium-sized local agency operating across an archipelagic territory. The practical problem is not simply the absence of sophisticated technology; it is the institutional challenge of linking digital assets, performance accountability, inter-agency data exchange, human capacity, and continuity arrangements under constrained conditions.

This study addresses that gap by asking: How is digital risk management reflected in the governance arrangements, performance documentation, and operating context of the Lingga Regency Fisheries Office, and what institutional model could strengthen accountability and effectiveness? The study has three objectives. First, it identifies the principal digital-risk themes supported by the document corpus. Second, it assesses the indicative maturity of governance capabilities without presenting the assessment as a technical audit. Third, it develops a phased roadmap that aligns agency-level action with SPBE, SAKIP, One Data Indonesia, interoperability requirements, and public-sector accountability. The theoretical contribution is a context-sensitive explanation of the performance–risk paradox in local digital government. The practical contribution is an implementable governance design for an island-based fisheries agency whose digital transformation depends on both technological reliability and institutional coordination.

To guide the document analysis, this study uses an analytical framework that links the archipelagic context of Lingga Regency with four operational domains: digital processes, risk-management functions, accountability mechanisms, and institutional capacity. Figure 2 summarizes the framework used to code the documents and interpret the relationship between reported performance and the maturity of digital-risk governance.

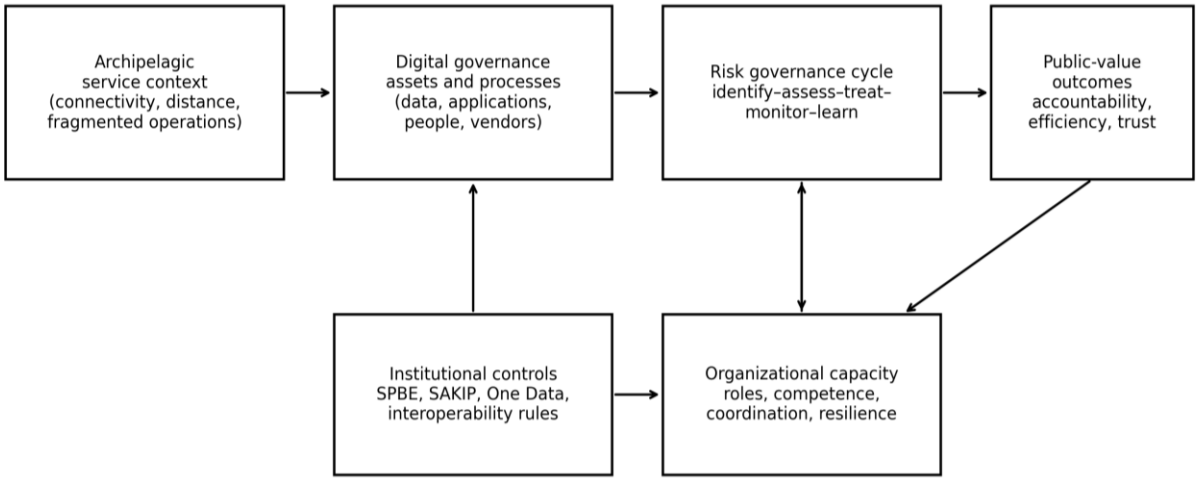

Figure 2. Analytical framework for risk-based digital governance.
Source: Author, 2026

The framework positions risk management as a cross-cutting analytical lens rather than a separate policy field. It allows the study to evaluate how documentary evidence reflects asset awareness, control procedures, monitoring practices, data governance, and adaptive capacity, while also clarifying why strong performance reporting may coexist with weak formalization of digital-risk oversight.

RESEARCH METHOD

This study adopted a qualitative case-study design based on systematic document analysis. Document analysis is appropriate when institutional processes, formal responsibilities, policy expectations, and reported performance are embedded in administrative records and regulations, and when the research objective is to interpret how those materials construct an organizational reality (Bowen, 2009). The design was not intended to test causal effects or calculate the probability of technical failure. Instead, it examined the coherence between reported digital practices, formal governance requirements, organizational responsibilities, and recognized risk-management capabilities. The Fisheries Office was treated as an embedded case within the broader institutional systems of Lingga Regency and Indonesia's SPBE framework, allowing agency-level evidence to be interpreted in relation to regional geography, national regulation, and the literature on digital government.

The primary case document was the 2024 Government Agency Performance Report of the Lingga Regency Fisheries Office, as identified and summarized in the source manuscript. The analysis also used Lingga Regent Regulation No. 45 of 2022 on the agency's position, organizational structure, duties, functions, and work procedures; the regional statistical profile; and the regulatory instruments governing SAKIP, SPBE, SPBE risk management, One Data Indonesia, the national SPBE architecture, integrated digital services, and data interoperability. Peer-reviewed literature was selected to provide theoretical and comparative lenses concerning public-sector digital transformation, organizational change, adaptive governance, information security, data governance, transparency, and enterprise risk management. The evidence corpus was purposive rather than bibliometric: documents were included when they directly informed the case, specified a governing requirement, or supplied a concept needed to interpret the findings.

The study applied four quality criteria to the documentary corpus. Authority referred to whether a document was issued by a responsible institution or published in a peer-reviewed outlet. Relevance referred to whether it addressed the Fisheries Office, the Lingga context, or a capability in the analytical framework. Temporal applicability referred to whether the document governed or described the period under study, while allowing foundational literature to establish concepts. Evidentiary specificity referred to whether a statement could support a concrete analytical claim rather than a general aspiration. These criteria were important because documents serve different purposes. A performance report may be strong evidence of reported target achievement but weak evidence of incident-response capability; a regulation may establish an obligation but not prove implementation; and a scholarly framework may explain significance but cannot substitute for case evidence.

The coding process combined deductive and inductive procedures. Deductive codes were derived from the conceptual framework and the SPBE risk-management cycle: governance mandate, asset and data inventory, risk identification, assessment, control, monitoring, incident response, recovery, human capacity, interoperability, accountability, and learning. Inductive codes captured case-specific pressures that emerged from the source material, including archipelagic connectivity, manual verification, licensing growth, cross-agency dependence, dispersed service locations, and the coexistence of high performance with limited documented risk institutionalization. Coding was conducted at the level of substantive claims. A passage could receive multiple codes when it linked, for example, data validation with accountability and operational delay. The coded

evidence was then condensed into thematic matrices to compare obligations, reported practices, risk implications, and evidence gaps.

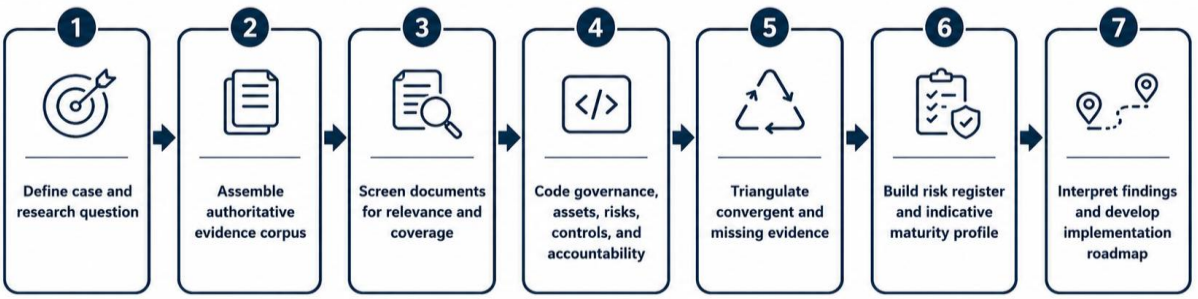

Figure 3. Document-analysis workflow used in the study.
Source: Developed by the authors.

Analysis proceeded through data condensation, display, and conclusion drawing, consistent with the interactive qualitative approach of Miles et al. (2014). First, statements were extracted and grouped by analytical dimension. Second, the groups were displayed in an evidence matrix, contextual-pressure table, risk register, and indicative maturity profile. Third, patterns were interpreted through repeated comparison between case documents, regulations, and scholarly concepts. Negative evidence was handled cautiously. The absence of a documented control was not treated as proof that the control did not exist; it was recorded as an absence of demonstrable institutionalization in the available corpus. This distinction is central to the study's claims. The results describe documented maturity and governance visibility, not the technical condition of every system or the behaviour of every employee.

The risk register was constructed as an analytical instrument rather than an official agency register. Likelihood and impact were scored on five-point ordinal scales to support prioritization. Scores were based on contextual exposure and the consequences described in the documents and literature, not on incident-frequency data. The maturity profile used a five-level scale: 1, ad hoc; 2, repeatable but fragmented; 3, defined; 4, managed and measured; and 5, optimized and continuously improved. Scores were assigned only where the documentary evidence permitted a reasoned judgement and are presented as indicative. Their purpose is to show relative strengths and gaps, especially the contrast between performance accountability and operational resilience, and to provide a baseline for future validation through interviews, system inspection, log analysis, and control testing.

Trustworthiness was strengthened through source triangulation, conceptual triangulation, and an audit trail. Source triangulation compared agency reporting, legal requirements, organizational provisions, statistical context, and peer-reviewed research. Conceptual triangulation compared digital-government, data-governance, information-security, adaptive-governance, and enterprise-risk perspectives so that no single framework dominated the interpretation. The audit trail consisted of the coding dimensions, evidence tables, scoring assumptions, and explicit qualifiers used in the results. Dependability was also supported by separating reported facts from proposed actions. For example, the 99.71% achievement is reported as a documentary finding, whereas the maturity scores and roadmap are clearly identified as analytical products. This approach enhances transparency and allows later fieldwork to confirm, revise, or reject specific interpretations.

The study has methodological boundaries. It did not include interviews, direct observation, penetration testing, configuration review, incident logs, or independent verification of every quantitative claim in the source manuscript. It therefore cannot determine the actual frequency of security events, the technical effectiveness of backups, or the perceptions of service users. It also does not compare Lingga statistically with other regencies. These limitations are deliberate rather than incidental: the study asks what can be learned from the documentary record and what that record reveals about governance visibility. The resulting framework should be understood as a diagnostic foundation for a subsequent mixed-method or field-based assessment, not as a certification of compliance or an external audit opinion.

RESULTS AND DISCUSSION

1. Documentary Evidence and Institutional Context

The documentary evidence portrays a governance environment in which territorial fragmentation, growing regulatory activity, and performance pressure interact. Figure 1 presents Lingga Regency as an archipelagic jurisdiction whose dispersed islands make digital connectivity, field supervision, data synchronization, and service continuity central governance concerns. The map therefore provides a direct spatial explanation for why a digital system that performs adequately at the regency headquarters may still encounter uneven access, delayed transmission, or limited technical support across operational locations. Read together with the official demographic and administrative information reviewed in this study, the visualization indicates that the value of digital governance in Lingga depends not only on the availability of applications but also on their capacity to remain accessible, reliable, and institutionally coordinated across a geographically fragmented territory.

The institutional context adds complexity because fisheries administration is inherently interdependent. The Fisheries Office may collect or produce information on aquaculture activities, business facilitation, production, supervision, and product quality, but licensing, environmental oversight, spatial information, investment administration, and fisheries-resource control can involve other governmental units. The source material specifically identifies coordination needs involving the environmental agency, the investment and one-stop service agency, and fisheries surveillance authorities. Where each institution maintains separate records, the agency may need to reconcile identifiers, dates, locations, permit status, and inspection results manually. This creates an interoperability risk: information can be individually accurate within one system yet collectively inconsistent across the governance network. The risk is not solved merely by exchanging spreadsheets; it requires shared definitions, reference codes, metadata, access rules, and responsibility for correcting discrepancies.

Table 1. Analytical dimensions of risk-based digital governance

Dimension	Core question	Documentary indicators
Governance mandate	Who authorizes and oversees digital risk?	Formal mandate; committee or team; reporting line; escalation criteria; integration with planning.
Assets and data	What must be protected and sustained?	Inventory of systems, devices, datasets, owners, locations,

Dimension	Core question	Documentary indicators
		dependencies, classifications, and retention.
Risk cycle	How is uncertainty converted into action?	Common criteria; risk register; ownership; treatment plans; residual-risk acceptance; review schedule.
Information security	How are confidentiality, integrity, availability, authenticity, and traceability maintained?	Access control; validation; logging; change control; backup; restoration; incident evidence.
Data governance	How are data quality and responsible use governed?	Standards; metadata; reference codes; stewardship; quality rules; correction and sharing procedures.
Interoperability	How are cross-agency exchanges controlled?	Authoritative sources; interfaces or exchange formats; update frequency; discrepancy resolution; agreements.
Human capacity	Can people operate and sustain controls?	Role-based competence; training; exercises; job aids; separation of duties; support arrangements.
Accountability and public value	Can the agency explain performance, risk, and corrective action?	Linked performance and risk indicators; traceable evidence; complaint/correction channels; management review.
Resilience and learning	Can critical services continue and improve after disruption?	Continuity procedures; recovery objectives; restoration tests; after-action review; tracked improvements.

Source: Author, 2026

Table 1 summarizes the conceptual dimensions used to interpret the case and translates them into observable documentary indicators. The table demonstrates that risk-based digital governance is multi-dimensional. A strong agency would not only possess policies or applications, but would be able to show an inventory of assets and data, assigned ownership, documented risk criteria, operating controls, monitoring evidence, incident and recovery procedures, trained personnel, interoperable data arrangements, and performance reports that connect controls to public outcomes. This integrated view is important because partial strength can mask systemic weakness. For example, comprehensive performance reporting may coexist with poor recovery readiness, while secure access controls may coexist with low data quality. The dimensions therefore function as a balanced diagnostic rather than a single compliance score.

The evidence corpus and its analytical purpose are set out in Table 2. The table shows that no individual document can answer the research question on its own. The LKjIP is the principal source for performance claims and indications of digitized reporting, but it was not designed as an information-security or continuity

report. Organizational regulations clarify formal duties but may not describe daily control practices. National regulations establish mandatory principles but do not confirm local implementation. Statistical publications explain geographic and demographic exposure, while peer-reviewed studies supply concepts and comparative findings. The results that follow are therefore based on convergence across sources. Where convergence is absent, the study uses terms such as "not demonstrated," "insufficiently documented," or "indicative" rather than asserting non-existence.

Table 2. Documentary corpus and analytical use

Document group	Principal contribution	Analytical limitation
2024 Fisheries Office LKjIP	Reported targets, outputs, achievement rates, and evidence of performance reporting.	Not designed as a technical security, continuity, or control-effectiveness report.
Lingga organizational regulation	Formal mandate, structure, duties, and functional responsibilities.	Does not necessarily describe informal practices or current technical arrangements.
BPS Lingga statistical profile	Territorial, demographic, and service context.	Provides contextual exposure rather than agency control evidence.
SPBE and SAKIP regulations	National obligations for digital government, risk, architecture, and accountability.	Establish requirements but do not prove implementation.
One Data and interoperability regulations	Principles for standards, metadata, reference codes, and controlled exchange.	Require local operational agreements and stewardship.
Peer-reviewed literature	Conceptual lenses, comparative evidence, and established risk or governance practices.	Cannot substitute for case-specific observation or technical testing.
Source manuscript and embedded figures	Case narrative, reported quantitative details, and visual context used as the revision basis.	Some contextual claims require future verification against primary records.

Source: Author, 2026

Taken together, the documents provide complementary forms of evidence: organizational regulations clarify authority, performance reports illuminate formal achievement and programme routines, while digital-government regulations provide the normative benchmark against which gaps in risk formalization can be assessed. This combination strengthens the analytical credibility of the study because no single source is treated as sufficient on its own.

2. Reported Performance and the Performance–Risk Paradox

The performance evidence is strong in relation to output delivery. The 2024 LKjIP reports average or aggregate achievement of 99.71% across programmes and activities. The source material also identifies several indicators at 100%,

including documents resulting from fisheries-resource supervision, quality-development activities, and facilitation of micro and small fisheries businesses. Production in processing and marketing reached 115.4 tons against a target of 105 tons, equivalent to approximately 109.9% of target. Figure 4 visualizes these values to clarify the distinction between target achievement and risk maturity. The chart shows that the agency's reported output performance is consistently high; however, none of these percentages directly measures availability, integrity, confidentiality, recoverability, interoperability, or incident readiness. They establish that activities were delivered, not that the digital environment supporting them is resilient.

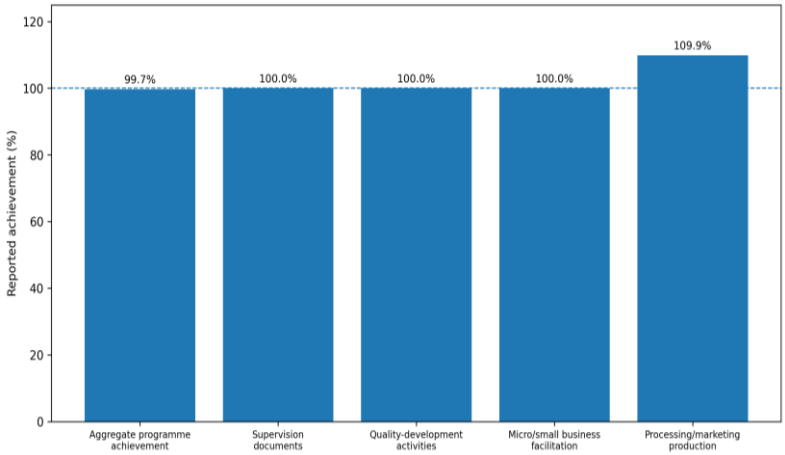

Figure 4. Selected performance achievements reported in the 2024 LKjIP.
Source: Author, 2026

The central finding is a performance–risk paradox: the Fisheries Office demonstrates high reported achievement while the documentary record shows uneven institutionalization of digital-risk governance. This is not a criticism of the reported performance. Rather, it reveals that output accountability and resilience accountability answer different questions. Output accountability asks whether activities and targets were completed; resilience accountability asks whether the organization understands the dependencies that enabled completion, can continue critical functions during disruption, can recover data and services, and can explain residual risk. COSO (2017) links risk to strategy and performance precisely because target achievement can be fragile when the conditions supporting it are not controlled. For Lingga, the high-performance rate should be used as a platform for the next stage of maturity, not as evidence that risk management is already complete.

This distinction advances digital-government theory by showing why transformation must be evaluated as organizational and institutional change. The presence of electronic reporting does not itself demonstrate transformation; it may represent digitized bureaucracy in which existing routines are performed through new media. Cordella and Tempini (2015) caution against assuming that ICT automatically replaces or simplifies bureaucratic structures, and Luna-Reyes and Gil-Garcia (2014) show that technology co-evolves with organizational and institutional conditions. The Lingga case supports these arguments. Manual validation, cross-agency fragmentation, and unclear risk ownership are not merely technical defects. They are manifestations of how authority, evidence, and

coordination have been organized. Sustainable reform therefore requires process and governance redesign alongside application development.

3. Contextual Pressures and Archipelagic Resilience

Table 3 identifies the principal contextual pressures and their governance implications. Archipelagic geography raises availability and service-continuity concerns; dispersed operations complicate support and standardization; aquaculture growth increases transaction volume and regulatory consequence; cross-agency dependence creates interoperability and ownership risks; performance pressure can encourage attention to output completion over control evidence; and uneven digital capability can produce inconsistent practices. These pressures are mutually reinforcing. A connectivity interruption, for example, may lead to delayed entry, which increases manual work, which creates version differences, which can then affect reporting accuracy or licensing follow-up. Risk treatment must therefore address chains of dependency rather than isolated technical problems.

Table 3. Contextual pressures and digital-governance implications

Contextual pressure	Risk mechanism	Governance implication
Archipelagic geography	Connectivity loss, delayed support, and difficult physical verification.	Offline continuity, synchronization rules, redundancy, and location-sensitive support.
Dispersed service and supervision locations	Inconsistent procedures and uneven access to expertise.	Common standards, job aids, remote support, and role-based training.
Growth of aquaculture and licensing activity	Higher transaction volume and greater consequences of inaccurate or delayed data.	Validation rules, authoritative records, workflow tracking, and escalation.
Cross-agency dependence	Inconsistent identifiers, duplicated records, and unclear correction authority.	Data stewardship, interoperability standards, agreements, and discrepancy resolution.
High performance expectations	Priority may shift toward output completion rather than control evidence.	Link risk indicators and assurance evidence to SAKIP reviews.
Hybrid manual–digital processes	Version differences, repeated entry, and delayed reconciliation.	Define the authoritative record, logging, reconciliation, and controlled fall-back procedures.
Limited specialist resources	Risk knowledge may remain concentrated in individuals or vendors.	Cross-functional team, documented procedures, succession, and shared regional services.

Source: Author, 2026

The archipelagic context extends this literature by foregrounding geographic resilience. Digital-government studies often emphasize integration and seamless service, but integration can create centralized dependencies that are vulnerable when local connectivity is uneven. In Lingga, a resilient design should combine common standards with operational redundancy. Critical field functions need documented offline or low-bandwidth procedures, locally available reference information, secure temporary storage, and rules for later synchronization. Central systems need backup, recovery, and support arrangements that account for travel time and remote locations. This is an example of adaptive governance: the core standards remain stable, but operational methods vary according to conditions, and deviations are recorded and reconciled (Janssen & van der Voort, 2016; Wang et al., 2018).

4. Digital-Risk Profile, Capability Maturity, and Organizational Gaps

The documentary record shows the clearest maturity in performance accountability. Targets, outputs, and achievement rates are formalized, and the agency can report results through the LKjIP. Risk identification is also visible at an operational level because the source material recognizes connectivity constraints, data-validation needs, staff capability, and the importance of coordination.

Table 4. Indicative digital-risk register

No.	Risk Theme	Likelihood	Impact
1	Connectivity interruption across island locations	Likely (4)	Major (4)
2	Data-entry or validation errors	Likely (4)	Major (4)
3	Unauthorized exposure of personal	Possible (3)	Severe (5)
4	Application or server downtime	Possible (3)	Major (4)
5	Inter-agency data fragmentation	Likely (4)	Major (4)
6	Uneven staff digital capability	Likely (4)	Moderate (3)
7	Weak backup or recovery mechanisms	Possible (3)	Severe (5)
8	Vendor or platform dependency	Possible (3)	Moderate (3)
9	Non-compliance with SPBE, data, or security requirements	Unlikely (2)	Major (4)

Source: Author, 2026

The indicative risk register in Table 4 consolidates ten risk themes. The highest-priority themes combine high impact with plausible exposure: connectivity interruption, data-validation error, inter-agency fragmentation, weak backup and recovery, and unauthorized exposure of personal or business information. Application downtime, uneven workforce capability, manual–digital duplication, vendor dependency, and regulatory non-compliance also require treatment. The controls proposed in the table are proportionate to a local agency: not all risks require expensive technology.

Figure 5 presents the risk themes on an indicative likelihood–impact matrix. The concentration in the upper-middle and upper-right areas suggests that the agency's most material digital risks are not rare catastrophic scenarios alone; they include recurring operational conditions that can create major cumulative effects. Connectivity, data validation, and fragmentation are likely to arise through normal work rather than malicious activity.

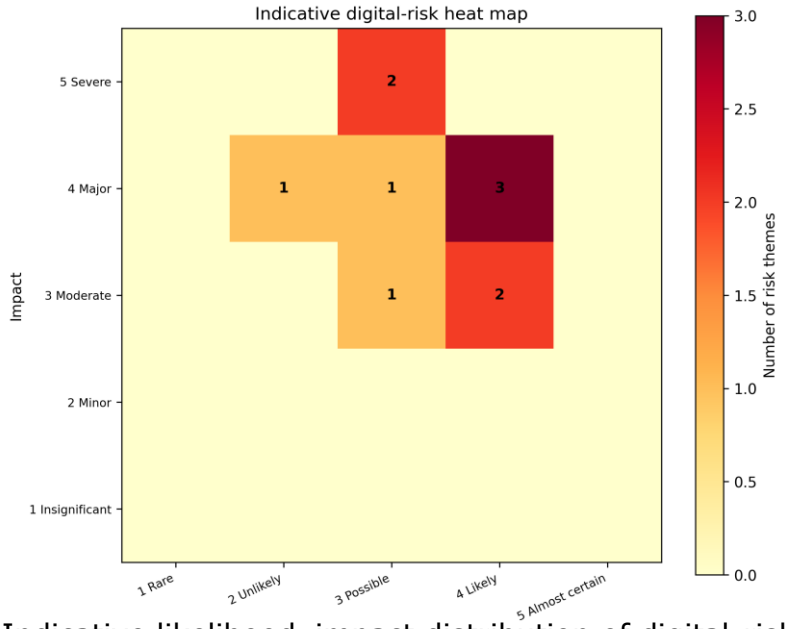

Figure 5. Indicative likelihood–impact distribution of digital-risk themes.
Source: Author, 2026

This finding supports a broad risk-governance approach. Cybersecurity controls remain necessary, but resilience also depends on mundane administrative disciplines: standardized data entry, clear fall-back procedures, version control, reconciliation, support arrangements, and tested restoration. A risk programme focused only on external attacks would overlook many of the conditions most likely to affect everyday accountability and service continuity. The indicative maturity scores in Table 5 and Figure 6 reinforce the performance–risk paradox.

Accountability and reporting receive the highest score because performance documentation is visible and structured. Risk identification is moderately developed because several operational concerns are recognized. Governance, asset inventory, and controls are assessed as partially defined but fragmented. Assessment, human capacity, and interoperability remain at an emerging level, while continuous monitoring and incident response are the weakest documented capabilities. The radar profile is intentionally uneven: it illustrates that digital maturity is not a single line of progression. An agency can be comparatively advanced in reporting and still be vulnerable in recovery or cross-system coordination. The profile should be validated by the agency through workshops and evidence review, but it provides a practical starting point for prioritization.

Table 5. Indicative maturity profile

No.	Capability	Score (1–5)	Document-Based Interpretation
1	Governance and Policy	2.5	Formal digital-government obligations are established; however, an agency-specific mandate for integrated risk management is not clearly demonstrated.
2	Asset and Data Inventory	2.5	Digital records are evident, but a comprehensive and classified inventory specifying ownership, dependencies, and accountability is not demonstrated.

No.	Capability	Score (1–5)	Document-Based Interpretation
3	Risk Identification	3.0	Key operational risks are recognized in the case narrative and relevant regulatory context.
4	Risk Assessment	2.0	Standardized criteria for likelihood, impact, risk acceptance, and prioritization are not demonstrated in the available documents.
5	Control Implementation	2.5	Verification and administrative controls are in place, but their standardization and supporting evidence across the full control cycle remain uneven.
6	Continuous Monitoring	1.5	Evidence of a dedicated risk dashboard, monitoring thresholds, and regular risk-review mechanisms is not demonstrated.
7	Incident Response and Recovery	1.5	An incident taxonomy, recovery objectives, simulation exercises, and evidence of restoration testing are not demonstrated.
8	Human-Resource Capacity	2.0	Digital activities are performed, but structured capacity development in risk management, cybersecurity, data governance, and business continuity appears limited.
9	Interoperability	2.0	Coordination requirements are acknowledged; however, authoritative data sources and controlled data-exchange arrangements require further development.
10	Accountability and Reporting	3.5	Performance targets and achievements are well documented, although indicators related to resilience, risk, and service continuity remain limited.

Source: Author, 2026

The maturity pattern demonstrates that accountability-oriented routines are more developed than resilience-oriented routines. In practical terms, the institution appears more prepared to document what has been achieved than to continuously detect, prioritize, and learn from digital vulnerabilities, which is precisely why maturity enhancement should focus on ownership, monitoring, and institutionalized follow-up.

A particularly significant gap concerns formal ownership. The organizational regulation establishes the Fisheries Office's mandate and internal structure, but the reviewed material does not demonstrate a dedicated digital-risk function or a cross-functional risk team with explicit responsibilities. Creating a large specialist unit may be unrealistic for a local agency; however, the absence of a named coordinating mechanism can leave risks distributed across administrative, programme, and technical personnel without an integrated view. A proportionate solution is a digital-risk committee or working team chaired by a senior official, with representatives from planning, administration, programme fields, data or IT support, and internal oversight. The team would not replace operational responsibility. It would maintain the risk register, define standards, coordinate

treatment, review incidents, and ensure that material risks enter planning and performance discussions.

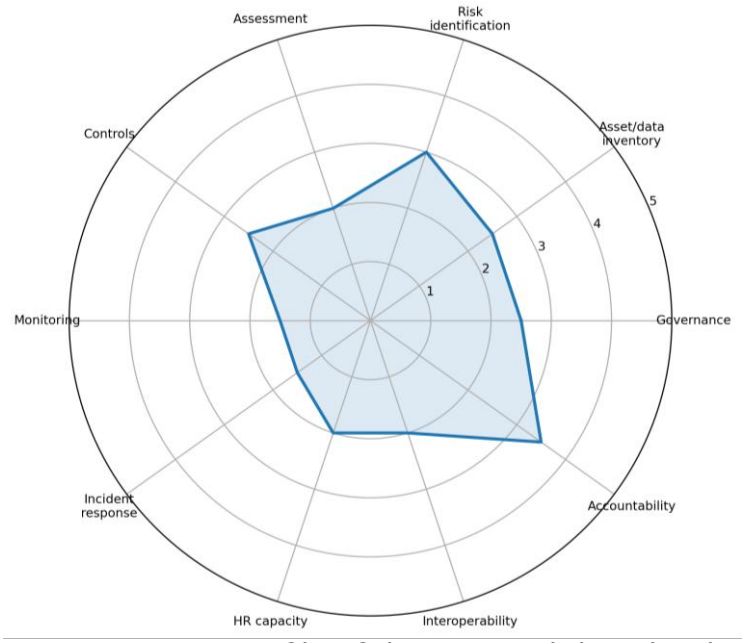

Figure 6. Indicative maturity profile of documented digital-risk capabilities.
Source: Author, 2026

Monitoring and incident learning are related gaps. The source material emphasizes achievement reporting but does not provide evidence of a digital-risk dashboard, incident taxonomy, recovery-time objectives, restoration tests, or lessons-learned reviews. Without these mechanisms, the agency may detect problems informally but struggle to aggregate patterns or demonstrate improvement. A simple monitoring system could track failed or delayed submissions, data-correction rates, duplicate records, system unavailability, unresolved access requests, backup completion, restoration-test results, and time to resolve incidents. These indicators should not become an additional reporting burden detached from operations. They should be selected because they reveal threats to strategic objectives and can trigger specific action when thresholds are exceeded.

Human capacity is both a risk source and a control. The source material notes that training has concentrated more heavily on fisheries-business management and product quality than on data security and digital-system management. This pattern is understandable because programme expertise is central to the agency's mandate, but digital duties now form part of programme delivery. Staff need role-specific capability: users require secure and accurate operating practices; validators require data-quality and anomaly-detection skills; managers require risk interpretation and escalation skills; and technical support personnel require configuration, backup, and recovery competence. Training should be reinforced by job aids, simulations, peer support, and supervision. One-off seminars are unlikely to change practice unless employees can apply the content to actual workflows and receive feedback.

Interoperability is the final major results theme. The growth of pond licensing and supervision intensifies the need to connect fisheries, environmental, investment, and surveillance information. The One Data framework and the interoperability regulation offer a basis for shared standards, but implementation

requires institutional agreements. The Fisheries Office should identify authoritative data elements, assign stewards, map data exchanges, define update frequencies, and establish a discrepancy-resolution process. Integration does not necessarily mean a single database. It may involve controlled interfaces or standardized exchange files, provided that provenance, authorization, and accountability are preserved. The key is to prevent multiple agencies from making decisions based on incompatible versions of the same business, permit, location, or compliance record.

The results also clarify the relationship between data governance and information security. In many organizations, security is assigned to technical personnel while data quality is assigned to programme units. The risk register shows that this separation is insufficient. A duplicate business identifier is a data-quality problem, but it can also cause unauthorized disclosure or incorrect enforcement. Excessive access is a security problem, but it often persists because data ownership is unclear. A failed backup is a technical problem, but its impact depends on retention rules and the availability of authoritative source documents. Janssen et al. (2020) argue that trustworthy data require integrated governance, and the Lingga case demonstrates that stewardship, access, interoperability, and continuity should be managed as connected responsibilities.

Accountability should likewise be designed into data and processes rather than added at the reporting stage. Saldanha et al. (2022) emphasize that digital transparency and accountability require institutional arrangements that allow decisions and responsibilities to be understood. For the Fisheries Office, this means recording who entered and validated data, which source was used, when a change occurred, how discrepancies were resolved, and which control supports a reported indicator. It also means giving business actors a clear route to correct inaccurate information or seek clarification. Such traceability can strengthen SAKIP because performance evidence becomes more reliable, and it can strengthen public trust because administrative decisions become explainable. The objective is not maximal disclosure; confidential data must remain protected. The objective is proportionate transparency about rules, status, responsibility, and correction.

5. Risk-Based Governance Model and Implementation Roadmap

A risk-based model also helps prevent indiscriminate technology investment. Digital transformation programmes sometimes respond to fragmentation by purchasing another application, even when the underlying problem is inconsistent definitions or unclear authority. The conceptual framework suggests a sequence: identify the public objective, map the process and data, determine risks and responsibilities, select controls, and only then decide whether technology is required. Some priorities in Lingga such as assigning data stewards, establishing a risk team, defining an authoritative record, and documenting fall-back procedures are primarily managerial. Others, such as automated validation, secure integration, monitoring dashboards, and early-warning analytics, may require technical investment.

The proposed governance model integrates five mechanisms. First, strategic alignment connects each critical digital process to a programme objective and public-value outcome. Second, ownership assigns responsibility for data, systems, controls, and residual risk. Third, the risk cycle identifies, assesses, treats, monitors, and reviews uncertainty using common criteria. Fourth, assurance provides evidence through access reviews, reconciliation, backup tests,

incident records, and internal evaluation. Fifth, learning converts incidents, near misses, user feedback, and performance anomalies into process improvement. These mechanisms correspond to SPBE risk management, SAKIP, One Data, and enterprise-risk principles, but the model translates them into an agency-level operating system. Its value lies in integration: each mechanism reinforces the others rather than generating separate documents.

Table 6 and Figure 7 present a three-phase roadmap. The foundation phase establishes governance, inventory, minimum continuity, and an initial register. The integration phase standardizes controls, develops interoperability arrangements, trains staff, and connects risk indicators to performance dashboards. The resilience phase introduces tested recovery, analytical early warning, continuous assurance, and stronger public accountability. The phases are cumulative but not rigid. A high-priority risk such as backup failure should be addressed immediately even if other foundation work is incomplete. Conversely, advanced analytics should not be introduced before data definitions and ownership are stable. The roadmap therefore combines time horizons with risk-based prioritization.

Table 6. Phased implementation roadmap

Phase	Priority actions	Evidence of completion
1. Foundation (0–6 months)	Issue mandate; form cross-functional team; identify critical services; inventory assets and data; establish initial register; implement minimum backup and fall-back procedures.	Signed mandate; membership and terms of reference; approved inventory; prioritized register; successful restoration record; continuity instructions.
2. Integration (6–18 months)	Standardize access, validation, change, incident, and reconciliation controls; deliver role-based training; define high-value inter-agency data exchanges; add risk indicators to SAKIP reviews.	Approved procedures; access-review records; training and exercise results; data-sharing specification; dashboard and management minutes.
3. Resilience (18–36 months)	Automate validation and alerts; test recovery scenarios; strengthen vendor assurance; conduct continuous monitoring and after-action review; publish proportionate accountability information.	Alert and anomaly reports; exercise results; service-level evidence; closed improvement actions; public-facing service and correction information.

Source: Author, 2026

The roadmap table emphasizes sequencing rather than simultaneity. By organizing activities into manageable phases, the model avoids overwhelming the institution and helps ensure that governance rules, control procedures, and learning mechanisms mature in a coordinated manner before more advanced automation or integration is pursued.

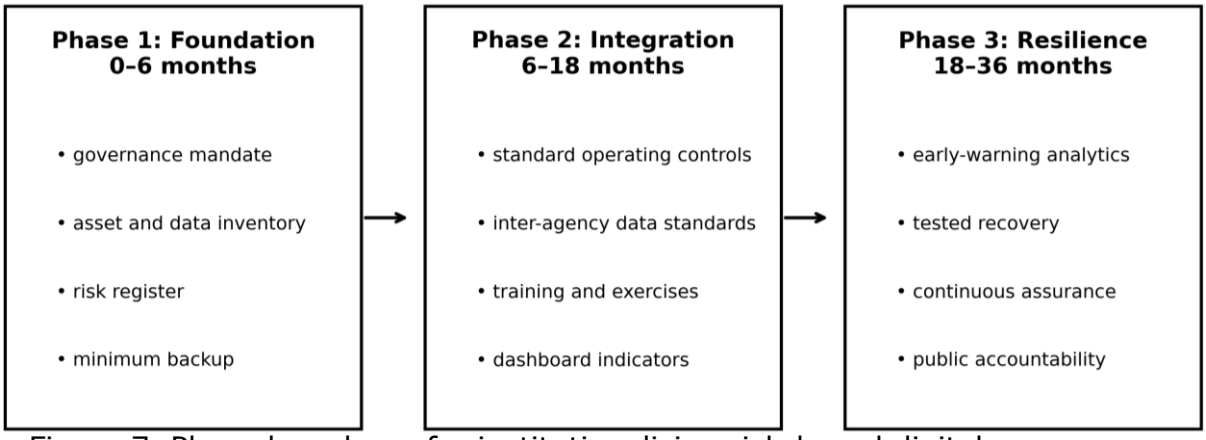

Figure 7. Phased roadmap for institutionalizing risk-based digital governance. Source: Author, 2026

During the foundation phase, the agency should issue a leadership mandate that defines purpose, scope, roles, and reporting lines. It should create a cross-functional digital-risk team and identify the services whose failure would most affect statutory duties or stakeholders. An asset and data inventory should record applications, devices, datasets, owners, locations, dependencies, access categories, backup arrangements, and retention requirements. The initial risk register should focus on the ten themes identified in this study and specify existing controls, gaps, owners, deadlines, and residual risk. Minimum continuity measures should include reliable backups, a restoration test, alternative communication channels, and documented offline procedures for critical work. These actions create visibility and can be achieved without waiting for a complex platform.

The integration phase should convert visibility into consistent practice. Standard operating procedures need to define access approval, data entry and validation, change management, backup, incident reporting, reconciliation, and third-party support. Training should be role-based and followed by exercises. Inter-agency work should begin with a small number of high-value data elements such as business identifiers, permit status, location, and supervision findings and establish agreed standards and exchange rules. The performance system should include a limited set of risk indicators linked to strategic objectives. For example, the agency could report the percentage of critical datasets with assigned stewards, the completion of backup and restoration tests, the rate of records requiring correction, the number of unresolved interoperability discrepancies, and the time required to restore a critical function.

The resilience phase should deepen monitoring and learning. Automated validation can detect incomplete fields, invalid reference codes, duplicate identities, unusual values, or inconsistent permit status. A dashboard can combine performance and risk indicators so managers see both delivery and vulnerability. Recovery arrangements should be exercised under realistic scenarios, including prolonged connectivity loss at an island location, corruption of a dataset, unauthorized access, and failure of a third-party service. Exercises should test decision authority, communication, evidence preservation, and service continuity, not merely technical restoration. After-action reviews should assign improvements and track completion. Over time, the agency can use incident and correction data to identify recurrent process weaknesses and target training or redesign.

The roadmap also requires coordination beyond the Fisheries Office. Regional leadership should clarify common SPBE architecture, information-security services, data standards, and support responsibilities. The

communications and informatics function can provide technical guidance, shared infrastructure, monitoring, and incident coordination; the planning and internal-supervision functions can connect risk to SAKIP and assurance; sectoral agencies can retain ownership of domain data while complying with common standards. External service providers should be governed through agreements that specify availability, support, security, data location, backup, exit arrangements, and incident notification. This whole-of-government design reduces duplication and prevents a small agency from carrying risks it cannot manage alone.

CONCLUSION

This study examined the implementation of risk management within the digital governance of the Lingga Regency Fisheries Office through a qualitative analysis of performance, regulatory, organizational, statistical, and scholarly documents. The evidence shows an agency with strong reported programme delivery and meaningful use of digital documentation, but it does not demonstrate a fully institutionalized cycle of digital-risk governance. The agency's 99.71% aggregate achievement and several indicators at or above target confirm administrative performance; however, the continued reliance on manual validation, archipelagic connectivity constraints, inter-agency data dependence, uneven capability, and limited documentary evidence of monitoring, incident response, tested recovery, and explicit ownership reveal a resilience gap. The main conclusion is therefore that output success and digital resilience are related but distinct dimensions of accountability.

Risk-based digital governance offers a way to connect these dimensions. For Lingga, the priority is not an isolated cybersecurity project or another stand-alone application. It is an integrated governance system that links SPBE risk management, SAKIP, One Data principles, interoperability, information security, continuity, and organizational learning. A proportionate institutional design should establish a cross-functional risk mandate, inventory critical assets and data, assign owners, maintain a prioritized register, standardize access and validation controls, test backup and recovery, develop role-based capability, and report a small set of risk indicators alongside programme performance. Inter-agency coordination should begin with authoritative identifiers and high-value data exchanges, supported by clear stewardship and discrepancy-resolution rules.

The proposed three-phase roadmap provides a practical sequence from foundation to integration and resilience. Its implementation would allow the Fisheries Office to preserve the benefits of digitalization while making dependencies, vulnerabilities, and responsibilities more visible. The broader implication is relevant to other island and remote local governments: mature digital governance is not defined by the number of online systems, but by the ability to sustain lawful, accurate, accessible, and accountable public functions under variable conditions. Future fieldwork should validate the maturity assessment, test controls, incorporate stakeholder experience, and measure whether risk treatment improves service continuity and public value over time.

ACKNOWLEDGEMENT

The authors acknowledge the availability of the Lingga Regency Fisheries Office's 2024 performance information and the institutional and statistical documents that supported this analysis. The interpretations, indicative scores, and proposed roadmap are the authors' analytical responsibility and do not constitute an official audit or compliance certification of the agency.

REFERENCES

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

Badan Pusat Statistik Kabupaten Lingga. (2024). Kabupaten Lingga dalam angka 2024 [Lingga Regency in figures 2024]. BPS-Statistics of Lingga Regency.

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. Government Information Quarterly, 31(1), 119–128. https://doi.org/10.1016/j.giq.2013.06.002

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

Bisma, R. (2022). Information technology asset risk management: A case study of SPBE risk management implementation in the Balikpapan City Communication and Information Office. JIEET (Journal of Information Engineering and Educational Technology), 6(2), 73–79.

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance.

Cordella, A., & Tempini, N. (2015). E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery. Government Information Quarterly, 32(3), 279–286. https://doi.org/10.1016/j.giq.2015.03.005

Dawes, S. S. (2009). Governance in the digital age: A research and action framework for an uncertain future. Government Information Quarterly, 26(2), 257–264. https://doi.org/10.1016/j.giq.2008.12.003

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—Long live digital-era governance. Journal of Public Administration Research and Theory, 16(3), 467–494. https://doi.org/10.1093/jopart/mui057

Eom, S.-J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. Government Information Quarterly, 39(2), 101690. https://doi.org/10.1016/j.giq.2022.101690

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: Finding the crossroads. Public Management Review, 20(5), 633–646. https://doi.org/10.1080/14719037.2017.1327181

Government of the Republic of Indonesia. (2014). Presidential Regulation No. 29 of 2014 concerning the Government Agency Performance Accountability System.

Government of the Republic of Indonesia. (2018). Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System.

Government of the Republic of Indonesia. (2019). Presidential Regulation No. 39 of 2019 concerning One Data Indonesia.

Government of the Republic of Indonesia. (2020). Regulation of the Minister of Administrative and Bureaucratic Reform No. 5 of 2020 concerning guidelines for electronic-based government system risk management.

Government of the Republic of Indonesia. (2022). Presidential Regulation No. 132 of 2022 concerning the National Electronic-Based Government System Architecture.

Government of the Republic of Indonesia. (2023a). Presidential Regulation No. 82 of 2023 concerning acceleration of digital transformation and integration of national digital services.

Government of the Republic of Indonesia. (2023b). Regulation of the Minister of Communication and Informatics No. 1 of 2023 concerning data interoperability in the implementation of the Electronic-Based Government System and One Data Indonesia.

International Organization for Standardization. (2018). ISO 31000:2018 risk management—Guidelines.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. Government Information Quarterly, 32(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Janssen, M., & van der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. Government Information Quarterly, 33(1), 1–5. https://doi.org/10.1016/j.giq.2016.02.003

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. Government Information Quarterly, 37(3), 101493. https://doi.org/10.1016/j.giq.2020.101493

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

Lingga Regency Government. (2022). Lingga Regent Regulation No. 45 of 2022 concerning the position, organizational structure, duties, functions, and work procedures of the Lingga Regency Fisheries Office.

Lingga Regency Government. (2024). Government Agency Performance Report (LKjIP) of the Lingga Regency Fisheries Office 2024. Lingga Regency Fisheries Office.

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

Meijer, A., & Bolívar, M. P. R. (2016). Governing the smart city: A review of the literature on smart urban governance. International Review of Administrative Sciences, 82(2), 392–408. https://doi.org/10.1177/0020852314564308

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

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). SAGE.

Moser-Plautz, B., & Schmidthuber, L. (2023). Digital government transformation as an organizational response to the COVID-19 pandemic. Government

Information Quarterly, 40(3), 101815. https://doi.org/10.1016/j.giq.2023.101815

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.

Organisation for Economic Co-operation and Development. (2014). Recommendation of the Council on digital government strategies. OECD Publishing.

Organisation for Economic Co-operation and Development. (2020). The path to becoming a data-driven public sector. OECD Publishing. https://doi.org/10.1787/059814a7-en

Saldanha, D. M. F., Dias, C. N., & Guillaumon, S. (2022). Transparency and accountability in digital public services: Learning from the Brazilian cases. Government Information Quarterly, 39(2), 101680. https://doi.org/10.1016/j.giq.2022.101680

Scholta, H., Mertens, W., Kowalkiewicz, M., & Becker, J. (2019). From one-stop shop to no-stop shop: An e-government stage model. Government Information Quarterly, 36(1), 11–26. https://doi.org/10.1016/j.giq.2018.11.010

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. Computers & Security, 90, 101709. https://doi.org/10.1016/j.cose.2019.101709

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation model of driving and impeding factors. International Journal of Information Management, 60, 102356. https://doi.org/10.1016/j.ijinfomgt.2021.102356

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Wang, C., Medaglia, R., & Zheng, L. (2018). Towards a typology of adaptive governance in the digital government context: The role of decision-making and accountability. Government Information Quarterly, 35(2), 306–322. https://doi.org/10.1016/j.giq.2017.08.003

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. International Journal of Public Administration, 42(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103