Check for updates

Government & Resilience

Journal Homepage: https//journal.dealingsfoundation.com/index.php/GR/
ISSN: 3032-2820 (Online) / 3032-7601 (Print)

Institutional Preparedness for Cyberocracy: Digital Capability Transformation in Indonesia's Public Sector

Steven Anthony[1], Atrika Iriani[2], Doris Febriyanti[3]*, and Siti Zubaidah[4]

[1]Department of Public Administration, Universitas Terbuka, Indonesia
[2]Department of Public Administration, Universitas Sriwijaya, Indonesia
[3]Department of Government Studies, Universitas Indo Global Mandiri, Indonesia
[4]Department of Public Administration, STIA Bala Putra Dewa, Indonesia

*Corresponding Author Email: dorishakiki@uigm.ac.id , No Telp: +62 812-7860-271;

Received: 3 June 2026; Revised: 7 August 2026; Accepted: 25 August 2026

Abstract

This study examines how institutional preparedness facilitates digital capability transformation toward cyberocracy in Indonesia's regional public sector, focusing on the Dinas Komunikasi dan Informatika (Diskominfo) of South Sumatra Province. A qualitative single-case study was conducted. Data were collected through semi-structured interviews with 15 purposively selected informants and a systematic analysis of four national and provincial policy and performance documents. Data were analysed using reflexive thematic analysis; NVivo 12 Pro was used to organise and code the data and to produce query-based visualisations of the document corpus. The findings show that cyberocratic transformation is shaped by the interaction between institutional preparedness (leadership commitment, institutional coordination, regulatory support, and institutional adaptation) and digital capability transformation (digital literacy, data governance, technological infrastructure, information governance, and innovation culture). Bureaucratic fragmentation emerged as the most consequential constraint: sectoral data ownership, siloed systems, and unclear mandates turn data integration into a negotiation over authority rather than a technical task. Unequal digital competencies, infrastructure gaps, and governance risks reinforce this constraint. The study conceptualises cyberocracy as an institutional and political transformation rather than a technological advancement and identifies institutional preparedness as the enabling mechanism that links digital capability development with data-driven governance. It contributes empirical evidence from a regional government in a developing country and offers practical implications for strengthening data authority, inter-agency coordination, and regulatory coherence.

Keywords: Cyberocracy, Institutional Preparedness, Digital Capability Transformation, Bureaucratic Fragmentation, Digital Governance

How to Cite: Anthony, S., Iriani, A., Febriyanti, D., & Zubaidah, S. (2026). Institutional Preparedness for Cyberocracy: Digital Capability Transformation in Indonesia's Public Sector. *Government & Resilience, 4*(2), 148-170. https://doi.org/10.62503/gr.v4i2.91

Copyright © 2026 by Authors, Published by Dealings Publishing. This work is licensed under the CC BY-NC-SA 4.0 (https://creativecommons.org/licenses/by-nc-sa/4.0).

Introduction

The rapid diffusion of digital technologies has reshaped contemporary public administration, encouraging governments to adopt digital platforms, integrated information systems, artificial intelligence, and data-driven decision-making to improve administrative efficiency and public service delivery (Adewusi et al., 2024; Wirtz et al., 2023). Digital governance has consequently become a dominant paradigm in public administration research, emphasising the use of digital technologies to modernise government operations, enhance citizen engagement, and improve organisational performance (Mergel et al., 2019; Xing et al., 2020). These developments, however, have also generated new institutional problems concerning governance authority, organisational adaptation, inter-agency coordination, and the strategic role of information as a governing resource (Dunleavy et al., 2006; Gil-Garcia et al., 2018).

These problems raise a scientific question that remains insufficiently addressed: what institutional conditions enable governments to move beyond digital service delivery toward cyberocracy as a distinct form of governance? Although governments increasingly adopt digital technologies, many transformation initiatives fail to produce integrated, adaptive, and data-driven governance because institutional arrangements lag behind technological development (Ansell et al., 2021; Kelder et al., 2025; Wilson & Mergel, 2022). Technological adoption alone cannot explain why some governments institutionalise digital governance while others continue to experience fragmented systems, limited interoperability, and weak coordination.

The concept of cyberocracy was introduced by Ronfeldt (1992) and later revisited by Ronfeldt and Varda (2018). Cyberocracy refers not merely to the use of digital technology in government but to a mode of governance in which information, digital networks, and knowledge become primary sources of institutional authority, coordination, and decision-making. It is therefore an explicitly institutional and political concept: Ronfeldt (1992) argued that the information revolution would alter who governs, how bureaucracies are organised, and how power is distributed between state actors.

Cyberocracy is theoretically stronger than the two dominant neighbouring concepts for the question posed in this study. E-government explains the digitisation of administrative processes and service delivery (Bhimavarapu, 2025; Dias, 2020), while digital governance explains technology-enabled collaboration, participation, and public management improvement (Sharmin & Chowdhury, 2025; Wagola et al., 2023). Both perspectives largely treat technology as the principal driver of change and organisational structures as relatively stable. Digital-era governance theory moves closer by arguing that information technology reintegrates fragmented public management structures (Dunleavy et al., 2006; Margetts & Dunleavy, 2013), but it still focuses on administrative reform rather than on the redistribution of authority around information. Cyberocracy adds three explanatory elements that the other concepts lack: (1) it treats information as an institutional resource that confers authority, (2) it expects organisational boundaries and coordination patterns to be restructured around information flows, and (3) it recognises that this restructuring is contested because control over information is also control over decisions. These elements allow cyberocracy to explain why similar technologies produce different governance outcomes across institutions: the outcome depends on whether institutions are prepared to share, govern, and act on information, not on whether the technology exists.

To establish the state of the literature rather than assert it, a structured search of the Scopus database was conducted on 7 October 2026 using the TITLE-ABS-KEY field. The search returned 26,951 documents for "digital governance" OR "e-government" OR "digital government", of which 693 concerned Indonesia. Only 33 documents combined these terms with "institutional readiness"

or "institutional preparedness". The term "cyberocracy" appeared in only five documents: Ronfeldt's (1992) original article, one book on algorithmic government (Gupta & Pal, 2021), two conference papers, and one book chapter; none was an empirical study of a public organisation, and none examined Indonesia or another developing country.

A synthesis of the most relevant studies identified four dominant streams. The first stream examines e-government implementation and its determinants, such as organisational capacity, funding, and leadership at the local level (Dias, 2020; Nurdin et al., 2014). The second examines employee adoption and digital competencies, showing that attitudes, facilitating conditions, and skills shape whether civil servants use new systems (Batara et al., 2017; Bhimavarapu, 2025). The third examines leadership and organisational culture as drivers of digital capability (Cyfert et al., 2025; Kelder et al., 2025; Sahibzada et al., 2025). The fourth examines smart and data-driven governance, emphasising integrated information systems, data utilisation, and the governance of urban data (Meijer & Bolívar, 2016; Xing et al., 2020). Across these streams, institutional readiness is usually treated as one influencing factor among several rather than as the mechanism that connects digital capability with a change in the mode of governance. Studies on Indonesia focus largely on SPBE compliance, service quality, and adoption (Aminah & Saksono, 2021; Wagola et al., 2023; Yulianto et al., 2026).

From this synthesis, four specific research gaps follow. The **theoretical gap** is that cyberocracy has remained a largely conceptual proposition; it has not been operationalised into observable institutional dimensions. The **empirical gap** is the absence of field evidence showing how leadership, coordination, regulation, and organisational adaptation jointly translate digital capabilities into information-based governance. The **contextual gap** is that existing evidence comes mostly from national governments or highly digitised countries, while regional governments in developing countries, where institutional capacity is uneven, remain under-studied. The **mechanism gap** is that previous studies describe barriers such as fragmentation or limited skills but do not explain how these barriers interrupt the pathway from digital capability to cyberocratic governance.

Indonesia is selected because it represents a transitional digital governance environment in which technological development occurs alongside unresolved institutional arrangements. Unlike highly digitised countries with mature digital institutions, Indonesian governments must simultaneously develop technological capability, organisational readiness, regulatory frameworks, and inter-agency coordination (Anggara, 2025; Martín & Palomo Zurdo, 2021; Yulianto et al., 2026). The national frameworks of the Electronic-Based Government System (SPBE) under Presidential Regulation No. 95/2018 and Satu Data Indonesia under Presidential Regulation No. 39/2019 set uniform expectations for integration, yet decentralisation gives regional governments considerable discretion over how these frameworks are implemented. Regional politics also shapes bureaucratic priorities, because regional heads and their agencies operate within local configurations of power (Hadiz, 2010). Indonesia therefore allows the study to examine a central theoretical question of cyberocracy: why the same national policies and technologies produce different governance outcomes across institutions. It is a theoretically significant case for testing whether institutional preparedness, rather than technology, explains the transition from technology adoption toward information-centred governance.

The novelty of this study lies in conceptualising institutional preparedness as the mechanism that enables cyberocracy, thereby extending cyberocracy beyond existing digital governance and e-government perspectives. Its originality lies in providing, to the authors' knowledge and based on the Scopus search above, the first empirical examination of cyberocracy within a regional government institution in Indonesia, using reflexive thematic analysis to explain how institutional, organisational, technological, and political factors interact to shape cyberocratic transformation.

This study aims to analyse how institutional preparedness enables digital capability transformation toward cyberocratic governance within the Dinas Komunikasi dan Informatika (Diskominfo) of South Sumatra Province. It addresses three questions: (1) which dimensions of institutional preparedness support the transition toward cyberocracy; (2) how digital capabilities are transformed within the institution; and (3) which institutional and political conditions constrain this transformation. The findings are expected to contribute to the theoretical development of cyberocracy and to provide policy recommendations for strengthening institutional capacity and sustainable digital governance in developing countries.

Research Methods

Research Design and Case Selection

This study employed a qualitative single-case study design to explore institutional preparedness and digital capability transformation within their real administrative context (Yin, 2016). A case study is appropriate because the research questions ask how and why an institutional process unfolds, the boundaries between the phenomenon and its context are not clear-cut, and the researchers had no control over the events studied. Fieldwork was conducted from January to April 2026, during the implementation of regional digital governance initiatives related to SPBE and Satu Data Indonesia.

Diskominfo of South Sumatra Province was selected as an information-rich and theoretically informative case (Patton, 2015) for three reasons. First, it holds the coordinating mandate for SPBE implementation and for the Satu Data Sumsel ecosystem, which links provincial regional apparatus organisations (OPDs) with the 17 regency and city governments in the province; it is therefore the point at which institutional coordination problems become visible. Second, South Sumatra represents an intermediate level of digital maturity. The province's SPBE index reached 3.13 ("Good") in 2025, exceeding its target of 3.04, while its Digital Transformation Index for the government pillar reached 51.61 against a target of 56.04 (Diskominfo Provinsi Sumatera Selatan, 2026). This combination of formally adequate SPBE performance and incomplete digital transformation makes the province a typical case of the transitional condition described above, rather than an exemplary or a failing case. Third, the province combines a large provincial bureaucracy with diverse regency and city capacities, which allows inter-agency and multi-level dynamics to be observed within one case.

Informants and Sample Adequacy

Informants were selected through purposive sampling based on three criteria: (1) managerial, technical, or policymaking responsibility for digital governance; (2) at least three years of experience in SPBE, digital transformation, or public-sector data governance; and (3) active involvement in decision-making, system development, or inter-agency coordination. Fifteen informants participated as show in Table 1.

Table 1. Profile of Informants

Informant group	Code	Number
Head of agency	I1	1
Heads of division	I2–I4	3
Digital governance coordinators	I5–I7	3
Information technology officers	I8–I11	4
SPBE and Satu Data administrators	I12–I13	2
Regional development planners	I14–I15	2

Informant group	Code	Number
Total		**15**

Source: Research data, 2026.

Because reflexive thematic analysis treats meaning as generated through interpretation rather than discovered in the data, data saturation is not an appropriate stopping criterion for this approach (Braun & Clarke, 2021b). Sample adequacy was instead assessed through the concept of information power (Malterud et al., 2016). Information power was high because the study aim was narrow (one institutional process in one agency), the informants were highly specific (they were the actors directly responsible for SPBE and Satu Data), the analysis was guided by an established theory (cyberocracy), the interviews involved in-depth dialogue with experienced practitioners, and the analysis was conducted as a case analysis rather than a cross-case comparison. Fifteen interviews also fall within the range at which empirical studies typically observe code and meaning saturation in relatively homogeneous samples (Hennink & Kaiser, 2022).

Data Collection

Primary data were collected through semi-structured interviews conducted face-to-face at the informants' offices, lasting approximately 45 minutes each. Interviews were audio-recorded with the participants' consent and transcribed verbatim. The interview guide covered institutional preparedness, leadership commitment, inter-agency coordination, regulatory arrangements, digital capability, and implementation challenges. Informants are identified by role only to protect confidentiality.

Document analysis was conducted systematically rather than as background reading. Four publicly available, text-searchable documents formed the document corpus: (1) Presidential Regulation No. 95/2018 on the Electronic-Based Government System (SPBE; 101 pages); (2) Presidential Regulation No. 39/2019 on Satu Data Indonesia; (3) Presidential Regulation No. 82/2023 on the Acceleration of Digital Transformation and the Integration of National Digital Services; and (4) the 2025 performance report of Diskominfo South Sumatra (Diskominfo Provinsi Sumatera Selatan, 2026; 65 pages). The two national SPBE and Satu Data regulations define the formal mandates that the province must implement, Presidential Regulation No. 82/2023 represents the most recent national response to fragmented digital services, and the performance report shows how the provincial agency itself reports progress. The agency's strategic plans were also consulted, but they are published only as scanned images and could not be coded as text. Document evidence was used in three ways: to verify claims made by informants (for example, the status of regulations and the progress of data integration), to identify gaps between formal mandates and reported practice, and to provide contextual data on institutional performance.

NVivo-Assisted Document Coding

The four documents were imported into a dedicated NVivo 12 Pro project. A codebook derived from the thematic framework of this study (three themes and eleven sub-themes that could be identified in written policy text) was imported as a node hierarchy. Each sub-theme was then coded with a predefined Indonesian-language text search query, with results spread to the broad context (the surrounding paragraph) and stored in the corresponding node. The query terms were: leadership commitment (*pimpinan, kepala daerah, komitmen, gubernur, kepala dinas*); institutional coordination (*koordinasi, kolaborasi, kerja sama, keterpaduan*); regulatory support (*kebijakan, pedoman, regulasi*); institutional adaptation (*reformasi birokrasi, proses bisnis, tata kelola*); digital literacy and human-resource capacity (*sumber daya manusia, kompetensi, pelatihan, bimtek, bimbingan teknis, kapasitas*); data governance (*satu data, interoperabilitas, metadata, walidata,*

produsen data, pembina data, standar data, kode referensi, data induk); technological infrastructure (*infrastruktur, jaringan, pusat data*); information governance (*akuntabel, akuntabilitas, transparan, transparansi, keterbukaan informasi, verifikasi, validasi, kualitas data*); innovation culture (*inovasi, inovatif*); integration gaps and fragmentation (*duplikasi, sinkronisasi, hambatan, permasalahan, belum*); and governance risks (*keamanan informasi, keamanan siber, risiko, serangan*). A matrix coding query (nodes × documents), a hierarchy chart, and a word frequency query were then produced in NVivo. Because keyword-based coding captures explicit mentions rather than implicit meaning, the document coding is used to describe how formal documents frame cyberocratic preparedness, not as a substitute for interpretive analysis.

Interpretive Analysis

The analysis followed reflexive thematic analysis (Braun & Clarke, 2019, 2021a). The analysis itself was an interpretive process conducted by researchers; NVivo 12 Pro was used only as a tool to organise transcripts and documents, attach codes, retrieve coded extracts, and visualise relationships between codes. The software did not generate codes or themes. The analysis proceeded through six recursive phases: (1) familiarisation through repeated reading of transcripts and documents; (2) systematic generation of initial codes across the full data set; (3) construction of candidate themes by clustering codes with shared meaning; (4) review of themes against coded extracts and the full data set; (5) definition and naming of themes and sub-themes; and (6) writing up, in which analytic interpretation was connected to the literature. The process produced 126 initial codes, which were developed into 31 categories, 13 sub-themes, and three overarching themes: (1) institutional preparedness toward cyberocracy, (2) digital capability transformation, and (3) challenges in implementing cyberocratic governance as shown in Table 2.

Table 2. Coding Framework of the Reflexive Thematic Analysis

Theme	Sub-theme	Illustrative codes
1. Institutional preparedness toward cyberocracy	Leadership commitment	leadership awareness; strategic direction; vision alignment; resource mobilisation; budget support
	Institutional coordination	Kominfo cannot act alone; OPD and BPS collaboration; shared data standards; information exchange
	Regulatory support	no legal umbrella yet; institutional legitimacy; regional supporting regulations; operationalisation of rules
	Institutional adaptation	application consolidation; workflow adjustment; shift from agency-based to integrated systems
2. Digital capability transformation	Digital literacy	literacy training for OPDs; capacity building; organisational learning
	Data governance	Satu Data Sumsel; data integration; standardisation; data verification
	Technological infrastructure	connectivity; system compatibility; supporting facilities
	Information governance	validation; transparency; traceability; accountability
	Innovation culture	self-initiated innovation; creative problem-solving; continuous improvement

Theme	Sub-theme	Illustrative codes
3. Challenges in implementing cyberocracy	Institutional barriers (bureaucratic fragmentation)	different OPD data; separate systems; organisational silos; unclear mandates
	Human-resource limitations	not all staff ready; uneven competencies; limited continuous learning
	Infrastructure constraints	facility and connectivity gaps; uneven infrastructure quality
	Governance risks	data quality; cybersecurity; regulatory uncertainty; accountability

Source: Reflexive thematic analysis of interview and document data, 2026.

Trustworthiness was supported through source triangulation between interviews and documents, member checking in which preliminary interpretations were returned to six informants, and peer debriefing with qualitative researchers who reviewed the coherence of codes and themes (Franklin & Ballan, 2001). Consistent with reflexive thematic analysis, inter-coder reliability statistics were not calculated; instead, the researchers documented analytic decisions and discussed alternative interpretations during theme development, as illustrated in the research procedure in Figure 1.

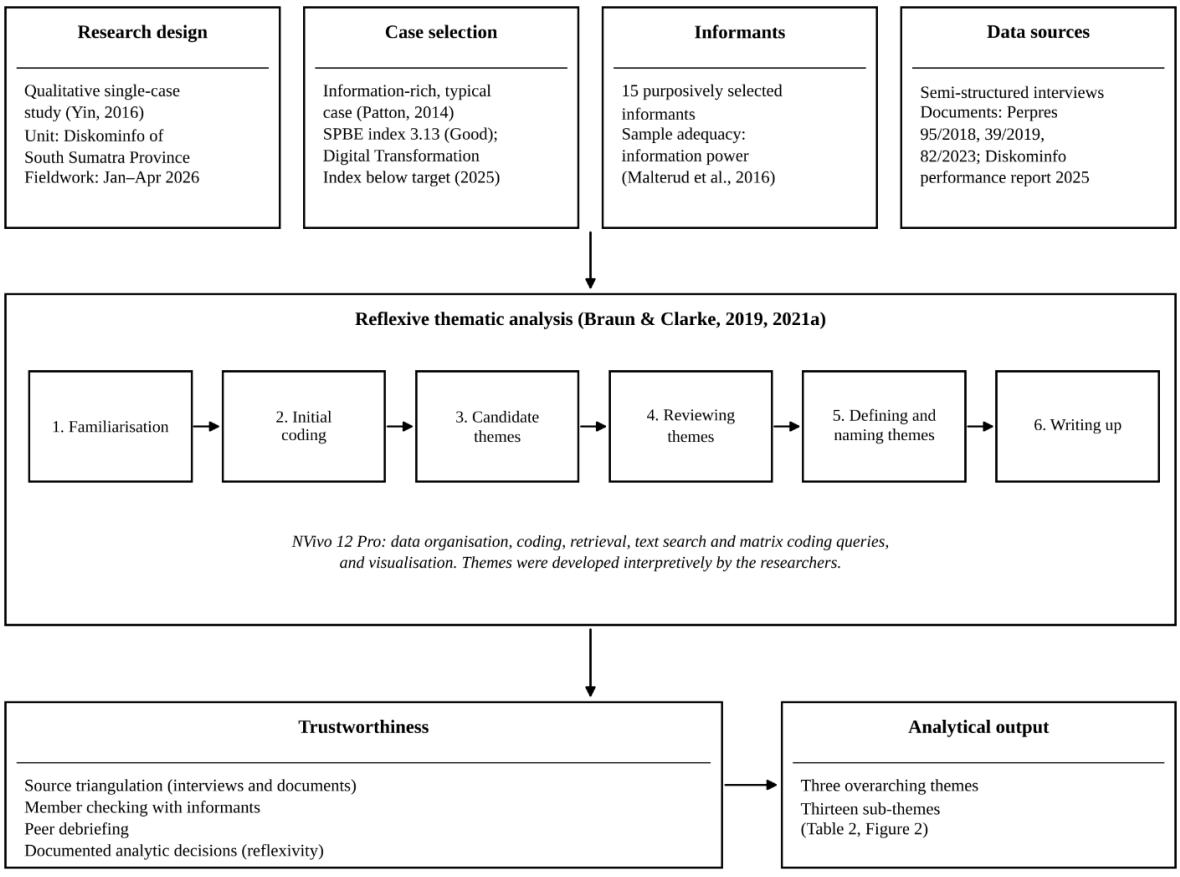


Figure 1. Research Design and Reflexive Thematic Analysis Procedure. *Source: Developed by the authors based on Yin (2016), Patton (2015), Malterud et al. (2016), and Braun and Clarke (2021a).*

Results and Findings

The findings demonstrate that the transition toward cyberocratic governance within Diskominfo South Sumatra is an **institutional transformation rather than merely a technological process**. The analysis generated three overarching themes and 13 sub-themes (Table 2 and Figure 2). Institutional preparedness provides the organisational foundation for developing digital capabilities, while institutional, human-resource, infrastructural, and governance challenges constrain how far those capabilities can be converted into information-centred governance. The sections below discuss each theme, followed by an analysis of bureaucratic fragmentation and the political dimension of cyberocracy, which together explain why the transformation remains incomplete.

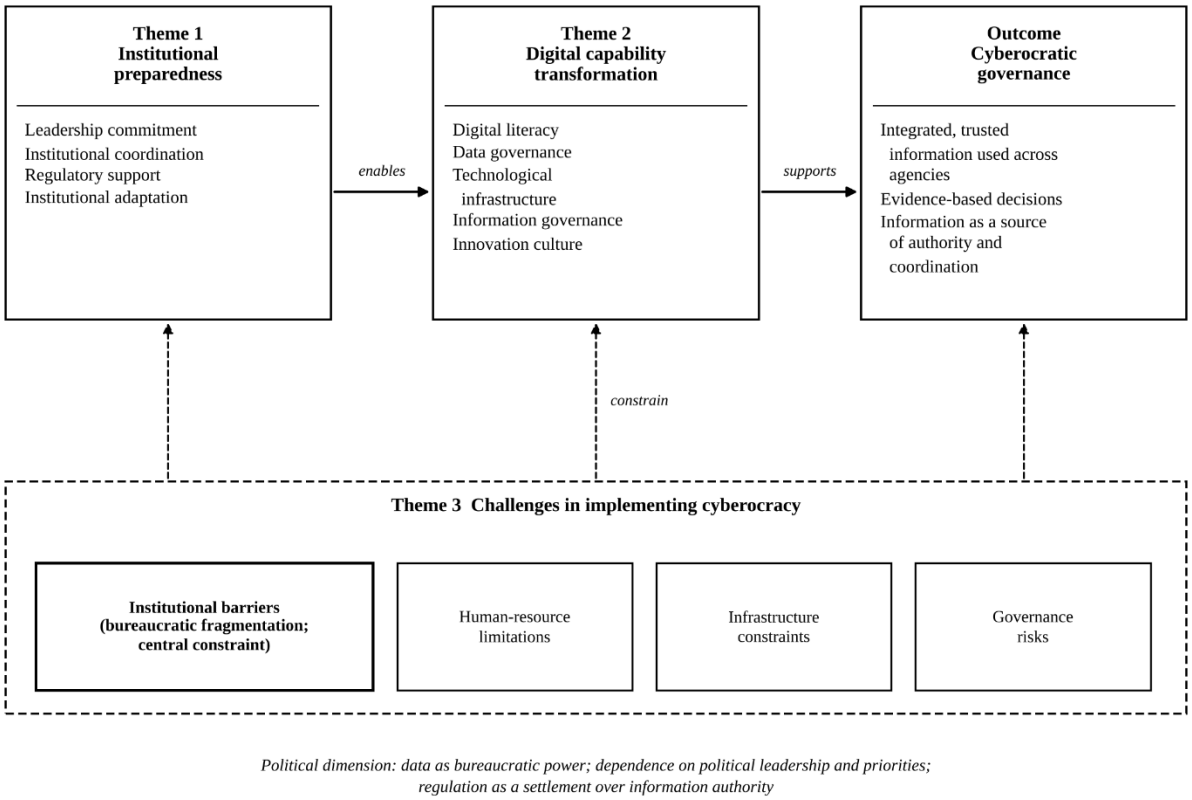


Figure 2. Thematic Map of Institutional Preparedness, Digital Capability Transformation, and Challenges toward Cyberocracy. Source: Developed by the authors from the reflexive thematic analysis, 2026.

Institutional Preparedness toward Cyberocracy

The first theme shows that institutional preparedness extends beyond technological availability and is shaped by four interrelated sub-themes: **leadership commitment, institutional coordination, regulatory support, and institutional adaptation**. Leadership provides direction, coordination enables integration, regulation provides legitimacy, and adaptation embeds digital practices in administrative processes. Together, these sub-themes constitute the initial enabling

condition through which digital resources can be transformed into integrated governance capabilities.

1. Leadership Commitment

Leadership commitment emerged as a central dimension of institutional preparedness. Digital transformation cannot be sustained through technological investment alone; it requires leadership awareness, strategic direction, and resource mobilisation so that digitalisation becomes an institutional priority. A senior managerial informant emphasised this point:

"Digital transformation is impossible to carry out if the leadership is not aware of the importance of digitalization."

(Senior Managerial Informant, Interview, 2026)

Leadership awareness constitutes a starting point for institutional transformation. Leaders are responsible not only for approving digital initiatives but also for establishing an organisational understanding that digitalisation is a strategic necessity. Without such awareness, digital initiatives risk remaining fragmented technological projects. Leadership commitment was further reflected in the need for clear strategic direction:

"Digital transformation in local government environments is not enough just by providing applications or technological infrastructure. The most important thing is how leaders provide clear direction so that each regional apparatus understands the objectives of SPBE implementation and data integration. We need to ensure that the systems we build don't operate in silos, but support faster, more accurate, and data-driven decision-making processes. Therefore, the role of leadership is to unify the vision, encourage collaboration between units, and ensure digital transformation is part of the organization's strategy."

(Managerial Informant and Head of Division, Interview, 2026)

This statement shows that leadership commitment extends beyond awareness to **strategic alignment**: it connects SPBE implementation, data integration, inter-unit collaboration, and evidence-based decision-making with organisational objectives, preventing digital systems from developing as isolated applications. Leadership commitment was also associated with the mobilisation of resources:

"Implementing digital transformation requires broader support, not just from the technological side. We need to strengthen human resources, improving employee competency, budget support, and internal policies that can accelerate implementation. Without such support, existing digital systems will not run optimally because users and organizations are not fully ready to make changes."

(Digital Governance Informant, Interview, 2026)

Leadership therefore operates as a **resource mobilisation mechanism** that converts institutional commitment into implementation capacity through human-resource development, budget allocation, and internal policies. This finding is consistent with studies showing that leadership behaviour and entrepreneurial orientation shape digital capability and innovation (Kelder et al., 2025; Sahibzada et al., 2025), and with evidence that digital champions are critical for overcoming institutional barriers in government (Wilson & Mergel, 2022). In the context of cyberocracy, however, the finding adds that leadership matters because it legitimises the

redistribution of information across units, which subordinate units are unlikely to initiate themselves.

2. Institutional Coordination

Institutional coordination emerged as a key dimension because the production, verification, integration, and use of government data involve multiple OPDs, Statistics Indonesia (BPS), regency and city governments, and other stakeholders. A Diskominfo informant summarised the limitation of an agency-centred approach:

"Kominfo cannot act alone."

(Diskominfo Informant, Interview, 2026)

An SPBE administrator explained the practical meaning of this limitation:

"One of the challenges in implementing SPBE and Satu Data is coordination between regional agencies. Each organization has different systems, needs, and levels of digital readiness. Data integration requires a shared understanding of data standards, information exchange mechanisms, and a shared commitment to ensure that the data used is not only available but also utilized to support regional government policies."

(SPBE Administrator, Interview, 2026)

Coordination therefore involves more than communication between agencies. Differences in systems, organisational needs, and digital readiness create barriers to interoperability, so effective coordination requires common data standards, mechanisms for information exchange, and a shared commitment to use data in decision-making. Through the Satu Data Sumsel ecosystem, Diskominfo coordinates sectoral data from OPDs, while collaboration with BPS supports standardisation. Coordination thus functions as an **institutional integration mechanism** that allows digital capabilities to operate collectively rather than within isolated silos. Earlier Indonesian evidence similarly shows that local e-government succeeds when dynamic coordination and cooperation between internal and external actors are sustained (Nurdin et al., 2014).

3. Regulatory Support

Regulatory support emerged as a further dimension because digital transformation requires a regulatory framework that provides legitimacy, direction, and accountability. National policies on SPBE and Satu Data Indonesia provide a general framework, but implementation at the regional level depends on the availability and clarity of supporting regulations. A policymaker highlighted the regulatory gap:

"There is no legal umbrella yet."

(Policymaker Informant, Interview, 2026)

The absence of a clear regional legal basis creates uncertainty, particularly when initiatives involve data sharing, cross-agency coordination, and changes to established procedures. The document analysis is consistent with this account: the national regulations allocate data roles in general terms (Section 3.4), but no provincial implementing regulation that specifies which unit owns, verifies, and publishes particular datasets was found among the publicly accessible, text-searchable documents analysed. Regulation therefore functions as an **institutional legitimisation**

mechanism: clear and operational rules give institutions the confidence to share information and transform digital governance from an emerging practice into an accountable administrative process.

4. Institutional Adaptation

Institutional adaptation emerged as the fourth dimension. Digital transformation requires institutions to adjust structures, workflows, and applications so that systems can operate in an integrated manner. An informant described the direction of this adaptation:

"All applications are united in one data."

(Informant, Interview, 2026)

Adaptation involves more than introducing new applications; it requires changes in how applications, data, and organisational processes are structured and connected. Rather than maintaining separate systems within individual units, institutions are encouraged to reorganise digital resources toward integration. This represents a shift from **agency-based digitalisation toward integrated digital governance**, which is the organisational form that cyberocracy anticipates (Ronfeldt, 1992) and that digital-era governance theory describes as reintegration (Dunleavy et al., 2006).

Digital Capability Transformation

The second theme shows that digital capability extends beyond infrastructure to include the organisational capacity to generate, integrate, verify, manage, and use digital information for governance. Five sub-themes emerged: **digital literacy, data governance, technological infrastructure, information governance, and innovation culture**. Digital capability therefore develops through the interaction of technological resources, organisational learning, data management, and adaptive practices rather than through technology adoption alone.

1. Digital Literacy

Digital literacy emerged as an organisational requirement rather than only individual competency. One informant stated:

"Regency/city OPDs and Kominfo also need literacy training."

(Informant, Interview, 2026)

The involvement of both provincial and regency/city OPDs shows that integrated systems require relatively consistent capability across institutional boundaries. When OPDs possess different levels of capability, integration becomes more difficult. Literacy development must also be continuous because systems and administrative practices keep evolving. Digital literacy thus functions as an **institutional learning capability** that enables personnel to absorb technological change and participate in integrated information systems, in line with evidence that employee readiness and facilitating conditions shape local e-government adoption in Indonesia (Batara et al., 2017).

2. Data Governance

Data governance emerged as a central component of digital capability. Digital governance in South Sumatra increasingly depends on the ability to integrate, standardise, verify, and use data

across organisational boundaries, with Satu Data Sumsel as the main institutional mechanism. An informant summarised this as:

"One Data South Sumatra, big data, data verification."

(Informant, Interview, 2026)

The statement reflects three related practices: data integration, the development of a broader data environment, and data verification. Sectoral information produced by OPDs must be coordinated, standardized, and validated before it can be used across institutions. Data governance therefore provides the **operational basis for cyberocratic governance**: by making information integrated, consistent, and usable, it allows digital systems to support coordination and evidence-based decision-making.

3. Technological Infrastructure

Technological infrastructure emerged as a supporting dimension. Improvements in systems and connectivity have supported digital governance, but infrastructure remains uneven across institutions. One informant noted:

"There are still many obstacles to facilities and infrastructure."

(Informant, Interview, 2026)

Limitations in connectivity, system compatibility, and supporting facilities reduce the effectiveness of systems in everyday administration and limit the movement of information between units. Infrastructure nevertheless should not be interpreted as the sole determinant of transformation; it creates the technical possibility for integration, but its governance value depends on literacy, data governance, and organisational adaptation. The agency's ICT development index of 5.97 in 2025 (Diskominfo Provinsi Sumatera Selatan, 2026) indicates that provincial infrastructure is relatively developed, which reinforces the interpretation that the remaining constraints are institutional rather than primarily technical.

4. Information Governance

Information governance emerged as the quality-control dimension of digital capability. Information needs to be checked and validated before it is incorporated into government databases and used for policy. Sectoral data produced by different units must pass through verification to ensure consistency with established standards, and data integrated without adequate validation may create inconsistencies between agencies and reduce confidence in decisions. In this sense, cyberocracy requires not merely more digital information, but **trusted information that can legitimately support governmental decisions**. This dimension also links to accountability, since information technology governance has been shown to improve transparency and accountability in Indonesian local government (Sofyani et al., 2020).

5. Innovation Culture

Innovation culture emerged as the final dimension of digital capability. Innovation does not originate only from formal programmes or external requirements; it also emerges from employees and units that identify problems and develop solutions. One informant stated:

"We initiated it ourselves."

(Informant, Interview, 2026)

Although brief, this statement indicates that innovation may originate within the organisation rather than through top-down directives. When employees initiate improvements, digital transformation becomes a continuous process rather than a one-time system implementation. Innovation culture therefore functions as a **continuous improvement mechanism** that allows digital capabilities to evolve in response to operational and governance challenges.

Challenges in Implementing Cyberocracy

The third theme concerns the conditions that constrain the transformation. Four sub-themes were identified: **institutional barriers, human-resource limitations, infrastructure constraints, and governance risks**. These challenges are not independent; they reinforce one another, and the analysis indicates that institutional barriers, in the form of bureaucratic fragmentation, are the most consequential. Fragmentation is therefore analysed separately in Section 3.5, after the document evidence in Section 3.4.

1. Human-Resource Limitations

The introduction of digital systems does not automatically create equal capability across institutions. One informant stated:

"Not all human resources are ready."

(Informant, Interview, 2026)

This statement points to the distinction between **technology readiness and organisational readiness**. Systems may be available, but their effectiveness depends on whether employees have the capacity and confidence to use them. Without continuous competency development, transformation may remain concentrated in technically capable units, which deepens differences between OPDs and indirectly reinforces fragmentation.

2. Infrastructure Constraints

Infrastructure constraints affect the consistency of implementation across institutions. Where facilities or connectivity are insufficient, units continue to rely on separate systems or manual processes, reducing the effectiveness of integration. Infrastructure is therefore a **necessary but not sufficient condition** for cyberocracy; its contribution becomes meaningful only when combined with capable personnel, coordinated institutions, and appropriate governance arrangements.

3. Governance Risks

Greater dependence on digital information increases the need to maintain **data reliability, accountability, cybersecurity, and regulatory certainty**. As data from different institutions is integrated, weaknesses in quality or verification can affect the credibility of policy decisions, and interconnected systems increase exposure to security threats. Local governments are particularly vulnerable because cybersecurity is a sociotechnical problem that depends on organisational practice as much as technology (Frandell & Feeney, 2022). The agency's information security index (Indeks KAMI) of 446 in 2025 (Diskominfo Provinsi Sumatera Selatan, 2026) suggests progress at the provincial level, but the integration of regency and city data extends risk beyond the agency's direct control. Cyberocracy therefore requires the institutional capacity not only to collect and integrate information, but also to **protect, validate, and govern it responsibly**.

Document Evidence: How Formal Policy Frames Cyberocratic Preparedness

The NVivo coding of the four policy and performance documents produced 505 coding references across the eleven document-level sub-themes (Table 3). Institutional preparedness (220 references) and digital capability transformation (228 references) dominate the corpus, whereas challenges account for only 57 references (11.3%). Figure 3 shows the relative weight of each sub-theme as an NVivo hierarchy chart, and Figure 4 shows how coding references are distributed across the four documents.

Table 3. Coding References by Sub-theme and Document (NVivo 12 Matrix Coding Query)

Sub-theme	Perpres 95/2018 (SPBE)	Perpres 39/2019 (Satu Data)	LKjIP Diskominfo Sumsel 2025	Perpres 82/2023	Total
1.1 Leadership commitment	24	7	5	0	36
1.2 Institutional coordination	21	6	25	15	67
1.3 Regulatory support	27	5	20	3	55
1.4 Institutional adaptation	28	6	25	3	62
2.1 Digital literacy & HR capacity	4	1	24	1	30
2.2 Data governance	6	64	15	8	93
2.3 Technological infrastructure	45	1	18	6	70
2.4 Information governance	15	1	17	1	34
2.5 Innovation culture	0	0	1	0	1
3.1 Integration gaps & fragmentation	3	10	2	3	18
3.2 Governance risks	14	0	24	1	39
Total	**187**	**101**	**176**	**41**	**505**

Source: NVivo 12 Pro matrix coding query of the document corpus, processed by the authors, 2026.

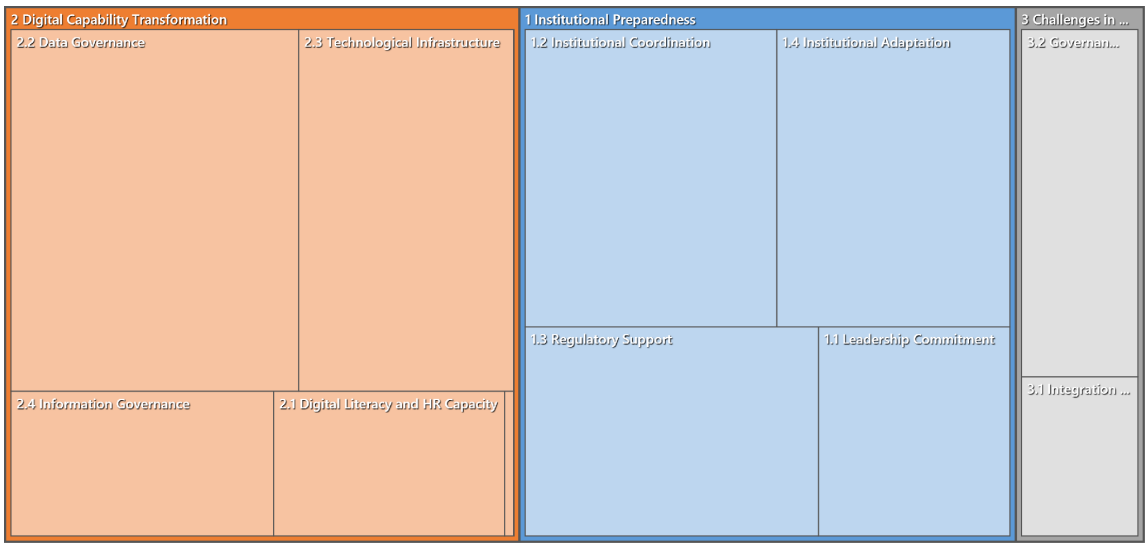


Figure 3. NVivo Hierarchy Chart of Document Coding by Sub-theme (Coding References). Source: NVivo 12 Pro output, processed by the authors, 2026.

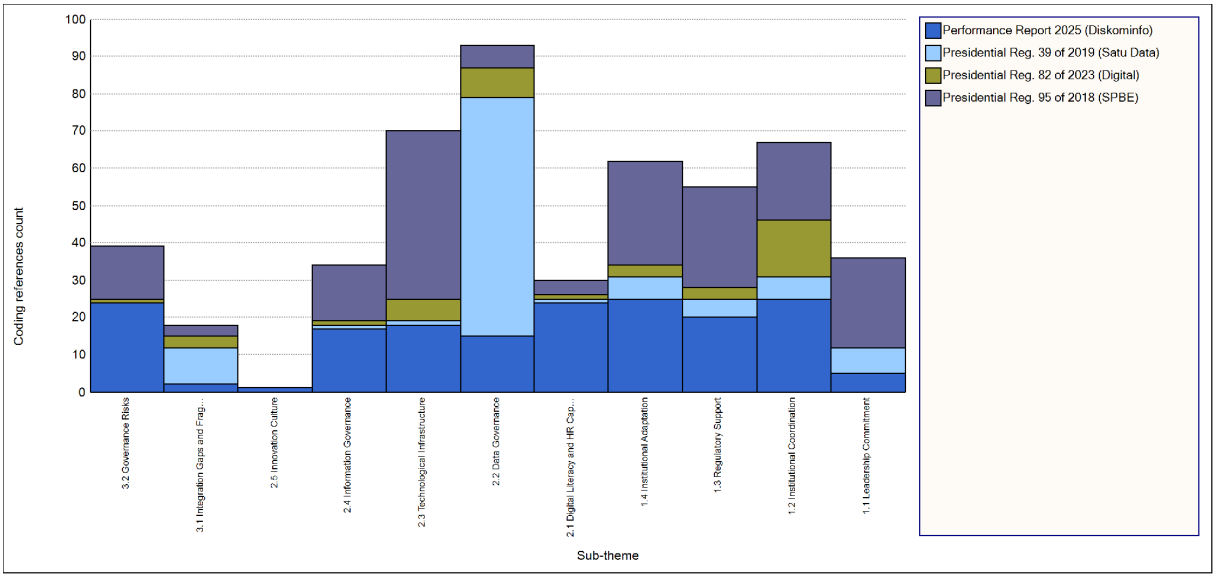


Figure 4. NVivo Matrix Coding Query: Coding References by Sub-theme and Document. Source: NVivo 12 Pro output, processed by the authors, 2026.

Three patterns are relevant to the argument of this study. First, each document emphasises a different layer of preparedness. Presidential Regulation No. 95/2018 is dominated by technological infrastructure (45 references), institutional adaptation (28), regulatory support (27), and leadership (24), reflecting an architectural model of SPBE in which governance is organised through national architecture, business processes, and SPBE coordination teams (*Tim Koordinasi SPBE*). Presidential Regulation No. 39/2019 is concentrated almost entirely on data governance (64 references), and it formally allocates authority over data to specific roles: the *pembina data* (data supervisor), the *walidata* (data custodian, which collects, checks, manages, and disseminates data), and the *produsen data* (data producer). This confirms that integrating data is formally an allocation of authority among institutions, not only a technical task.

Second, the provincial performance report translates these mandates into coordination (25 references), institutional adaptation (25), human-resource capacity (24), and information security (24), which mirrors the interview emphasis on coordination, literacy training, and governance risk. Presidential Regulation No. 82/2023 has the highest proportion of coordination content (11.6% of the document), and its preamble justifies the policy by the need for an integrated and comprehensive SPBE and Satu Data and for coordination and collaboration between ministries, agencies, and state-owned enterprises. The most recent national policy therefore implicitly acknowledges that earlier digitalisation produced fragmented services.

Third, formal documents are almost silent on obstacles. Integration gaps and fragmentation account for only 18 references, innovation culture for one, and terms that would signal bureaucratic barriers, such as *ego sektoral* (sectoral ego), *kendala* (constraint), or *keterbatasan* (limitation), do not appear at all in the corpus. The word frequency query (Figure 5) likewise shows a vocabulary centred on government, data, systems, and coordination. Read alongside the interview evidence, this silence is itself a finding: formal policy documents describe the architecture of cyberocratic preparedness but do not record the bureaucratic fragmentation that informants identified as the main barrier. Fragmentation is therefore visible mainly in practice and in the corrective mandates of newer regulations, rather than in the self-reporting of the institutions involved.



Figure 5. NVivo Word Frequency Query of the Document Corpus (60 most frequent words, minimum length six characters). Words are shown in the original Indonesian; English equivalents of the most frequent terms are *daerah* (region), *pemerintah* (government), *instansi* (agency), *informasi* (information), *pemerintahan* (governance), *komunikasi* (communication), *nasional* (national), *layanan* (service), *peraturan* (regulation), *aplikasi* (application), *keamanan* (security), *arsitektur* (architecture), and *koordinasi* (coordination). Source: NVivo 12 Pro output, processed by the authors, 2026.

Bureaucratic Fragmentation as the Central Constraint

Across the three themes, bureaucratic fragmentation emerged as the most important analytical finding. It appears not only as one challenge among others but as the condition that explains why preparedness and capability do not automatically produce cyberocratic governance. One informant described the problem directly:

"OPD data is still different."

(Informant, Interview, 2026)

The analysis identified four interlocking forms of fragmentation. **Fragmented authority**: each OPD retains formal responsibility for its sectoral data, so Diskominfo can coordinate but cannot compel integration ("Kominfo cannot act alone"). **Fragmented systems**: applications developed separately by units use different structures and standards, so integration requires reconciliation before data can be combined. **Fragmented rules**: without regional implementing regulations ("There is no legal umbrella yet"), responsibilities for ownership, verification, and publication remain unclear. **Fragmented capability**: differences in digital competence and infrastructure between OPDs and between provincial and regency/city governments mean that integration proceeds at the pace of the least prepared unit.

These forms of fragmentation interact. Fragmented authority makes it rational for units to protect their own systems; fragmented systems then make integration technically costly; fragmented rules remove the legitimacy needed to override unit preferences; and fragmented capability creates

uneven participation. The result is a pattern in which **digitalisation occurs within institutions without producing integration across them**. This explains why South Sumatra can achieve a "Good" SPBE index while falling short of its digital transformation target (Diskominfo Provinsi Sumatera Selatan, 2026): SPBE indicators largely reward the existence of systems and policies within agencies, whereas cyberocratic governance requires information to flow and be used across agencies.

This finding refines both digital-era governance theory and cyberocracy theory. Digital-era governance expects information technology to reintegrate fragmented bureaucracies (Dunleavy et al., 2006), and Ronfeldt (1992) expected information networks to weaken hierarchical boundaries. The evidence from South Sumatra shows that this reintegration is not automatic: in a decentralised and sectorally organised bureaucracy, technology can reproduce existing silos in digital form. The central challenge of cyberocracy is therefore not technological limitation, but the difficulty of restructuring traditional bureaucratic arrangements into interconnected, data-driven governance networks. Institutional preparedness matters precisely because it is the set of conditions (leadership, coordination, regulation, and adaptation) that can counteract fragmentation.

The Political Dimension of Cyberocracy

Cyberocracy is not merely a digital phenomenon; it is also political, because changing how information flows changes who holds authority over decisions (Ronfeldt, 1992). The findings point to three political dynamics that shape the transformation, although these dynamics were not the primary focus of the interviews and should be read as interpretive implications that warrant further research.

First, **data are a source of bureaucratic power**. When an OPD controls a dataset, it controls the information on which budgets, programmes, and performance assessments are based. Integration into Satu Data Sumsel therefore requires units to relinquish part of this control, which helps explain why fragmentation persists even when technical solutions exist. Coordination problems are, in this sense, also problems of sectoral interests and inter-agency bargaining (Nurdin et al., 2014; Wilson & Mergel, 2022).

Second, **digital transformation depends on political leadership and priorities**. The repeated emphasis on leadership awareness indicates that the pace of transformation depends on whether regional leaders treat digital governance as a priority. In Indonesia's decentralised system, regional bureaucracies operate within local configurations of political power (Hadiz, 2010), so priorities can shift with leadership changes and electoral cycles. Cyberocratic transformation is therefore vulnerable to discontinuity unless it is institutionalised through regulation and organisational routines.

Third, **regulation is a political settlement over authority**. The absence of a regional "legal umbrella" is not only a technical gap; it reflects the fact that assigning responsibility for data ownership, verification, and publication allocates authority between agencies and between levels of government. Regulatory support thus functions as the mechanism through which political agreement on information authority is made binding.

These dynamics show that institutional preparedness has a political as well as an administrative character. Leadership commitment and regulatory support are the points at which political will is translated into institutional arrangements, while fragmentation is partly the expression of unresolved political interests. Recognising this dimension extends cyberocracy beyond technocratic accounts of digital government and reconnects it with Ronfeldt's (1992) original concern with the redistribution of power in the information age.

From Institutional Preparedness to Cyberocratic Governance

The findings show that cyberocratic governance develops through the interaction between **institutional preparedness and digital capability transformation**. Leadership commitment, institutional coordination, regulatory support, and institutional adaptation create the foundation for developing digital literacy, data governance, technological infrastructure, information governance, and innovation culture. These capabilities, in turn, support the integration and use of reliable information for data-driven governance. Bureaucratic fragmentation and political dynamics act on every stage of this pathway, while human-resource limitations, infrastructure constraints, and governance risks reinforce them (Figure 6).

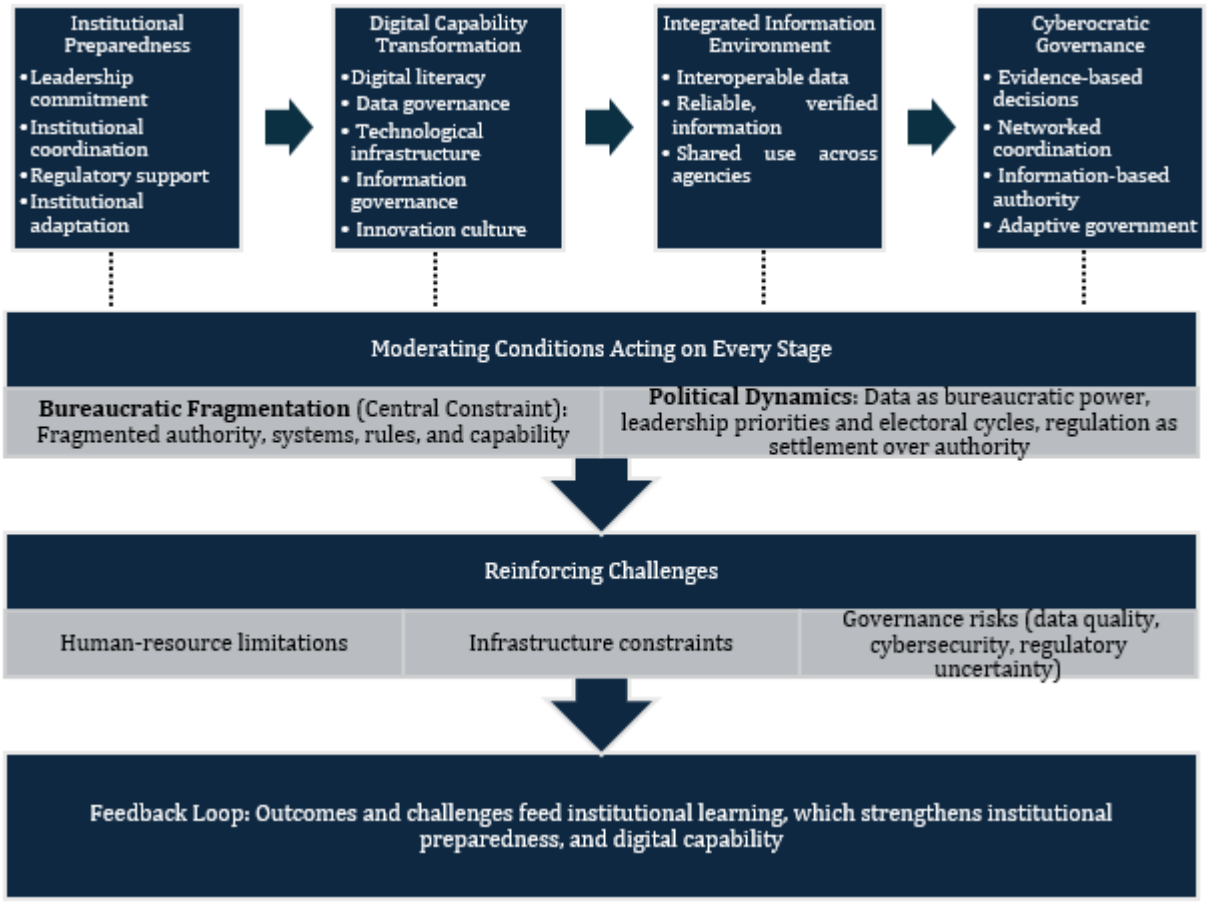


Figure 6. Conceptual Model: From Institutional Preparedness and Digital Capability Transformation to Cyberocratic Governance. Source: Developed by the authors, 2026.

Figure 6 illustrates the transformation as a progressive and conditional process. Institutional preparedness enables digital capability; integrated and trusted information supports cyberocratic governance; and outcomes feed back into institutional learning. The pathway is moderated by fragmentation and politics, which determine whether capabilities developed within individual institutions are converted into shared, government-wide information resources.

Key Finding and Theoretical Implications

The central finding is that **cyberocratic governance is shaped by institutional capacity and the resolution of bureaucratic fragmentation rather than by technological adoption alone**. The

study makes three theoretical contributions. First, it operationalises cyberocracy into observable institutional dimensions, nine enabling sub-themes and four constraining sub-themes, thereby moving the concept from a conceptual proposition toward an empirically testable framework. Second, it identifies institutional preparedness as the **enabling mechanism** between digital capability and cyberocratic governance, explaining why similar technologies and national policies produce different outcomes. Third, it shows that the main barrier to cyberocracy in a decentralised developing-country context is bureaucratic fragmentation sustained by political interests over information, which qualifies the expectation in digital-era governance and cyberocracy theory that information technology will automatically reintegrate government.

Conclusion

This study demonstrates that the transition toward cyberocratic governance in South Sumatra's regional government is fundamentally an **institutional and political transformation rather than a purely technological process**. Cyberocracy develops through the interaction between institutional preparedness and digital capability transformation: leadership commitment, institutional coordination, regulatory support, and institutional adaptation provide the foundation, while digital literacy, data governance, technological infrastructure, information governance, and innovation culture translate this foundation into practice.

The transformation remains constrained, above all, by bureaucratic fragmentation in the form of fragmented authority, systems, rules, and capability. Because control over data is also control over decisions, fragmentation is sustained by sectoral and political interests, and it is reinforced by unequal human-resource capacity, infrastructure gaps, and governance risks. Technological investment alone is therefore insufficient; digital capabilities must be embedded within coordinated institutional and governance arrangements.

The principal contribution of this study is the proposition that **institutional preparedness functions as the enabling mechanism through which digital capability is transformed into cyberocratic governance**, and that its effectiveness depends on overcoming bureaucratic fragmentation. This extends cyberocracy beyond e-government and digital service delivery by positioning information authority, organisational adaptation, and inter-agency coordination as interconnected foundations of data-driven public administration.

In practical terms, regional governments should (1) adopt regional regulations that clearly assign data ownership, verification, and publication responsibilities; (2) strengthen the coordinating authority of the agency responsible for Satu Data; (3) institutionalise leadership commitment through planning and budgeting documents so that transformation survives leadership changes; and (4) invest in continuous digital competency development across provincial and regency/city OPDs alongside infrastructure.

This study is limited to a single regional government institution and to the perspectives of internal government actors, which constrains the transferability of the findings. The political dimension was derived interpretively and was not examined directly through political actors. Future research should compare cyberocratic transformation across regions and levels of government, include regional political leaders, legislators, and citizens, and examine the role of emerging technologies such as artificial intelligence, predictive analytics, and decision-support systems in reshaping public administration.

Declaration of Competing Interest

The authors declare that they have no financial or personal conflicts of interest that could influence the results reported in this article.

Use of Artificial Intelligence (AI)-Assisted Technology

During the revision of this manuscript, the authors used an Proofread to support language editing, restructuring of the text (such as Claude AI) in response to reviewer comments, preparation of figures from the authors' analytical framework, retrieval of the policy documents, and execution used Nvivo version 12 aplication to of the predefined NVivo text search and matrix coding queries for the document analysis under the authors' direction. The interview data collection, the interpretation of findings, and all analytical decisions were made by the authors. The authors reviewed and edited all content and take full responsibility for the publication.

References

Adewusi, B. A., Adekunle, B. I., Mustapha, S. D., & Uzoka, A. C. (2024). A conceptual model for responsible AI integration in public-facing digital services and platform governance. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(3), 735–767. https://doi.org/10.32628/cseit2425416

Aminah, S., & Saksono, H. (2021). Digital transformation of the government: A case study in Indonesia. *Jurnal Komunikasi: Malaysian Journal of Communication*, *37*(2), 272–288. https://doi.org/10.17576/JKMJC-2021-3702-17

Anggara, S. (2025). Public policy reform in Indonesia: Navigating bureaucratic culture in the age of disruption. *Tec Empresarial*, *20*(2), 716–728. https://doi.org/10.1229/tecempresarialjournal.v20i2.637

Ansell, C., Sørensen, E., & Torfing, J. (2021). The COVID-19 pandemic as a game changer for public administration and leadership? The need for robust governance responses to turbulent problems. *Public Management Review*, *23*(7), 949–960. https://doi.org/10.1080/14719037.2020.1820272

Batara, E., Nurmandi, A., Warsito, T., & Pribadi, U. (2017). Are government employees adopting local e-government transformation? The need for having the right attitude, facilitating conditions and performance expectations. *Transforming Government: People, Process and Policy*, *11*(4), 612–638. https://doi.org/10.1108/TG-09-2017-0056

Bhimavarapu, U. (2025). Smart digital literacy: AI-powered solutions for skill development. In A. Diogo, A. F. Joaquim, & C. V. Almeida (Eds.), *Rethinking literacy in the era of sustainability and artificial intelligence* (pp. 161–186). IGI Global. https://doi.org/10.4018/979-8-3373-0725-1.ch006

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Braun, V., & Clarke, V. (2021a). *Thematic analysis: A practical guide*. SAGE Publications.

Braun, V., & Clarke, V. (2021b). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, *13*(2), 201–216. https://doi.org/10.1080/2159676X.2019.1704846

Cyfert, S., Dyduch, W., Szumowski, W., & Prause, G. (2025). Are we ready for digital transformation? The role of organizational culture, leadership and competence in building digital advantage. *Central European Management Journal*, *33*(2), 219–231. https://doi.org/10.1108/CEMJ-11-2024-0346

Dias, G. P. (2020). Determinants of e-government implementation at the local level: An empirical model. *Online Information Review*, *44*(7), 1307–1326. https://doi.org/10.1108/OIR-04-2020-0148

Diskominfo Provinsi Sumatera Selatan. (2026). *Laporan kinerja instansi pemerintah Dinas Komunikasi dan Informatika Provinsi Sumatera Selatan tahun 2025*. Pemerintah Provinsi Sumatera Selatan. https://esakip.sumselprov.go.id/storage/Files/lainnya_2026_dinas_komunikasi_dan_informatika_v29.pdf

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

Frandell, A., & Feeney, M. K. (2022). Cybersecurity threats in local government: A sociotechnical perspective. *The American Review of Public Administration*, *52*(8), 558–572. https://doi.org/10.1177/02750740221125432

Franklin, C., & Ballan, M. (2001). Reliability and validity in qualitative research. In B. A. Thyer (Ed.), *The handbook of social work research methods* (pp. 273–292). SAGE Publications. https://doi.org/10.4135/9781412986182.n15

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

Gupta, R., & Pal, S. K. (2021). *Introduction to algorithmic government*. Springer Nature Singapore. https://doi.org/10.1007/978-981-16-0282-5

Hadiz, V. R. (2010). *Localising power in post-authoritarian Indonesia: A Southeast Asia perspective*. Stanford University Press.

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine*, *292*, Article 114523. https://doi.org/10.1016/j.socscimed.2021.114523

Kelder, J.-A., Crawford, J., Al Naabi, I., & To, L. (2025). Enhancing digital productivity and capability in higher education through authentic leader behaviors: A cross-cultural structural equation model. *Education and Information Technologies*, *30*(12), 17751–17767. https://doi.org/10.1007/s10639-025-13422-x

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research*, *26*(13), 1753–1760. https://doi.org/10.1177/1049732315617444

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *371*(1987), Article 20120382. https://doi.org/10.1098/rsta.2012.0382

Martín, A. G., & Palomo Zurdo, R. J. (2021). Digital inability and social sustainability in the face of the fourth industrial revolution: A proposal of new non-financial indicators. *Sustainability*, *13*(24), Article 13958. https://doi.org/10.3390/su132413958

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), Article 101385. https://doi.org/10.1016/j.giq.2019.06.002

Nurdin, N., Stockdale, R., & Scheepers, H. (2014). Coordination and cooperation in e-government: An Indonesian local e-government case. *The Electronic Journal of Information Systems in Developing Countries*, *61*(1), 1–21. https://doi.org/10.1002/j.1681-4835.2014.tb00432.x

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE Publications.

Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia. (2019). Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112.

Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. (2023). Lembaran Negara Republik Indonesia Tahun 2023 Nomor 159.

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. (2018). Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182.

Ronfeldt, D. (1992). Cyberocracy is coming. *The Information Society*, *8*(4), 243–296. https://doi.org/10.1080/01972243.1992.9960123

Ronfeldt, D., & Varda, D. (2018). The prospects for cyberocracy (revisited). In G. R. Ricci (Ed.), *Culture and civilization* (Vol. 1, pp. 130–146). Routledge. https://doi.org/10.4324/9781351319720-7

Sahibzada, U. F., Aslam, N., Muavia, M., Shujahat, M., & Rafi-ul-Shan, P. M. (2025). Navigating digital waves: Unveiling entrepreneurial leadership toward digital innovation and sustainable performance in the Chinese IT industry. *Journal of Enterprise Information Management*, *38*(2), 474–501. https://doi.org/10.1108/JEIM-01-2024-0023

Sharmin, S., & Chowdhury, R. H. (2025). Digital transformation in governance: The impact of e-governance on public administration and transparency. *Journal of Computer Science and Technology Studies*, *7*(1), 362–379. https://doi.org/10.32996/jcsts.2025.7.1.27

Sofyani, H., Riyadh, H. A., & Fahlevi, H. (2020). Improving service quality, accountability and transparency of local government: The intervening role of information technology governance. *Cogent Business & Management*, *7*(1), Article 1735690. https://doi.org/10.1080/23311975.2020.1735690

Wagola, R., Nurmandi, A., Misran, & Subekti, D. (2023). Government digital transformation in Indonesia. In C. Stephanidis, M. Antona, S. Ntoa, & G. Salvendy (Eds.), *HCI International 2023 Posters* (Communications in Computer and Information Science, Vol. 1836, pp. 286–296). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-36001-5_37

Wilson, C., & Mergel, I. (2022). Overcoming barriers to digital government: Mapping the strategies of digital champions. *Government Information Quarterly*, *39*(2), Article 101681. https://doi.org/10.1016/j.giq.2022.101681

Wirtz, B. W., Becker, M., & Langer, P. F. (2023). An integrated model of digital open government. *International Journal of Public Administration*, *46*(13), 951–970. https://doi.org/10.1080/01900692.2022.2050386

Xing, Q., Miranda, S. M., & Singh, R. (2020). Resource utilization uncertainty reduction in hospitals: The role of digital capability and governance structure. In *Proceedings of the 41st International Conference on Information Systems (ICIS 2020)*. AIS eLibrary. https://aisel.aisnet.org/icis2020/is_health/is_health/12

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). The Guilford Press.

Yulianto, T., Saleh, C., Noor, I., & Suryadi, S. (2026). Policy implementation in the digital era: A comprehensive analysis of the Electronic-Based Government System (SPBE) in Indonesia. *F1000Research*, *15*, Article 523. https://doi.org/10.12688/f1000research.175463.1

Author's Bio*

Steven Anthony, S.I.P., M.Si. is a lecturer in the Department of Public Administration at Universitas Terbuka, Indonesia. His academic expertise encompasses political theory, journalism, and mass communication, with research interests focusing on governance, public administration, dynamic governance, government-community collaboration, public sector digital transformation, and institutional capacity building in public service delivery. He actively conducts research, scientific publications, and community empowerment initiatives addressing contemporary public governance, digital transformation, and institutional innovation. Email: steven@ecampus.ut.ac.id, ORCID: https://orcid.org/0009-0004-8874-6567.

Dr. Atrika Iriani, M.Si. is an assistant professor and lecturer in the Doctoral Program of Public Administration, Faculty of Social and Political Sciences, Universitas Sriwijaya, Indonesia. Her scholarly expertise centers on public governance, with a specific focus on public policy, dynamic governance, public sector digital transformation, public entrepreneurship, and organizational capacity development. She has authored numerous scientific publications in national and international journals, focusing on public institutional strengthening and governance innovation. Email: atrikairiani@fisip.unsri.ac.id, ORCID: https://orcid.org/0009-0007-4327-5185.

Dr. Doris Febriyanti, M.Si. is an assistant professor and researcher at the Department of Government Studies, Faculty of Government and Cultural Studies, Universitas Indo Global Mandiri, Palembang, Indonesia. She is an awardee of the BPPDN doctoral scholarship from the Ministry of Finance of the Republic of Indonesia. She teaches courses in government ethics, development planning, and research methodology. Her research interests focus on local government studies, public sector performance, urban governance, bureaucratic reform, and sustainable regional development. Email: dorishakiki@uigm.ac.id, ORCID: https://orcid.org/0000-0001-8705-3612.

Dr. Siti Zubaidah, S.Sos., M.Si. is a lecturer and researcher in Public Administration at STIA Bala Putra Dewa and an online tutor at Universitas Terbuka, Indonesia. Her scholarly focus covers urban planning policy, governance, public policy, public sector digital transformation, and tourism development policy. She actively contributes as a peer reviewer for reputable academic journals, is a member of the Indonesian Association for Public Administration (IAPA), and has extensive professional experience as a public policy expert for the South Sumatra Regional Police. Email: sitizu@kampusbalaputradewa.ac.id, ORCID: https://orcid.org/0000-0002-7870-2315.