KIMAP: KAJIAN ILMIAH MAHASISWA ADMINISTRASI PUBLIK
https://journal.unismuh.ac.id/index.php/kimap

(Original Article)

Digital Governance for Safeguarding Digital Population Identity Services in Makassar

Aura Rafika Yusuf [1*], Andi Luhur Prianto [2], Nur Wahid [3]

[1] Public Administration, Muhammadiyah University of Makassar, Indonesia
[2] Government Studies, Muhammadiyah University of Makassar, Indonesia
[3] Public Administration, Muhammadiyah University of Makassar, Indonesia
*Correspondence: aurarafikaa@gmail.com

Abstract : *This study examines digital governance in addressing the misuse of Digital Population Identity (IKD) services at the Population and Civil Registration Office (Disdukcapil) of Makassar City. The rapid digitalization of public services, including IKD, has improved administrative efficiency but also introduced new risks, particularly misuse and digital fraud. This research aims to analyze how digital governance is implemented in mitigating such risks. The study employs a descriptive qualitative approach using the information ecology framework proposed by Bekkers and Homburg (2005), which includes four dimensions: institutional arrangements, information relations, technical infrastructure, and monitoring and control. Data were collected through in-depth interviews with Disdukcapil officials and citizens affected by IKD misuse, as well as observation and documentation. The findings reveal that digital governance practices are primarily administrative, focusing on formal procedures, controlled service access, complaint recording, and basic public education. However, limitations persist in terms of centralized authority, uneven information dissemination, limited digital literacy, and reactive monitoring mechanisms. These conditions reduce the effectiveness of efforts to prevent misuse, especially those driven by social engineering practices. This study concludes that strengthening digital governance requires improved cross-sector coordination, more adaptive and participatory communication strategies, enhanced digital literacy, and the development of risk-based monitoring systems to effectively mitigate misuse in digital public services.*

Keywords: *Digital Governance; Digital Population Identity (IKD); Service Misuse; Digital Fraud; Public Service*

1. Introduction

The utilization of digital technology has become a key driver of modern bureaucratic transformation in many countries. Digitalization not only improves the efficiency of public administration but also enhances transparency, accountability, and public participation in governance (Pasenko, 2022). In the context of developing countries, this transformation plays an important role in bridging the gap between bureaucratic capacity and the increasing demands of society for fast,

accessible, and integrated public services (Huang et al., 2021). The Indonesian government has continuously promoted digital transformation through the implementation of Electronic-Based Government Systems (SPBE), digital population administration, and the development of digital identity as part of public service reform (Cahyarini & Samsara, 2021).

However, the acceleration of digitalization is not always accompanied by the readiness of society to utilize technology safely. Low levels of digital literacy create opportunities for various forms of cybercrime, such as the distribution of phishing links, fake applications, and manipulative communication impersonating official institutions to obtain personal data (Sukmadiansyah & Noviaristanti, 2022). This condition is reinforced by data from the Global Anti-Scam Alliance, which reports that approximately 65% of Indonesians receive digital fraud attempts every week, with total losses reaching IDR 476 billion within a three-month period (Haryanto, 2024). In addition, a survey by APJII shows a significant increase in online fraud victims, from 10.3% in 2022 to 32.5% in 2023 (Rama & Keevy, 2023).

This phenomenon is also evident in the implementation of Digital Population Identity (Identitas Kependudukan Digital/IKD), which was introduced through the Regulation of the Minister of Home Affairs No. 72 of 2022 (Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022, 2022). Although it is normatively supported by data protection regulations, particularly Law No. 27 of 2022 on Personal Data Protection, various cases of misuse continue to occur across regions, including illegal requests for personal data, the spread of fake applications, and fraud through digital communication.

Previous studies have shown that the challenges in implementing digital public services are not limited to technical aspects but also include inadequate infrastructure, low digital literacy, and suboptimal monitoring and service management systems (Kurniawan et al., 2022) However, most studies focus on service implementation and have not specifically

examined how digital governance plays a role in addressing the misuse of digital services.

In practice, efforts by relevant institutions to address misuse in IKD services remain partial, largely limited to public advisories. This approach is considered insufficient as it does not reach all segments of society and fails to keep pace with increasingly complex fraud schemes. Therefore, a more comprehensive approach is needed through the implementation of digital governance that integrates regulatory frameworks, information management, technological infrastructure, and monitoring mechanisms.

Based on the findings of this study, the implementation of digital governance for IKD services in Makassar City has not been fully effective in mitigating the risk of misuse. This is reflected in the centralized nature of authority, the absence of specific Standard Operating Procedures (SOPs) for handling IKD misuse, low levels of digital literacy among citizens, and the underutilization of complaint data in the monitoring system. These conditions indicate that current responses remain administrative and reactive rather than grounded in comprehensive digital risk management.

In this context, digital governance is essential, integrating regulatory, informational, technological, and supervisory aspects into a systematic framework. This study adopts the perspective of Bekkers & Homburg (2005), which emphasizes the interaction between institutional arrangements, information relations, technical infrastructure, and monitoring and control mechanisms in supporting effective digital governance.

The novelty of this research lies in its analytical approach, which not only examines the implementation of IKD services but also specifically explores how digital governance contributes to addressing the risks of misuse in digital-based services. Therefore, this study is expected to provide theoretical contributions to the development of digital governance

studies as well as practical implications for enhancing security and public trust in technology-based population administration services.

2. Method

This study employed a qualitative, descriptive research method. The qualitative approach was chosen because it enables an in-depth understanding of digital governance in addressing the misuse of IKD services by emphasizing meaning, processes, and informants' experiences. Meanwhile, the descriptive type was used to systematically and factually describe the implementation of digital governance within the Disdukcapil of Makassar City.

The data sources in this study consisted of primary and secondary data. Primary data were obtained through in-depth interviews with six informants, including structural officials, technical staff responsible for IKD services, complaint-handling officers, as well as community members who are users and reporters of alleged service misuse. In addition, non-participant observation was conducted to directly observe the IKD service process, data verification mechanisms, and interactions between officers and the public.

Secondary data were collected through documentation studies of various official documents, such as Standard Operating Procedures (SOP) for IKD services, public complaint reports, and relevant regulations, including the Regulation of the Minister of Home Affairs No. 72 of 2022 and Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System (SPBE). Furthermore, scientific literature and online sources, such as official websites and institutional social media, were used as supporting data in this research.

Data collection techniques included in-depth interviews, non-participant observation, documentation studies, and social media analysis. Interviews were conducted in a semi-structured manner to obtain comprehensive and detailed information from informants. Observation was

carried out to understand empirical conditions in the field, while documentation and social media analysis were used to examine policies, information transparency, and communication patterns between the institution and the public. (Sugiyono, 2000)

Data analysis in this study employed the interactive model of Miles and Huberman, which consists of data reduction, data display, and conclusion drawing and verification. Data reduction was carried out by selecting and categorizing data according to the research focus. The data were then presented in a descriptive narrative form to facilitate analysis of relationships among findings. The final stage involved drawing conclusions, which were continuously verified using triangulation techniques of sources, methods, and time to ensure data validity.

3. Results And Discussion

Institutional Arrangements

The findings indicate that institutional arrangements in the implementation of Digital Population Identity (Identitas Kependudukan Digital/IKD) services in Makassar City are supported by a clear regulatory framework, referring to the Regulation of the Minister of Home Affairs No. 72 of 2022. This regulation serves as the foundation for the activation process, digital identity verification, and the management of digital-based population administration services. Operationally, the Department of Population and Civil Registration (Disdukcapil) of Makassar City has implemented a structured activation procedure that requires citizens to undergo direct verification by authorized officers as a form of administrative control to minimize misuse of digital identity.

However, the findings also reveal that the institutional structure governing IKD remains centralized. Local governments face limitations in making technical decisions, such as handling system disruptions or deactivating accounts, as these actions require coordination with the

central government. This condition reflects a significant vertical dependency in digital service governance, which limits local authorities' flexibility in responding to operational issues.

From an implementation perspective, the increasing number of IKD activations in Makassar City indicates the institution's capacity to implement digital policies. Data show a significant rise in the number of IKD users, from 420 individuals in 2021 to 33,333 in 2025. This trend suggests that, administratively, institutional arrangements have supported service expansion and enhanced public adoption of digital technology.

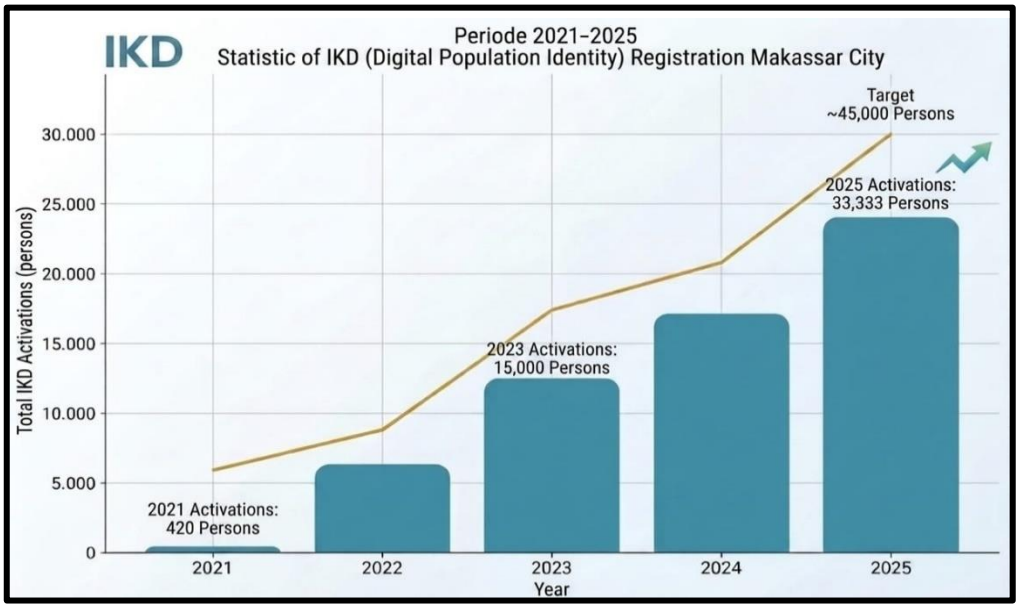

Figure 1. IKD Users in Makassar (2021–2025)
Source: *Department of Population and Civil Registration of Makassar City*

Despite these achievements, they have not been accompanied by adequate strengthening of risk-mitigation measures. The findings reveal the absence of specific Standard Operating Procedures (SOPs) that comprehensively regulate the handling of misuse in IKD services. The current response remains administrative and reactive, primarily involving data blocking in response to citizens' requests after incidents have occurred. This condition indicates that the existing security system is not yet supported by institutional mechanisms for prevention or early detection.

From a theoretical perspective, as noted in (Bovens, 2007) institutional arrangements in digital governance function not only as formal legitimacy but also as mechanisms that determine the distribution of authority and the capacity of institutions to respond to risks. In this context, although the regulatory framework for IKD has been established, its effectiveness remains limited by the limited autonomy of local governments in technical implementation. This is consistent with (Scott, 2013), who emphasizes that institutions are shaped not only by formal rules but also by the organizational capacity to adapt these rules in practice.

Furthermore, this condition reflects a gap between service delivery and protection functions within digital service governance. Previous studies have also shown that e-government implementation in Indonesia tends to focus on service provision, while risk management aspects remain insufficiently integrated (Mahmood et al., 2024). In the case of IKD services in Makassar City, this is evident in the absence of a preventive and standardized system for handling misuse.

In conclusion, the institutional arrangements of IKD services in Makassar City demonstrate strong regulatory legitimacy and structured service procedures. However, the centralized authority structure and the absence of specific SOPs for handling misuse indicate that risk mitigation has not yet been fully institutionalized. Therefore, strengthening digital governance is necessary, not only by focusing on service delivery but also by integrating protection mechanisms and systematic risk management.

Information Relations

The findings indicate that information relations in the implementation of Digital Population Identity (Identitas Kependudukan Digital/IKD) services in Makassar City are carried out through various communication channels, both digital and face-to-face. The Department of Population and Civil Registration (Disdukcapil) of Makassar City has utilized social media, information dissemination in service areas, and direct outreach activities

through mobile service programs (*jemput bola*) as means of educating and disseminating information to the public. These efforts demonstrate that the organization has, institutionally, developed a relatively diverse public service communication system.

Furthermore, the delivery of information accompanied by direct practical implementation through on-site IKD activation reflects the integration between communication and service functions. This communication model enables two-way interaction between officers and the public, allowing clarification processes to occur directly and more effectively.

Figure 2. Fraud Awareness on Digital ID (IKD) Activation
Source: *Youtube, Radio Teslar FM (2025)*

However, the findings indicate that the distribution of information has not been fully equitable. Some members of the public still obtain initial information about IKD through informal social networks, such as family or friends. This condition suggests that official communication channels have not yet been fully effective in reaching all segments of society.

Furthermore, limited digital literacy emerges as a key factor affecting the effectiveness of information relations. Individuals who do not fully understand the basic procedures of IKD services, particularly the requirement for face-to-face verification, are more vulnerable to misinformation. This vulnerability is exploited by fraudsters through

personalized social engineering tactics, such as phone calls or instant messages, that impersonate official institutions.

In this context, information relations do not merely function as a medium for government communication but also constitute a contested space between official information and manipulative narratives constructed by fraud actors. These actors capitalize on gaps in digital literacy and the limited reach of formal communication to quickly build trust through interpersonal approaches.

This phenomenon reflects information asymmetry between institutions and the public. In practice, the information relations established by fraud perpetrators tend to be faster, more personal, and more persuasive compared to formal government communication. As a result, such manipulative information is more easily accepted by certain segments of society, particularly those with lower levels of digital literacy.

From a theoretical perspective, (Castells, 2007) argue that information relations in digital governance are concerned not only with information dissemination but also with the distribution of knowledge and control over information flows. In this case, the limited reach of formal communication indicates that information management has not yet effectively covered all layers of society.

Moreover, from the perspective of the network society, (Castells, 2007) emphasizes that power is not solely held by institutions that produce information but also by actors who control communication flows. This is evident in digital fraud practices, where perpetrators are able to construct more adaptive and responsive communication patterns than formal institutions.

These findings are consistent with previous studies indicating that low levels of digital literacy significantly increase vulnerability to misinformation in digital public services (Schiavo, 2020). In this context, government communication, which tends to be one-way and formal, is

considered insufficient for building public awareness of the risks of digital services.

In addition, the lack of integration between information dissemination and public complaint systems has limited the use of fraud-related reports as continuous public education material. In fact, information derived from public complaints has strong potential to serve as a strategic resource in strengthening risk-based communication strategies.

In conclusion, information relations in IKD services in Makassar City have been implemented through various communication channels in accordance with public service functions. However, their effectiveness is still constrained by the limited reach of formal communication and low levels of digital literacy. Furthermore, information relations have not yet fully served as a mechanism to address misuse, as they are not integrated with complaint-based information management and fraud pattern analysis. Therefore, strengthening information relations should focus on developing more participatory, responsive, and adaptive communication strategies that function as effective instruments for risk mitigation in digital services.

Technical Infrastructure

The findings indicate that the technical infrastructure in the implementation of Digital Population Identity (Identitas Kependudukan Digital/IKD) services in Makassar City has been designed with a layered security system standardized at the national level. This system is centrally managed by the Directorate General of Population and Civil Registration, while the Department of Population and Civil Registration (Disdukcapil) of Makassar City is responsible for service activation, biometric verification, and providing technical assistance to the public. This condition reflects a centralized distribution of authority, in which local governments do not have the capacity to modify the core system but are responsible for ensuring that technical implementation complies with national standards.

Technically, the IKD system is equipped with several security mechanisms, including the use of personal identification numbers (PINs), data encryption, and biometric validation through facial recognition. In addition, the activation process cannot be conducted independently without the involvement of authorized officers, thereby establishing institutional control to ensure the authenticity of user identities. This demonstrates that the IKD system has been designed based on the precautionary principle to minimize the risk of digital identity misuse.

However, the IKD technical infrastructure does not operate in isolation. The National Identification Number (Nomor Induk Kependudukan/NIK), as a single national identity, is integrated across various sectors, including banking, telecommunications, and other public services. While this integration enhances service accessibility, it also increases potential risks, particularly in the event of data breaches occurring at any point within the interconnected system.

Tabel 1. NIK Integration Across Sectors in Indonesia

No.	Sector	Form of NIK Integration	Technical Risk Implications
1.	Banking	KYC verification & account registration	Illegal account creation
2.	Telecommunications	Mandatory SIM card registration using NIK	Misuse of phone numbers for fraud
3.	Health Insurance	NIK as participant identity	Unauthorized access to service data
4.	Public Services	Beneficiary data validation	Manipulation of aid distribution data

The findings indicate that risks in IKD services do not only originate from internal systems but also from interconnections between systems that are beyond the direct control of the Civil Registry Office (Disdukcapil). Data breaches in other institutions that utilize the National Identification Number (NIK) may lead to the misuse of digital identity access, even

though the IKD system itself has been designed securely. This condition reflects the presence of inter-organizational vulnerability within the digital governance ecosystem.

Furthermore, the study reveals that most cases of IKD misuse occur through social engineering, rather than through direct hacking of internal systems. Perpetrators exploit user vulnerabilities by distributing fake application links, requesting personal data, and directing victims to disable security features on their devices. This indicates that threats in digital services are not solely technical in nature, but also social.

This phenomenon emphasizes that the strength of internal security systems does not automatically guarantee user protection, as the primary vulnerability lies in the interaction between the system and its users. In other words, the greatest risk in IKD services exists within the usage ecosystem, rather than merely in the system design itself.

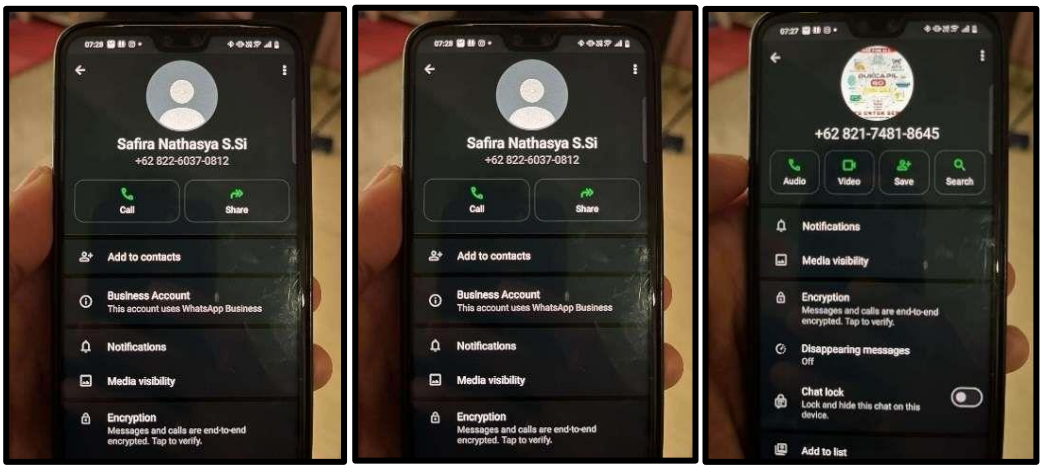

Figure 3. Fraud Impersonation via WhatsApp Numbers
Source: *Mediakonsumen.com, 2024*

The phenomenon illustrated in the figure further demonstrates that although the internal system has an adequate level of security, institutional technical control becomes limited when interactions shift to users' personal devices. In such conditions, fraud perpetrators are able to establish manipulative interactions that are faster, more personal, and more persuasive compared to the formal security mechanisms embedded in the system.

From a theoretical perspective, (Pasenko, 2022) argue that technical infrastructure in digital governance does not merely function as an operational tool, but also as a control mechanism designed to limit potential misuse through security features and technological procedures. However, its effectiveness largely depends on the level of system interconnectedness and the institution's capacity to manage risks that emerge beyond the core system.

In addition, from an interoperability perspective, (Janssen et al., 2015) highlight that cross-sector system integration enhances service efficiency, but simultaneously creates complexity and interdependence that may generate new risks. In this context, the broader the integration of the National Identification Number (NIK) across various services, the greater the potential vulnerability arising from the involvement of multiple actors within the digital ecosystem.

These findings are consistent with previous studies indicating that government digital services tend to have strong core system security, yet remain vulnerable at points of external integration and user interactions outside official platforms (Yuliana & Hasibuan, 2022). This reinforces the argument that the greatest threats in digital services often do not stem from system weaknesses, but rather from user manipulation through social engineering approaches.

Moreover, the limited authority of local governments in managing core systems also constrains the institution's ability to conduct direct technical interventions when potential misuse occurs. This condition further emphasizes that the security of technical infrastructure is inherently multi-actor in nature and cannot rely on a single institution.

Based on these findings, it can be concluded that the technical infrastructure of IKD services in Makassar City possesses adequate internal security capacity through the implementation of encryption, PIN-based authentication, and biometric validation. However, its effectiveness

is still influenced by external risks arising from cross-sector integration, limited institutional control over interactions outside the system, and low levels of digital literacy among the public. Therefore, strengthening technical infrastructure should not only focus on enhancing internal system security, but also adopt an ecosystem-based approach that includes cross-institutional coordination, user protection, and integration with monitoring and risk-based information management mechanisms.

Monitoring and Control

The findings indicate that organizational control in the implementation of Digital Population Identity (IKD) services in Makassar City is carried out through structured administrative supervision mechanisms, particularly at the service activation stage. The Department of Population and Civil Registration (Disdukcapil) of Makassar City implements activation procedures that require citizens to physically visit service offices, where identity verification is conducted through barcode scanning by authorized officers. This mechanism reflects that, institutionally, organizational control is primarily focused on preventing misuse by restricting service access strictly to formal procedures.

Furthermore, the activation process, which involves direct interaction with officers, demonstrates that organizational control is not solely system-based but also relies on administrative interactions. The presence of officers serves as a key instrument in ensuring the validity of digital identities and minimizing the potential for data manipulation from the initial stage of service delivery.

However, organizational control is also closely related to the limitation of service operational hours. The supervision carried out by Disdukcapil is essentially confined within formal working hours, and therefore is not always present when service-related interactions occur beyond these timeframes. In practice, the public often uses time indicators as a

reference to distinguish between official and unofficial communications, for instance when receiving calls or messages outside government office hours.

This empirical condition indicates that organizational control is reflected not only in internal procedures but also in institutional attributes, such as service operating hours. In this context, control functions as a preventive mechanism by establishing boundaries that indirectly help the public recognize irregular interaction patterns.

On the other hand, the monitoring dimension in IKD services is reflected through the implementation of periodic internal evaluations conducted by the Disdukcapil of Makassar City. These evaluations are conducted quarterly or semiannually to identify constraints in service implementation, particularly in technical and operational aspects. This demonstrates that the institution has established a monitoring mechanism as part of its effort to maintain service quality on a continuous basis.

In addition to internal evaluation, monitoring is also indirectly conducted through the reception of public reports and complaints. Information provided by citizens, such as reports of fraud or misuse of IKD services, essentially represents a form of external monitoring that can be utilized to identify risk patterns in practice. Thus, monitoring does not solely originate from internal systems, but also from the interaction between the institution and service users.

However, the findings reveal that the focus of evaluation remains largely centered on internal technical aspects and has not yet fully evolved toward strengthening a risk-based monitoring and control system. In this regard, public complaints actually hold significant potential as a strategic source of information to support organizational monitoring and control functions. Nevertheless, the absence of specific documentation and the lack of structured complaint data management result in this information not being optimally utilized as a basis for trend analysis or policy-making.

Furthermore, the continued occurrence of IKD activation fraud cases indicates that organizational control has not been fully capable of addressing service interactions within the digital space. Such fraud typically occurs through personal communication channels, such as phone calls and messaging applications, which fall outside the direct scope of institutional supervision.

This phenomenon suggests that the existing organizational control remains partial in nature effective within internal bureaucratic settings, yet not sufficiently adaptive to the open and borderless dynamics of digital interactions. Consequently, supervision tends to be reactive, carried out only after public complaints are received, rather than through preventive, system-based mechanisms.

From a theoretical perspective, (Erlenheim et al., 2020) argue that the monitoring and control dimension in digital governance is not limited to compliance with internal procedures, but also reflects the institution's capacity to oversee service interactions involving actors beyond the organization. In this context, the limited scope of control indicates that supervision has not been fully integrated into the broader digital ecosystem.

Moreover, from the perspective of public accountability, (Bovens, 2007) emphasizes that effective organizational control requires proper information management as a foundation for evaluation and policy improvement. In this case, the limitations in managing complaint data indicate that the control system is not yet supported by a strong feedback mechanism.

These findings are consistent with previous studies indicating that monitoring systems in digital public services tend to be administratively oriented and not yet integrated with a risk-based approach (Vaira, 2022) Under such conditions, institutions tend to act after problems occur, rather than anticipating risks proactively.

Therefore, it can be concluded that organizational control in IKD services in Makassar City has been implemented through procedural mechanisms and operational evaluations in line with the institutional functions of Disdukcapil. Meanwhile, the monitoring function is present, but not yet systematically managed or utilized as a risk-based early detection instrument. As a result, its effectiveness remains limited to internal spaces and has not fully extended to digital service interactions. Future improvements should focus on developing an integrated monitoring system, strategically utilizing complaint data, and enhancing adaptive supervisory capacity to respond to the dynamic nature of digital risks.

4. Conclusion

This study aims to analyze the implementation of digital governance in addressing the misuse of Digital Population Identity (IKD) services in Makassar City using the perspective of (Erlenheim et al., 2020). The findings demonstrate that digital governance has been implemented across institutional arrangements, information relations, technical infrastructure, and monitoring and control mechanisms. However, its effectiveness in mitigating misuse risks remains limited due to the lack of integration between these dimensions, particularly in responding to the dynamic nature of digital threats.

The study highlights that governance practices are still predominantly administrative and internally oriented, while risks emerge more significantly in external and user-driven environments. This indicates that the current governance model has not fully adapted to a risk-based and ecosystem-oriented approach. As a result, the handling of misuse tends to be reactive rather than preventive, and monitoring mechanisms have not yet functioned as early detection systems.

This research has several limitations. First, the study is limited to a single local context, which may not fully represent variations in digital governance implementation across regions. Second, the qualitative

approach relies on a limited number of informants, which may affect the generalizability of the findings. Third, the study focuses primarily on institutional perspectives, while broader user behavior and cross-sector dynamics are not explored in depth.

Based on these limitations, future research is recommended to adopt a comparative approach across regions or institutions to provide a more comprehensive understanding of digital governance practices. Further studies should also integrate quantitative data or system-based analysis to strengthen the measurement of risks and effectiveness. In addition, exploring user behavior and digital literacy in greater depth would provide valuable insights into addressing social engineering threats.

From a practical perspective, this study suggests the need to strengthen digital governance by developing integrated, risk-based monitoring systems; managing complaint data as strategic information; enhancing cross-institutional coordination; and increasing public digital literacy. Such efforts are essential to ensure that digital public services are not only efficient, but also secure and resilient against the growing complexity of digital misuse.

Acknowledgments: The author thanks the Department of Population and Civil Registration (Disdukcapil) of Makassar City and all informants for their support.

Declaration Of Conflicting Interests: The author declares no conflict of interest.

Funding: No funding was received

Referensi

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework *European Law Journal*, *13*(4), 447–468.

Cahyarini, B. R., & Samsara, L. (2021). Public Sector Responsiveness in the Strategic Environment Change. *2nd International Conference on Administration Science 2020 (ICAS 2020)*, 212–216.

Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication*, *1*, 29.

Erlenheim, R., Draheim, D., & Taveter, K. (2020). Identifying design principles for proactive services through systematically understanding the reactivity-proactivity spectrum. *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, 452–458.

Huang, N., Yan, Z., & Yin, H. (2021). Effects of online–offline service integration on e-healthcare providers: a quasi-natural experiment. *Production and Operations Management*, *30*(8), 2359–2378.

Janssen, M., Van Der Voort, H., & van Veenstra, A. F. (2015). Failure of large transformation projects from the viewpoint of complex adaptive systems: Management principles for dealing with project dynamics. *Information Systems Frontiers*, *17*(1), 15–29.

Kurniawan, I. A., Yusman, D., Kultsum, G. U., & Junianto, A. (2022). Implementasi E-Government Pada Dinas Kependudukan dan Pencatatan Sipil Kota Tangerang. *Sawala: Jurnal Administrasi Negara*, *10*(2), 256–265.

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*, *32*(1), e12549.

Pasenko, N. (2022). Current trends in digital transformation of public administration. *Scientific Bulletin of Mukachevo State University. Series "Economics*, *9*(2), 46–51.

Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022. (2022). *Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022 Tentang Standar Dan Spesifikasi Perangkat Keras, Perangkat Lunak, Dan Blangko Kartu Tanda Penduduk Elektronik Serta Penyelenggaraan Identitas Kependudukan Digital*.

Rama, P., & Keevy, M. (2023). Public cybersecurity awareness good practices on government-led websites. *International Journal of Research in Business and Social Science (2147-4478)*, *12*(7), 94–104.

Schiavo, R. (2020). The role of civic literacy in infodemic management. In *Journal of Communication in Healthcare* (Vol. 13, Issue 4, pp. 253–255). Taylor & Francis.

Scott, W. R. (2013). *Institutions and organizations: Ideas, interests, and identities*. Sage publications.

Sugiyono. (2000). *Metode Penelitian Administrasi*. Alfabeta.

Sukmadiansyah, R., & Noviaristanti, S. (2022). Digital readiness analysis in Bandung government for smart city implementation. *Int. J. Manag. Finance Account*, *3*(1), 10–17.

Vaira, V. (2022). Smart City Governance and the challenge of digital platforms within the public sector. *2022 IEEE International Smart Cities Conference (ISC2)*, 1–7.

Yuliana, R., & Hasibuan, Z. A. (2022). Best practice framework for information technology security governance in Indonesian government. *International Journal of Electrical and Computer Engineering*, *12*(6), 6522.