VOL. 14 , NO 1, 2026 (145-159)

JURNAL NATAPRAJA:
Kajian Ilmu Administrasi Negara

2406-9515 (p) / 2528-441X (e) https://journal.uny.ac.id/index.php/natapraja

Digital Risk Oversight in the Public Sector: Between Innovation and Institutional Limits

Matheus Gratiano Mali, Natta Sanjaya, Citra Mugi Rahayu

Department of Public Administration, Universitas Tidar, Magelang, Indonesia

ARTICLE INFO

Article history:
Received 3 November 2025
Received in revised form 5 April 2026
Accepted 14 May 2026

ABSTRACT

Digital transformation has become essential for strengthening risk-based public sector oversight. In Indonesia, however, digital supervision remains fragmented and uneven, with limited integration under the Electronic-Based Government System (SPBE). This study examines how digital technologies are applied to enhance risk management and oversight in the Special Region of Yogyakarta. Using a qualitative case study approach, data were collected through in-depth interviews with key stakeholders, including BPKP, the Regional Inspectorate, BPKA, and Diskominfo. The findings show that applications such as SIWARIS, SIPETIR, SIPD, and RMIS have improved efficiency, transparency, and risk visibility; however, their effectiveness is constrained by limited interoperability, fragmented systems, low digital literacy, and weak enforcement authority. As a result, risk management remains largely reactive, with digital tools functioning more as compliance mechanisms than as preventive systems. This study highlights the paradox of partial digitalization and contributes to digital governance literature by emphasizing that effective digital oversight requires integrated systems, early warning capabilities, and a risk-aware institutional culture.

Keyword:
Digital Transformation, Risk Management, Public Sector Oversight, Electronic-Based Government System (SPBE), Accountability Reform

E-mail address: theogratiano@untidar.ac.id

https://doi.org/10.21831/natapraja.v14i1.91063

INTRODUCTION

Digital transformation has increasingly become a core strategy for strengthening governance and public sector oversight across countries. Rather than merely introducing new technologies, digital transformation in government is understood as a fundamental shift in how public institutions organize processes, manage risks, and ensure accountability through data-driven decision-making and integrated digital systems (Gil-Garcia et al., 2017; Mergel et al., 2019). Recent studies emphasize that the adoption of digital tools—such as data analytics, e-audit platforms, and integrated information systems—can enhance transparency, improve monitoring capacity, and support earlier identification of risks and irregularities in public administration (Janssen et al., 2020). In the context of public sector oversight, these technologies enable oversight bodies to move beyond reactive control toward more preventive and risk-based approaches. At the same time, risk management remains a critical governance function in the public sector, not only to prevent fraud and inefficiency but also to safeguard the achievement of policy objectives and public value. Contemporary research highlights that effective risk management increasingly depends on the integration of digital systems with institutional arrangements, organizational capacity, and accountability mechanisms, rather than on technology alone (Arena et al., 2013).

Empirical evidence underscores the impact of digitalization in oversight. digital transformation reduced audit processing time from 30 days to 20 days and decreased the number of irregularities by 30% (Riyanto et al., 2025). Similarly, data from the World Bank (2020) show that countries adopting integrated e-governance platforms report on average 25% faster service delivery and 18% fewer corruption-related complaints compared to those with conventional systems. In Indonesia, the introduction of e-audit by the Audit Board (BPK) and digital procurement systems has improved transparency and reduced collusion in public tenders (Wardi et al., 2024). Support from the digital complaint system is very helpful in realizing good governance, because the purpose of this site is in line with the concept of good governance (Maulana et al., 2020).

Nevertheless, significant challenges persist in digital governance at the local level. Pramuditha et al. (2025) highlight that limitations in digital infrastructure, uneven digital literacy among civil servants and citizens, bureaucratic resistance, and weak system integration continue to hinder the effectiveness of e-government implementation and digital oversight in Indonesian local governments. Despite regulatory frameworks such as the SPBE Presidential Regulation No. 95/2018, fragmented institutional roles and lack of cross-agency coordination persist (Nurhidayat et al., 2024). These findings resonate with international scholarship on digital transformation, which emphasizes that the success of digital initiatives depends less on the technology itself than on organizational readiness and adaptive capacity. A comprehensive review by Plekhanov, Franke, and Netland (2023) highlights that uneven preparedness across organizational units, limited process alignment, and insufficient cultural acceptance frequently undermine the intended benefits of digital transformation initiatives. Their analysis underscores that without parallel changes in organizational structures, capabilities, and governance practices, digital systems—including those supporting risk management and oversight—are unlikely to deliver sustainable performance improvements.

The Yogyakarta Special Region (DIY) provides a critical case for examining these dynamics. DIY has been recognized as one of the most innovative provinces in Indonesia, with steady progress in adopting digital oversight. The Inspectorate employs SIWARIS and SIPETIR for risk-based audit planning and integrated supervision. The Communication and Information Agency (Diskominfo) leads SPBE implementation, promoting interoperability and

cybersecurity standards such as ISO 27001. The Regional Financial and Asset Agency (BPKA) digitized financial reporting via SIPD and online SP2D, though still constrained by manual backups. Meanwhile, BPKP introduced the Risk Management Information System (RMIS) and big data analytics to strengthen internal control maturity (SPIP).

Despite these innovations, quantitative indicators show persistent gaps. The Inspectorate (2023) reported that the digitalization level of oversight in DIY is only 45%, with most agencies still relying on manual methods. BPKA continues to perform double entry between digital and manual systems, exposing risks of inconsistency. Diskominfo's role is advisory rather than mandatory, limiting enforcement capacity. BPKP itself notes that leadership commitment and risk-aware culture remain the biggest barriers to sustainability. These conditions echo global findings: studies in OECD countries indicate that without strong leadership commitment, up to 40% of digital oversight initiatives fail to achieve long-term institutionalization (OECD, 2020).

While existing studies highlight the benefits of digital oversight, ranging from improved efficiency (Yusuf et al., 2025) to reduced corruption risks (Yusuf et al., 2025), most research isolates technological tools from their institutional and organizational contexts. In the Indonesian context, institutional capacity and governance arrangements at the local level often constrain the effective implementation of public sector reforms (Yusuf et al., 2025). However, limited attention has been paid to how these constraints operate within digital risk oversight frameworks. The exploration of multiple oversight actors is critical, as public sector supervision involves complex interactions among institutions with overlapping mandates, fragmented authority, and varying levels of digital readiness. Without effective coordination, digital oversight systems risk becoming siloed and reactive rather than integrated and preventive. Nevertheless, existing studies tend to focus on single institutions or technological adoption alone, overlooking inter-agency collaboration, governance structures, and risk culture. This study addresses this gap by presenting a multi-institutional analysis involving the Inspectorate, Diskominfo, BPKA, and BPKP in the Special Region of Yogyakarta. It demonstrates how digital transformation functions not merely as technological adoption but as a governance strategy for risk oversight, integrating institutional synergy, organizational readiness, and regulatory frameworks.

Theoretically, this study advances the literature by explicitly bridging technology adoption theories notably the Technology Acceptance Model (Davis, 1989) and Diffusion of Innovation (Rogers, 1983) with governance and risk management frameworks, including the COSO Internal Control – Integrated Framework (2013), COSO ERM (2017), ISO 31000:2018, and the World Bank's governance principles (1992). While prior studies have typically examined digital transformation in isolation as either a technological adoption challenge or a governance reform issue, this research contributes a novel integration of both perspectives, situating digital oversight as a socio-technical system embedded within risk-aware governance. The novelty of this approach lies in its focus on how digital platforms, when aligned with institutional risk management frameworks, can transform oversight from a reactive compliance mechanism into a proactive, preventive, and integrative governance process. Practically, this study provides evidence-based policy recommendations for strengthening digital oversight in subnational governance, with the case of the Special Region of Yogyakarta serving as a reference point. Although rooted in DIY, the findings carry broader implications for other Indonesian regions facing similar structural and cultural constraints, thus extending the conversation on digital risk oversight beyond national-level policies to the subnational context where institutional fragmentation is most visible.

METHODS

This study adopted a qualitative approach with a case study design to examine how digital transformation has been implemented to strengthen risk management within public sector oversight in the Yogyakarta Special Region (DIY). A qualitative case study was considered most suitable since it allows for an in-depth exploration of complex institutional dynamics and contextual practices that cannot be adequately captured through quantitative methods. The case study design is particularly relevant when the boundaries between the phenomenon under study and its real-life context are blurred (Creswell & Poth, 2018), as is the case with digital transformation in public oversight which involves multiple actors, overlapping mandates, and evolving institutional frameworks.

The research was situated within the provincial government of DIY, focusing on four central institutions that represent the backbone of the regional oversight ecosystem: the Inspectorate of DIY, the Department of Communication and Informatics (Diskominfo), the Regional Financial and Asset Management Agency (BPKA), and the Financial and Development Supervisory Agency (BPKP). These institutions were selected because each plays a unique yet interdependent role in shaping digital oversight ranging from internal audit and risk-based monitoring, digital infrastructure and cybersecurity, financial management and asset reporting, to capacity building and supervisory functions under the national SPIP framework.

Informants were identified through purposive sampling, emphasizing individuals who possess direct involvement in digital oversight initiatives, hold responsibilities in planning, implementation, or evaluation, and occupy either strategic or technical roles within their respective organizations. A total of eleven informants participated, representing diverse perspectives from the four institutions. As purposive sampling in qualitative inquiry ensures the selection of participants with the most relevant knowledge to illuminate the phenomenon under investigation (Musa et al., 2016).

Table 1. List of Research Informants

No	Institution	Number of Informants	Position/Role	Focus in Digital Oversight
1	Inspectorate of DIY	4	Officials/staff responsible for audit and public sector performance oversight	Implementation of supervision and risk management in the context of digital transformation
2	Department of Communication and Informatics (Diskominfo) DIY	2	Staff involved in the development and management of digital governance systems	Technology infrastructure, system integration, digital regulation, and role in digital transformation
3	Regional Financial and Asset Management Agency (BPKA) DIY	4	Staff responsible for regional financial management and digital-based transparency systems	Budget transparency, digital financial reporting, system integration, and risk-based accountability
4	Financial and Development Supervisory	1	Staff involved in risk management development	Risk management assistance and evaluation,

Agency (BPKP) Representative of DIY	through assistance, supervision, and evaluation	digitalization strategies in oversight, and institutional strengthening
Total	**11 Informants**	

Source: Processed by Author, 2025

Data were collected through in-depth interviews, participant observation, and document analysis to capture both subjective experiences and institutional practices. The interviews explored perceptions of digital adoption, implementation challenges, and institutional strategies for strengthening risk management, guided by theoretical frameworks of digital transformation Elia et al. (2024), risk management Kumar (2022), and good governance (Bank, 1992) . Observations were conducted to examine the use of key digital platforms, including SIWARIS (risk management information system), SIPETIR (inspection and monitoring system), SIPD (regional development information system), and RMIS (risk management information system). These platforms were selected because they represent core components of digital oversight, encompassing risk management, inspection processes, and financial governance within the regional government. Documentary analysis complemented the primary data by examining regulatory frameworks such as Government Regulation No. 60/2008 on SPIP and Presidential Regulation No. 95/2018 on SPBE together with provincial regulations, oversight reports, and performance evaluations. The data were analyzed using thematic analysis, following the framework developed by Braun and Clarke (2006). The analytical process involved familiarization with the transcripts, open coding to generate initial categories, development of overarching themes, and interpretation in relation to the research questions. Themes were further mapped against established theoretical lenses, including the Technology Acceptance Model (Davis, 1989), Diffusion of Innovation (El Malouf & Bahemia, 2025) and the Levers of Control framework (Tessier & Otley, 2012), in order to capture both technological and institutional dimensions of digital oversight. To enhance the trustworthiness of the findings, triangulation of sources and methods was applied, and member checking was conducted by validating interpretations with key informants, consistent with Creswell and Poth (2018) recommendations for enhancing credibility in qualitative research.

The research adhered to ethical standards in qualitative inquiry. All informants were briefed about the objectives of the study and provided informed consent prior to participation. Their identities were anonymized to protect confidentiality, and data were used solely for academic purposes. These procedures align with internationally recognized ethical guidelines for social research (Israel & Hay, 2006).

RESULT AND DISCUSSIONS

From Conventional Oversight to Digital Demands: Expanding Functions and Institutional Pressures

The findings reveal that across institutions in the Yogyakarta Special Region (DIY), digital transformation has become an indispensable requirement for strengthening oversight functions, particularly those involving large volumes of data, multi-stakeholder coordination, and time-sensitive monitoring. The Inspectorate emphasized that “the implementation of oversight in government is increasingly dependent on digital systems, especially for planning,

monitoring, and accelerating follow-up of audit results" (Interview, Inspektorat DIY). This statement reflects how core oversight functions traditionally manual and fragmented now demand integration with digital platforms such as SIWARIS for risk-based audit planning, SIM HP for accelerating follow-up actions, and SIPETIR for integrated monitoring of strategic programs.

A similar pattern is observed in financial oversight. BPKA officials underlined that "the use of SIPD since 2020 was intended to replace manual systems, but given its technical limitations, we still perform double entries between SIPD and Excel" (Interview, BPKA DIY). This condition illustrates that the function of financial transparency and accountability has formally shifted to digital platforms but remains challenged by system immaturity, which necessitates parallel manual processes. Such reliance on hybrid approaches indicates that while oversight tasks have formally adapted to digital frameworks, the transition remains incomplete.

From a risk management perspective, BPKP highlighted that oversight functions must be reframed within digital infrastructures: "the integration of SPIP with digital applications like RMIS and SIMA NG has allowed us to embed risk registers and audit processes in a more systematic way, but the challenge lies in ensuring that OPDs internalize these practices" (Interview, BPKP DIY). This shows that oversight is no longer limited to evaluation or control but extends to developing institutional capacities in digital risk awareness, in line with COSO ERM and ISO 31000 principles.

Diskominfo, while not directly responsible for auditing, plays a strategic supporting role in enabling digital oversight. An official explained: "we facilitate interoperability between OPD systems and provide security standards like ISO 27001 and Indeks KAMI, but we cannot enforce compliance; we can only recommend" (Interview, Diskominfo DIY). This reinforces the notion that digital oversight requires not only internal adaptation of monitoring tasks but also institutional synergy, where IT governance becomes foundational to effective supervision.

These findings resonate with a growing body of literature emphasizing that the adaptation of oversight functions to digital platforms extends beyond technical modernization and requires fundamental changes in institutional roles, workflows, and organizational culture. Mergel, Edelmann, and Haug (2019) argue that digital transformation in the public sector demands organizational restructuring, capacity building, and leadership-driven change rather than mere technology adoption. In the Indonesian context, Sigit Wahyudi, Aldian Yusup, and Muhammad Rizki Perdana (2025) find that digital transformation has improved service speed, transparency, and citizen experience in government services, but effective implementation remains hindered by organizational constraints such as inadequate digital competencies among civil servants, fragmented infrastructure, and governance readiness gaps. At the international level, studies on digital government emphasize that digital initiatives including digital oversight systems often struggle to achieve sustainable outcomes when institutional coordination is weak, leadership support is insufficient, and technological solutions are not aligned with existing organizational structures and governance arrangements (Gil-Garcia et al., 2017).

In DIY's case, the evidence indicates that the oversight functions most in need of digital adaptation include (1) audit planning and execution, (2) monitoring and evaluation of financial processes, (3) risk identification and mitigation, and (4) data security and system interoperability. The reliance on platforms like SIWARIS, SIPETIR, and SIPD demonstrates the institutional recognition of digital oversight as a necessity. However, the persistence of manual practices, hybrid reporting systems, and reliance on advisory rather than regulatory enforcement highlights the unevenness of adaptation across institutions.

This reflects a dual reality. On one hand, digital technologies have enabled oversight institutions to enhance efficiency, accelerate decision-making, and improve transparency by strengthening data availability, traceability, and real-time monitoring capacities. Empirical studies on digital government show that the use of data-driven systems and digital audit tools can reduce information asymmetry and limit opportunities for discretionary manipulation (Janssen et al., 2012; Mergel et al., 2019). On the other hand, the partial adoption observed in the DIY context illustrates persistent institutional risks associated with digital oversight, including system dependency, fragmented implementation, and resistance from actors embedded in traditional bureaucratic routines, as highlighted in comparative studies of digital governance reforms (Kitchin, 2014).

In sum, the adaptation of oversight functions to digital environments in DIY illustrates both progress and limitation. It signifies a transition from conventional oversight mechanisms towards integrated, technology-driven practices, yet the process remains uneven, shaped by institutional readiness, system maturity, and leadership commitment. The findings reinforce that digital adaptation is not solely about adopting new technologies but about embedding them within organizational routines, regulatory frameworks, and cultures of accountability. These findings suggest that existing digital transformation theories, which often assume linear progression toward integration and efficiency, may overlook the fragmented and politically constrained nature of oversight systems in decentralized governance contexts. In this regard, the DIY case highlights the need to reconceptualize digital transformation not merely as technological adoption, but as an institutional negotiation shaped by power, capacity, and governance asymmetries.

Fragmented Digital Transformation in Oversight: Between Innovation and Institutional Constraints

The study reveals that digital transformation in oversight within the Yogyakarta Special Region (DIY) has been implemented through a gradual yet uneven process, marked by institutional innovation, partial system integration, and persistent technical and organizational challenges. The Inspectorate of DIY has been at the forefront of adopting digital tools to systematize supervision. One senior official stated that “applications such as SIPETIR are being developed as an integrated platform, covering the entire cycle of oversight from risk-based work planning to follow-up actions, thereby reducing manual duplication and increasing timeliness” (Interview, Inspektorat DIY). This illustrates how oversight functions, which previously relied heavily on manual data management, are being restructured through digitalization to support efficiency and accountability.

In financial governance, BPKA has implemented the SIPD system for budget planning, financial reporting, and monitoring, replacing the older SIPKD. However, as another informant admitted, “because SIPD still cannot accommodate all modules, we still rely on parallel manual processes using Excel, especially for validation and reconciliation” (Interview, BPKA DIY). This hybrid implementation underscores the gap between regulatory expectations of a fully digital oversight mechanism and the technical realities of system maturity.

Diskominfo plays a crucial supporting role by ensuring system interoperability and cybersecurity. An official highlighted: “our role is to facilitate integration across OPDs through SPBE guidelines, prevent duplication of applications, and provide security standards, but enforcement remains limited since we cannot compel OPDs to comply” (Interview, Diskominfo DIY). Their statement reflects how digital transformation in oversight depends not only on technology but also on institutional authority and inter-organizational collaboration.

At the national supervisory level, BPKP has contributed to embedding risk management into digital oversight frameworks. A BPKP representative explained that "RMIS and SIMA NG have allowed us to digitize risk registers, audit workflows, and supervisory reporting, while simultaneously aligning with SPIP and international standards such as COSO ERM and ISO 31000" (Interview, BPKP DIY). The ability to digitize and centralize risk management processes represents a significant step in ensuring real-time oversight and evidence-based decision-making.

These findings are consistent with prior scholarship emphasizing the transformative potential of digitalization in government oversight. Studies on digital government demonstrate that the use of data-driven monitoring systems and integrated digital platforms enables public institutions to track performance more transparently and improve accountability by reducing information asymmetry (Janssen et al., 2020). Research on public sector digital transformation further indicates that digital audit tools and real-time data integration can enhance risk detection and accelerate oversight processes, provided that organizational readiness and governance structures are in place (Mergel et al., 2019). At the international level, OECD (2019) reports that countries implementing integrated digital oversight and monitoring systems tend to experience higher compliance and accountability outcomes, particularly when supported by strong institutional coordination and leadership commitment.

Yet, the DIY case also highlights critical limitations in the institutionalization of digital oversight. Despite advances in applications such as SIPETIR, SIPD, and RMIS, the continued reliance on manual backups, limited system interoperability, and the predominance of advisory rather than mandatory authority constrain the effectiveness of digital oversight mechanisms. This condition reflects broader findings in digital government literature, which emphasize that partial and uneven implementation often weakens the intended benefits of digitalization when human resource capacity, organizational integration, and bureaucratic culture are not adequately aligned with technological change (Janssen et al., 2020) ; (Mergel et al., 2019). Comparative international evidence further suggests that without strong institutional coordination and enforcement authority, digital oversight systems tend to coexist with traditional practices rather than replacing them, thereby limiting their transformative impact (Bank, 2021).

Taken together, the implementation of digital transformation in oversight in DIY demonstrates a transitional stage. Institutions have recognized the necessity of digital tools and have embedded them into core oversight processes, from financial monitoring to risk-based auditing. However, the persistence of hybrid practices and incomplete integration reveals that digitalization remains a work in progress, shaped as much by organizational readiness and political will as by technological capacity. In line with (Mergel et al., 2019).

This suggests that digital oversight must be seen not simply as a technological upgrade but as a broader governance reform that requires cultural adaptation, regulatory reinforcement, and institutional collaboration. These findings challenge dominant perspectives in digital transformation literature, which often assume a linear progression toward integration and efficiency. In contrast, the DIY case demonstrates that digital transformation in oversight is inherently fragmented, shaped by institutional constraints, uneven authority, and organizational resistance. This suggests that digital transformation should be reconceptualized as a non-linear and contested process, where technological innovation coexists with legacy practices rather than fully replacing them.

Reactive Risk Management Systems: Evidence of Limited Integration in Digital Oversight

The implementation of risk management and oversight systems in the Special Region of Yogyakarta (DIY) illustrates the opportunities and challenges of embedding digitalization into governance practices. At present, risk management has been formally integrated into various oversight mechanisms through the adoption of several digital platforms such as SIPETIR (the Inspectorate's risk-based supervision system), SIWARIS (Risk Management Information System), SIPD (Local Government Information System mandated nationally), and the risk management applications developed under the coordination of the BPKP Regional Office. These tools are designed to map, monitor, and mitigate risks across public administration and financial management processes. However, the effectiveness of these systems remains constrained by technical, institutional, and cultural factors that reveal the paradox of partial digitalization in oversight.

From the perspective of the Inspectorate of DIY, digitalization has provided new channels for structuring risk registers and aligning them with supervisory functions. Through SIPETIR, the Inspectorate seeks to integrate risk identification into audit planning. Yet, as one Inspectorate official admitted, "We already use SIPETIR to record risks, but in practice many agencies still rely on Excel and manual reporting. The integration with other platforms, such as SIPD, has not been fully realized" (Interview, Inspectorate DIY). This coexistence of manual and digital systems not only undermines operational efficiency but also generates inconsistencies in risk identification and categorization across agencies. Such fragmented practices are widely discussed in the public sector governance literature, which shows that risk-based approaches in government oversight often remain procedural and compliance-driven when they are not fully integrated into organizational decision-making processes and institutional routines (Arena et al., 2013; Power, 2007). As a result, digital tools tend to operate in parallel with traditional control mechanisms rather than transforming the underlying governance framework.

For the BPKP Regional Office, digital oversight is seen as a crucial instrument in advancing proactive risk management. BPKP promotes the adoption of risk management systems that integrate with audit activities, thereby strengthening prevention-oriented supervision. Nevertheless, BPKP acknowledges that digital tools alone cannot guarantee success. As one official highlighted, "Technology helps us visualize risks faster, but the problem is that risk awareness among managers is still low. Systems are sometimes treated as a formality instead of being internalized into daily decision-making" (Interview, BPKP DIY). This condition reflects a broader pattern in public sector governance in which risk oversight mechanisms tend to be treated as formal administrative requirements rather than as instruments that meaningfully influence organizational behavior and decision-making. The persistent gap between procedural compliance and substantive practice underscores the importance of organizational culture and institutional learning, which remain insufficiently developed in many public organizations implementing risk-based oversight frameworks (Arena et al., 2013; Hood & Dixon, 2015).

The Regional Financial and Asset Management Agency (BPKA) represents another critical node in risk oversight. With responsibility for budgetary planning and financial accountability, BPKA relies heavily on SIPD for reporting and monitoring. While SIPD offers transparency by centralizing financial data, its integration with risk-based monitoring remains inadequate. A BPKA representative explained, "We input and monitor budget realization through SIPD, but the connection with risk management systems is not automatic. Coordination with the Inspectorate or BPKP still requires manual data

reconciliation" (Interview, BPKA DIY). This demonstrates a persistent lack of interoperability between financial management systems and risk oversight mechanisms. Studies on digital government and public sector integration highlight that the absence of seamless data exchange across systems often limits the effectiveness of performance monitoring and risk prevention, as financial transparency alone does not automatically lead to proactive risk management when systems operate in silos (Janssen et al., 2020; Mergel et al., 2019). Without integrated data architectures and coordinated governance arrangements, digital oversight tools tend to support reporting functions rather than enabling anticipatory risk identification and mitigation.

Meanwhile, the Department of Communication and Informatics (Diskominfo) serves as the backbone of digital governance in DIY by ensuring infrastructure readiness and providing policy frameworks. However, Diskominfo has no binding authority to enforce the adoption of specific risk management systems across agencies. A Diskominfo official noted, "We can facilitate and provide the digital infrastructure, but it is not our authority to ensure that BPKA or the Inspectorate fully implement these systems. Each has its own mandate" (Interview, Diskominfo DIY). This structural limitation reveals persistent institutional fragmentation that undermines the effectiveness of digital governance in the region. Empirical research on e-government implementation in Indonesian public institutions indicates that unclear authority, overlapping responsibilities, and weak inter-organizational coordination continue to hinder the institutionalization of digital systems. Recent studies show that uneven institutional readiness and fragmented governance arrangements cause many digital initiatives to operate in silos, thereby limiting their capacity to support integrated accountability and effective oversight functions (Nurhidayat et al., 2024).

The challenges in DIY therefore extend beyond technical infrastructure to encompass organizational culture, regulatory clarity, and institutional coordination. Despite the presence of multiple digital platforms, the risk management process often remains reactive rather than preventive. Risks are identified once problems have already materialized, and oversight systems tend to be used more as reporting instruments than as predictive tools. As one auditor from the Inspectorate observed, "We conduct risk mapping, but often it is done after incidents occur, not before. The system is more of a compliance checklist" (Interview, Inspectorate DIY). This reactive orientation reflects a broader pattern in public sector risk oversight, where risk management practices tend to prioritize procedural compliance and post-event correction rather than preventive and anticipatory control, particularly when risk frameworks are not fully embedded in organizational decision-making processes (Arena et al., 2013).

Another significant complexity is the uneven digital literacy among auditors and government staff. Although training sessions have been conducted, adoption remains slow. A staff member from the Inspectorate revealed, "Some of our auditors are still not confident in using SIWARIS or SIPETIR optimally. They prefer manual documentation because they are more familiar with it" (Interview, Inspectorate DIY). Low digital capability among oversight personnel reduces the potential impact of technological tools and creates resistance to change. This condition is consistent with empirical research on e-government implementation in Indonesia, which shows that limited capacity and digital competencies among civil servants remain significant barriers to the effective implementation of electronic government systems (SPBE). Studies analyzing the E-Government Development Index in Indonesia point out that lack of understanding of technical aspects and information security among human resources, especially civil servants, contributes to uneven implementation and suboptimal outcomes in digital governance initiatives (Nurhidayat et al., 2024).

In addition, regulatory ambiguity and weak authority arrangements continue to undermine the institutionalization of digital risk management. Although SPBE and internal control frameworks formally encourage the integration of digital oversight, recent studies show that enforcement mechanisms remain limited, resulting in inconsistent implementation across government agencies. In the absence of clear sanctions, incentives, or binding authority, digital oversight systems are frequently treated as supplementary tools rather than mandatory governance instruments. Empirical evidence from Indonesia indicates that gaps in regulatory clarity and institutional authority contribute to fragmented implementation and weaken the effectiveness of digital governance reforms (Nurhidayat et al., 2024).

Taken together, the risk management and oversight systems in DIY present a picture of fragmented digital adoption, cultural resistance, and institutional misalignment. On the one hand, digital platforms have undeniably introduced greater transparency, efficiency, and potential for early warning. On the other hand, the persistence of manual practices, low interoperability, uneven digital literacy, and weak regulatory authority undermine the creation of a cohesive and proactive risk management system. This paradox of partial digitalization illustrates that the transformation of oversight cannot rely solely on technological innovation; it must be accompanied by institutional reform, capacity building, and a cultural shift towards risk-aware governance. Digital transformation in the public sector should not be understood merely as the adoption of technological tools, but as a broader reconfiguration of governance arrangements that embeds risk management into the core of organizational decision-making processes (Mergel et al., 2019).

In conclusion, the case of DIY highlights both the progress and the limitations of digital oversight in public risk management. Digital systems like SIPETIR, SIWARIS, SIPD, and RMIS have laid an important foundation, but their potential remains unrealized without integration, authority, and cultural alignment. Addressing these weaknesses requires a multi-dimensional approach that combines technological innovation with regulatory enforcement, cross-agency coordination, and sustained investment in human capital. Only then can digital risk oversight evolve from a fragmented compliance exercise into a truly preventive, integrated, and transformative governance system. These findings challenge dominant risk management frameworks, such as COSO ERM and ISO 31000, which often assume that formal structures and digital tools will lead to proactive and integrated risk governance. In the DIY context, however, the persistence of fragmented systems, limited interoperability, and weak institutional authority demonstrates that risk management remains embedded in compliance-oriented practices rather than strategic decision-making. This suggests that existing frameworks need to be reconceptualized to better account for institutional fragmentation, capacity disparities, and governance constraints in decentralized public sector environments.

Toward Integrated Digital Oversight: Bridging Institutional Silos and Strengthening Risk Governance

The effectiveness of digital transformation in oversight within the Yogyakarta Special Region (DIY) can be evaluated along three dimensions: efficiency gains, transparency improvements, and institutionalization of risk-based approaches. Evidence from the Inspectorate indicates that applications such as SIWARIS and SIPETIR have accelerated audit planning and monitoring processes, reducing the time required for oversight activities. As one official explained, “with SIPETIR, we can track the progress of audit follow-ups in real time, which was not possible when everything was done manually” (Interview, Inspektorat DIY). This demonstrates a tangible gain in efficiency and responsiveness.

BPKA also reported positive effects of digital adoption, particularly with the implementation of SIPD and SP2D Online. These systems improved the speed of financial reporting and reduced human error in bookkeeping. Yet, effectiveness remains constrained by technical immaturity, as another official admitted: "we still have to double-check and reconcile with Excel because SIPD often cannot generate the reports needed on time" (Interview, BPKA DIY). This dual reliance illustrates that while digitalization has improved transparency, it has not fully replaced conventional systems.

From BPKP's perspective, the introduction of RMIS and SIMA NG has improved the comprehensiveness of risk management. A BPKP representative emphasized that "the strength of RMIS lies in making risks visible across OPDs, but the effectiveness depends on whether the culture of risk awareness is truly embedded" (Interview, BPKP DIY). This suggests that digital tools provide opportunities for oversight effectiveness, but their sustainability relies on leadership commitment and organizational culture. Diskominfo also plays a role by strengthening cybersecurity, although its function is primarily facilitative rather than authoritative. An informant highlighted, "we can recommend compliance with ISO 27001 and Indeks KAMI, but we cannot enforce adoption across all OPDs" (Interview, Diskominfo DIY), thereby pointing to a structural limitation in institutional authority.

Despite these gains, several challenges persist. First, system fragmentation and limited interoperability continue to constrain the effectiveness of digital oversight, as multiple applications operate in silos and generate duplication and inefficiencies. Recent empirical studies on e-government and SPBE implementation in Indonesia highlight that fragmented system architectures and weak inter-agency integration undermine coherent digital governance and accountability mechanisms (Nurhidayat et al., 2024). Second, digital literacy and human resource capacity remain uneven. Research on digital transformation in the public sector indicates that limited technical skills, resistance to organizational change, and insufficient capacity-building strategies among civil servants slow the effective use of digital systems, resulting in continued reliance on manual or semi-digital tools despite the availability of advanced applications (Mergel et al., 2019). Third, institutional and regulatory constraints hinder full implementation. Comparative studies on digital governance reforms demonstrate that fragmented authority, unclear mandates, and weak enforcement mechanisms often prevent digital oversight initiatives from being fully institutionalized, causing them to remain symbolic rather than operational in daily governance practices (Cordella & Paletti, 2018).

Quantitative and institutional indicators from the DIY context further reinforce these challenges. Internal reports and field evidence from the Inspectorate indicate that digitalization of oversight functions remains partial, with many OPDs still relying on manual or semi-digital procedures alongside existing applications—resulting in dual systems that increase administrative workload and limit the analytical capacity of digital oversight tools. Moreover, interviews and institutional assessments reveal that leadership commitment is a recurring constraint in sustaining digital oversight initiatives in DIY; without clear managerial support and enforcement, organizational units tend to deprioritize full adoption of digital practices. These patterns are consistent with recent Indonesian research on e-government and SPBE implementation, which shows that fragmented system integration, uneven human resource capacity, and weak organizational readiness continue to hinder the institutionalization of digital governance and oversight, especially at the local government level (Kennedy et al., 2024; Yeremias et al., 2024).

In evaluating overall effectiveness, therefore, the digital transformation of oversight in DIY can be considered partially effective. It has yielded improvements in speed, transparency,

and risk visibility, but these outcomes are uneven across institutions. The key barriers lie not only in technology but also in organizational adaptation, leadership, and regulatory authority. This finding reinforces the view that digital transformation in the public sector should not be understood primarily as the deployment of technological tools, but as a process of embedding digital systems into governance arrangements and accountability cultures that shape organizational behavior and decision-making (Mergel et al., 2019).

In sum, while DIY has demonstrated progress in digital oversight, the persistence of manual practices, fragmented systems, limited digital literacy, and weak enforcement highlight the need for stronger institutional integration. The challenge moving forward is not merely technological innovation but ensuring cultural, structural, and regulatory alignment that can institutionalize digital oversight as an integral part of governance reform. These findings suggest that achieving integrated digital oversight requires more than technological alignment; it demands the deliberate bridging of institutional silos through coordinated governance mechanisms, shared data architectures, and strengthened regulatory authority. The DIY case illustrates that without clear enforcement, interoperable systems, and a unified risk governance framework, digital transformation will remain fragmented. Therefore, integrated digital oversight should be conceptualized as a governance reform process that aligns institutional mandates, enhances inter-agency collaboration, and embeds risk-based thinking into organizational practices.

CONCLUSION

This study demonstrates that digital transformation in public sector oversight in the Special Region of Yogyakarta (DIY) has improved efficiency, transparency, and risk visibility through the adoption of platforms such as SIPETIR, SIWARIS, SIPD, and RMIS; however, its implementation remains fragmented and only partially effective due to limited interoperability, hybrid manual–digital practices, uneven digital literacy, and weak enforcement authority. These findings highlight the need for stronger institutional integration, interoperable systems, and capacity building to support effective digital oversight practices. Theoretically, the study contributes to digital governance literature by revealing the paradox of partial digitalization, where technological adoption does not automatically lead to integrated and proactive oversight, thus emphasizing that digital transformation should be understood as a complex institutional reform shaped by governance structures, organizational readiness, and cultural dynamics rather than merely a technological upgrade.

AI DICLOSURE STATEMENT

Generative AI tools were utilized exclusively for language-related assistance, including paraphrasing, grammar checking, abstract translation, sentence structure improvement, and brainstorming of the manuscript outline. These tools were employed solely to enhance the readability and presentation of the manuscript. The intellectual and scientific substance of the study, including problem formulation, theoretical framework development, research methodology, data analysis, interpretation of results, discussion, and conclusions, was entirely developed by the authors. No AI tools were used to generate research data, conduct primary scientific analyses, interpret findings, or write the manuscript autonomously. The authors retain full responsibility for the content, accuracy, and scholarly integrity of this work.

ACKNOWLEDGEMENTS

The authors would like to express sincere gratitude to the Financial and Development Supervisory Agency (BPKP) Regional Office of Yogyakarta Special Region, the Inspectorate of Yogyakarta Special Region, the Regional Financial and Asset Management Agency (BPKA), and the Department of Communication and Informatics (Diskominfo) for their invaluable support and collaboration during the research process. Appreciation is also extended to the Institute for Research and Community Service (LPPM), Universitas Tidar, for providing financial support through its internal research grant under the Stimulus Scheme. The authors further acknowledge the contributions of fellow academic colleagues and research assistants whose dedication and input greatly enhanced the quality and completion of this study.

REFERENCES

Arena, M., Azzone, G., Cagno, E., Ferretti, G., Prunotto, E., Silvestri, A., & Trucco, P. (2013). Integrated Risk Management through dynamic capabilities within project-based organizations: The Company Dynamic Response Map. *Risk Management*, *15*, 50–77. https://doi.org/10.1057/rm.2012.12

Bank, W. (1992). *Governance - the World Bank's experience*.

Bank, W. (2021). *GovTech Maturity Index: The State of Public Sector Digital Transformation*. The World Bank Group.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101. https://doi.org/10.1191/1478088706qp063oa

Cordella, A., & Paletti, A. (2018). ICTs and value creation in public sector: Manufacturing logic vs service logic. *Information Polity*, *23*, 1–17. https://doi.org/10.3233/IP-170061

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry & Research Design* (fourth). SAGE Publications India.

Davis, F. D. (1989). *Perceived Usefulness , Perceived Ease of Use , and User Acceptance of Technology Information*. *13*(3), 319–340.

El Malouf, N., & Bahemia, H. (2025). *Diffusion of Innovations*. TheoryHub Book.

Elia, G., Solazzo, G., Lerro, A., Pigni, F., & Tucci, C. L. (2024). The digital transformation canvas: A conceptual framework for leading the digital transformation process. *Business Horizons*, *67*(4), 381–398. https://doi.org/https://doi.org/10.1016/j.bushor.2024.03.007

Gil-Garcia, J. R., Dawes, S., & Pardo, T. (2017). Digital government and public management research: finding the crossroads. *Public Management Review*, *20*, 1–14. https://doi.org/10.1080/14719037.2017.1327181

Hood, C., & Dixon, R. (2015). *A Government that Worked Better and Cost Less ? Reform and Change in UK Central Government*. Oxford University Press.

Israel, M., & Hay, I. (2006). *Research Ethics for Social Scientists Between ethical conduct and regulatory compliance*. SAGE Publications Ltd.

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. *Information Systems Management*, *29*, 258–268. https://doi.org/10.1080/10580530.2012.716740

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, *50*, 302–309. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.08.012

Kennedy, A., Surya, W. H., & Wartoyo, F. X. (2024). Tantangan dan Solusi Penerapan E-Government di Indonesia. *Jurnal Terapan Pemerintahan Minangkabau*, *4*(2), 134–147.

Kitchin, R. (2014). *Big Data , new epistemologies and paradigm shifts*. (June), 1–12. https://doi.org/10.1177/2053951714528481

Kumar, S. (2022). Risk Management Framework. In *SSRN Electronic Journal* (4). https://doi.org/10.2139/ssrn.4141546

Maulana, A., Aryaputri, H., & Rosyari, F. R. (2020). Application of e-Goverment System As An Effort to Create A Conductive Investment Climate in Banyuwangi Regency. *NATAPRAJA*, *8*(2), 106–119. https://doi.org/10.21831/jnp.v8i2.34023

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4), 101385. https://doi.org/https://doi.org/10.1016/j.giq.2019.06.002

Musa, S., Alkassim, R., & Sunusi, R. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4.

Nurhidayat, N., Nurmandi, A., & Misran, M. (2024). Evaluation of the Challenges of E-Government Implementation: Analysis of the E-Government Development Index in Indonesia. *Jurnal Manajemen Pelayanan Publik*, *8*, 371–383. https://doi.org/10.24198/jmpp.v8i2.52759

OECD. (2020). *The OECD Framework for digital talent and skills in the public sector* (Number 45).

Plekhanov, D., Franke, H., & Netland, T. H. (2023). Digital transformation: A review and research agenda. *European Management Journal*, *41*(6), 821–844. https://doi.org/https://doi.org/10.1016/j.emj.2022.09.007

Power, M. (2007). Organized Uncertainty: Designing A World of Risk Management. In *Public Administration* (Vol. 86). https://doi.org/10.1111/j.1467-9299.2008.00756_2.x

Pramuditha, R., Muhafidin, D., Sumaryana, A., & Susanti, E. (2025). E-Government Implementation and Public Service Quality: Challenges and Opportunities in Indonesian Local Administration. *Tec Empresarial*, *20*(1), 61–70.

Riyanto, J., Wijaya, T., Prasetyo, I., Rahmatika, N., & Indriasih, D. (2025). *ARTIFICIAL INTELLIGENCE AND AUDIT QUALITY : AN EMPIRICAL LITERATURE REVIEW FROM SCOPUS*. *20*(01), 61–76.

Rogers, E. M. (1983). *DIFFUSION OF INNOVATIONS Third Edition*.

Tessier, S., & Otley, D. (2012). A conceptual development of Simons' Levers of Control framework. *Management Accounting Research*, *23*(3), 171–185. https://doi.org/https://doi.org/10.1016/j.mar.2012.04.003

Wahyudi, S., Yusup, A., & Perdana, M. R. (2025). Analysis of digital transformation of public administration in improving the effectiveness of government services in Indonesia. *Jurnal Konseling Dan Pendidikan*, *13*(3), 575–585.

Wardi, W., Sugiyono, H., & Winanti, A. (2024). *International Journal of Social Science and Human Research Supervision System for Indonesia ' s Procurement of Goods and Services Government*. *07*(06), 4432–4440. https://doi.org/10.47191/ijsshr/v7-i06-105

Yeremias, T. K., Cahyadi, D., & Djunaedi, A. (2024). Modelling E-Government Maturity Determinants at the Local Level in Indonesia Using Technology-Organization-Environment Framework. *Jurnal Ilmu Sosial Dan Ilmu Politik*, *28*(1), 17–34.

Yusuf, M. A., Kusumawati, H., Irwansyah, A., & Syahirah, N. (2025). *The Role of Digital Technology in Enhancing Public Service Efficiency in Indonesia*. *9*(1), 16–23. https://doi.org/10.26487/hebr.v9i1.6420