

Human-Centered Digital Readiness and Internal Control for Strengthening Public Sector Accountability: A Conceptual Dataset-Based Review

Udin Saepudin¹, Ronaldo Fransiskus²

¹Universitas Pertiwi, Bekasi, Indonesia

²Universitas Sumatera Utara, Medan, Indonesia

*Corresponding author: udin.saepudin@pertiwi.ac.id

ABSTRACT

Abstract. Public institutions increasingly rely on digital technologies to manage transactions, deliver services, and support administrative decision-making. However, digital transformation alone does not ensure public accountability. This conceptual paper proposes a human-centered framework integrating digital readiness and internal control to strengthen public sector accountability. The study adopts a conceptual dataset-based review by synthesizing evidence from **ten selected Data in Brief articles** covering e-government readiness, public sector accounting readiness, corporate governance, corruption risk assessment, audit reporting, tax compliance, governance indicators, and public data management. Rather than statistically reanalyzing the datasets, the study examines how these articles conceptualize and connect key governance constructs. The synthesis indicates that digital readiness enhances organizations' capacity to utilize digital systems and interpret risk-related information, while internal control provides the mechanisms for authorization, monitoring, documentation, and regulatory compliance. Together, these complementary capabilities support a human-centered, risk-aware digital governance framework that strengthens transparency, accountability, and organizational resilience.

Keywords: *digital governance, digital readiness, internal control, public accountability, risk aware governance.*

1. INTRODUCTION

Digital transformation is no longer a distant policy slogan for the public sector. In many public organizations, daily work already depends on information systems, online services, data repositories, and administrative platforms. These tools can speed up services and make records easier to check. Yet a modern system does not automatically create accountable government. Accountability remains weak when users are not prepared to read data, make decisions from it, or operate within a reliable control environment.

Kaiser and Gadár (2023) show that e-government readiness goes beyond device ownership or the existence of online services. Their dataset covers digital literacy, internet-use patterns, attitudes toward smart systems, technophile and technophobic orientations, and citizens' administrative habits. These elements are important because digital readiness is also about people, habits, and institutional settings, not only technology.

The same issue appears in public sector accounting. Alghizzawi (2025) reports that government accountants' readiness to implement International Public Sector Accounting Standards is shaped by human resources and information technology. Accounting reform and digital reform therefore depend on people, systems, and institutions moving together.

Internal control remains just as important. Digital systems may accelerate administrative routines, but speed does not prevent errors, misuse of authority, or corruption. Vasconcelos and Cavique (2022) show that corruption risk assessment in public administration can be improved by integrating several government databases. Such integration becomes useful when risk information is connected with governance arrangements and control mechanisms.

Al-Jundi and Augustine (2026) add that tax evasion is associated with deviant culture, weak law enforcement, and administrative corruption. The point is clear: accountability requires more than digital tools. It also needs rule enforcement, institutional integrity, internal control, and public actors who can use information responsibly.

Based on these concerns, this paper discusses how digital readiness and internal control can be placed in one framework for public sector accountability. Its contribution is conceptual. The discussion uses selected dataset articles on e-government readiness, public sector accounting readiness, corruption risk assessment, corporate governance, audit quality, and public governance indicators to build a practical view of human-centered digital governance.

2. METHODS

This study adopts a conceptual dataset-based review. No new questionnaire was distributed, and the datasets were not reprocessed statistically. The data articles were read as published evidence of concepts, indicators, and measurement choices that are relevant to accountability in digital public administration.

The conceptual synthesis draws upon ten Data in Brief datasets representing different public sector contexts and observation periods. The reviewed datasets comprise both longitudinal and crosssectional datasets. The longitudinal dataset covers governance indicators from 2012 to 2022, while the remaining datasets consist of cross-sectional surveys on digital readiness, public sector accounting readiness, corporate governance, corruption risk assessment, audit reporting, and tax compliance conducted in different years. Considering the temporal coverage of the datasets strengthens the conceptual synthesis by integrating both long-term governance trends and recent developments in digital public administration.

The reviewed articles were arranged into three broad groups. The first group concerns digital readiness and e-government, including attitudes toward digital technology, e-government tasks, government accountants' readiness to implement IPSAS, and StatMetaQA. The second group concerns internal control and governance, including corporate governance practices, governance index construction, audit reporting standards, and Worldwide Governance Indicators. The third group concerns accountability risks, particularly corruption risk assessment, administrative corruption, and tax evasion.

The review was carried out in a practical sequence. Each article was examined for its topic, constructs, data source, and relevance to the framework. The constructs were then sorted into broader categories. Those categories were compared and connected to explain how digital readiness and internal control may support each other. Since the article is conceptual, the output is presented as propositions rather than statistical hypotheses.

The use of dataset articles also sets the boundary of the study. The selected datasets are not treated as a complete representation of all public sector settings. They are used to show how digital readiness, governance, control mechanisms, and corruption risk have been measured in different contexts. This matters because the aim is framework development, not generalization from one pooled dataset.

Table 1. Dataset articles synthesized in the review

Source	Dataset focus	Role in this paper
Kaiser & Gadár (2023)	Attitudes toward digital technologies and egovernment tasks	Shows digital readiness through literacy, internet use, device use, and acceptance of digital public services.
Alghizzawi (2025)	Readiness of government accountants to implement IPSAS	Shows the role of human resources and information technology in public sector accounting readiness.
Rachmawati & Yulianti (2024)	Indonesian statistical metadata question-answering dataset	Supports the idea that public data must be organized and accessible for data-informed administration.
Arslan & Alqatan (2020)	Governance practices, barriers, and drivers in organizations	Offers a governance lens for reading practices, barriers, and institutional drivers.
Mansour et al. (2020)	Corporate governance index in Jordanian firms	Shows how governance attributes can be organized to assess transparency and control.
Gooden & Mellon (2025)	Audit reporting standards in experimental markets	Links reporting behavior with disclosure, signoff, and accountability mechanisms.
Vasconcelos & Cavique (2022)	Corruption risk assessment in public administration	Illustrates data integration for identifying corruption risk signals.
Al-Jundi (2019)	Determinants of administrative corruption	Shows that corruption risk is related to culture, institutions, and organizational conditions.

Source	Dataset focus	Role in this paper
Al-Jundi & Augustine (2026)	Key drivers of tax evasion	Connects non-compliance with deviant culture, weak enforcement, and administrative corruption.
Handoyo (2023)	Worldwide Governance Indicators 2012-2022	Frames accountability within broader governance quality, rule of law, and control of corruption.

3. RESULTS AND DISCUSSIONS

3.1 Digital Readiness in Public Governance

In this paper, digital readiness is understood as the practical ability of individuals and institutions to adopt digital systems, use them appropriately, interpret the information produced by those systems, and respond to risks shown by the data. The concept is broader than software, internet access, or infrastructure. It also includes competence, data literacy, acceptance of technology, and organizational support.

Kaiser and Gadár (2023) describe e-government readiness through digital literacy, smart device use, purposes of internet use, fear of smart systems, and attitudes toward digital development. The indicators suggest that e-government works better when public services fit the capability and acceptance of users. If people do not trust, understand, or feel able to use digital services, the system may be available but still underused.

Alghizzawi (2025) offers a related picture from public sector accounting. The dataset on government accountants' readiness to implement IPSAS links readiness with human resources and information technology. Readiness is therefore not merely an IT matter. It is a combined condition involving capability, organizational support, and infrastructure for reform.

Rachmawati and Yulianti (2024) add another angle through StatMetaQA, a closed-domain questionanswering dataset for Indonesian statistical metadata. The dataset shows that public data can be organized as a digital knowledge base. This supports the argument that public sector digital readiness also includes the ability to organize, access, and use public data for decision-making.

Across these datasets, digital readiness appears as a socio-technical capacity. Public actors need competence to operate systems, data literacy to interpret information, acceptance to use digital tools consistently, and institutional support so that digital governance practices do not stop at the pilot stage.

The practical message is clear. Before expecting a digital platform to improve accountability, public organizations need to know whether their users are ready. A dashboard, database, or online reporting platform has limited value when users cannot read

what it shows or question the quality of the data. Readiness therefore includes technical training, but it also includes judgment, administrative understanding, and the ability to communicate results to decision makers.

3.2 Internal Control and Governance

Internal control refers to formal routines that keep organizational processes authorized, documented, monitored, compliant, and accountable. In public organizations, these routines help reduce opportunities for misuse of authority, reporting errors, and governance failure.

Arslan and Alqatan (2020) show that corporate governance practices can be studied through surveys that identify practices, barriers, and drivers. Although their dataset comes from the corporate sector, its logic is relevant for public accountability because it shows the usefulness of mapping governance practices and obstacles systematically.

Mansour et al. (2020) provide a structured measurement approach through a corporate governance index. Their dataset groups governance attributes into disclosure and transparency, board effectiveness and composition, and shareholders' rights. In public sector internal control, a similar logic can be used by emphasizing transparency, documentation, monitoring, and procedural compliance.

Gooden and Mellon (2025) show that audit reporting standards and accountability mechanisms can influence reporting behavior. Their experimental market dataset examines disclosure and sign-off requirements in relation to auditor misreporting. For internal control, this means that visibility, authorization, and formal responsibility can affect how individuals report, decide, and take responsibility.

For that reason, internal control remains central in digital governance. It keeps digital processes traceable, authorized, and accountable, not only efficient. Without such control, digitalization can make administration faster while leaving old accountability problems largely unchanged.

In digital environments, control must also follow the information trail. Authorization may be built into access rights, documentation may appear in electronic logs, and monitoring may rely on system alerts or periodic review. The basic logic is familiar, but its operation depends more heavily on system design and user behavior.

Table 2. Conceptual mapping of the proposed framework

Element	Main meaning	Accountability relevance
Digital readiness	Capacity to use systems, interpret data, accept technology, and maintain organizational support.	Helps institutions access information, identify risk signals, and make decisions informed by data.

Internal control	Authorization, documentation, segregation of duties, monitoring, and compliance routines.	Keeps decisions and transactions reviewable, traceable, and formally accountable.
Human-centered digital governance	A socio-technical arrangement that combines people, technology, routines, and safeguards.	Prevents digital reform from becoming merely technical and connects digital use with responsible action.
Public sector accountability	Transparency, responsibility, traceability, compliance, and risk responsiveness.	Represents the expected outcome of combining digital capacity with control discipline.
Corruption risk awareness	Ability to identify and respond to noncompliance, misuse of authority, and weak enforcement.	Links digital information with followup actions and institutional integrity.

3.3 Corruption Risk and Public Accountability

The corruption-related datasets in this review are useful because they do not reduce corruption to a single procedural mistake. They bring the discussion closer to everyday institutional behavior: how rules are followed, how authority is exercised, and how weak enforcement leaves space for noncompliance.

Al-Jundi (2019), for example, links administrative corruption with culture, organizational culture, political instability, institutional weakness, and social class. Vasconcelos and Cavique (2022) use a

more data-oriented route by combining government databases to detect corruption risk signals. AlJundi and Augustine (2026) add evidence from tax evasion, where deviant culture, weak law enforcement, and administrative corruption appear together.

For this paper, the lesson is practical. Digital capacity can help public institutions notice risk earlier, especially when data from different units are connected. After that, control routines are needed to check the information, assign follow-up, and record what has been done. Without this stage, a risk indicator remains only a signal on a screen or in a report.

Accountability cannot rest only on access to digital information. Information must lead to responsibility. A risk score, transaction record, or warning sign becomes meaningful when the organization knows who must respond, what evidence should be reviewed, and how the follow-up should be documented. Digital readiness helps the institution see the signal; internal control helps it decide the next step.

3.4 Governance Indicators and Public Accountability

Public accountability also belongs to the wider quality of governance. Handoyo (2023), through the Worldwide Governance Indicators dataset, includes voice and accountability, government effectiveness, regulatory quality, rule of law, and control of corruption. These indicators show that accountability is not limited to reporting. It is also related to whether institutions work effectively, follow rules, and limit the misuse of public authority.

In this study, digital readiness and internal control are therefore treated as conditions that support better governance. Digital systems can provide access to information and create transaction records. Internal control adds responsibility, review, and compliance. Together, they help public organizations respond to risk while keeping administrative discipline.

The connection with governance indicators also prevents the framework from becoming too narrow. The purpose is not simply faster digital administration. The purpose is public action that can be explained, reviewed, and protected from misuse. In this sense, the framework links routine administrative work with broader governance outcomes.

3.5 Proposed Conceptual Framework

The framework starts from a practical observation: public organizations need both digital capacity and control discipline. Digital readiness enables users to work with systems and data. Internal control keeps transactions, decisions, and administrative actions authorized, documented, and open to review.

Figure 1. Conceptual Framework of the Study

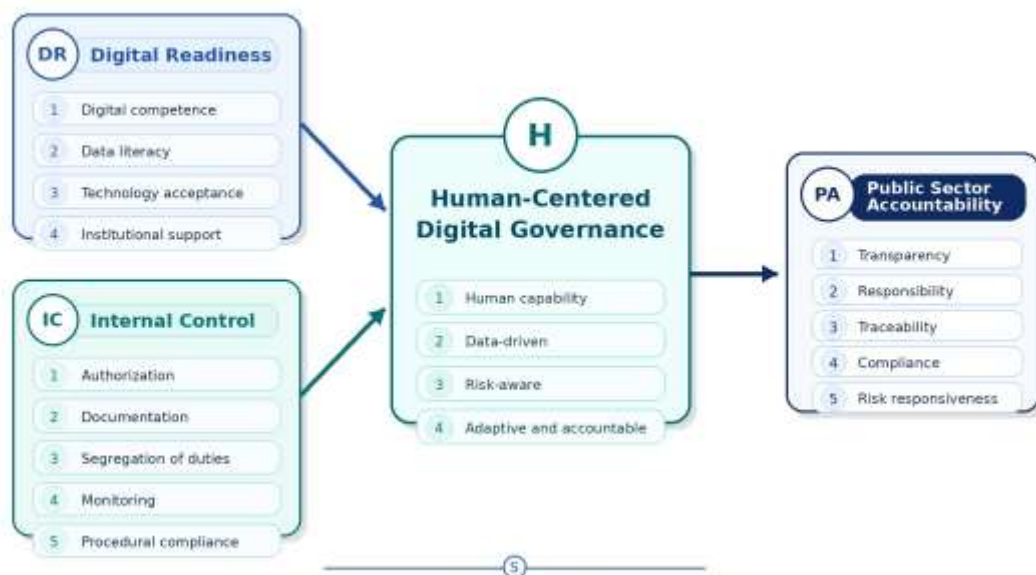


Figure 1 shows digital readiness and internal control as two inputs that meet in human-centered digital governance. This placement is deliberate. Technology contributes to

accountability when people can use it and when the organization places safeguards around its use.

An organization with advanced digital tools but weak control may complete tasks faster while responsibility remains unclear. An organization with strict control but low digital readiness may remain compliant but slow in responding to new risks. The framework brings the two sides together: readiness provides capacity, while control provides discipline.

3.5.1 Human-Centered Digital Governance

Human-centered digital governance starts from a simple premise: technology does not govern by itself. A platform may store files, record transactions, or produce dashboards, but people still decide what the information means and what action should follow. Accountability therefore depends on users who are capable, institutions that are prepared, and control routines that guide the use of digital information.

In practice, digital reform should not be treated only as a software project. It should also ask whether users understand the purpose of the system, whether the data are reliable, and whether control routines are present in daily work. These elements make digital governance a socio-technical arrangement rather than a purely technical reform.

3.5.2 Interaction between Digital Readiness and Internal Control

Digital readiness and internal control reinforce each other in daily administration. Readiness helps an organization gather and process information. Control asks whether that information is authorized, documented, and used for the right purpose.

The balance matters. Readiness without control can create speed without assurance. Control without readiness can preserve compliance but slow the response to new risks. A balanced arrangement allows public organizations to pursue efficiency while keeping responsibility visible.

3.5.3 Expected Accountability Outcomes

Several accountability outcomes may follow from this arrangement. Transparency improves when reliable information can be stored and shared on time. Traceability improves when decisions and transactions leave records that can be reviewed. Compliance becomes easier to maintain when procedures are embedded in digital routines and checked through internal control.

The broader outcome is public trust. Citizens tend to trust public institutions more when information is accessible, decisions can be explained, and control systems work in practice. In that sense, accountability is not only a reporting obligation. It is an organizational capability that supports legitimacy and governance performance.

3.6 Proposition Development

Proposition 1: Digital readiness strengthens public sector accountability when public actors can operate digital systems, interpret data, and respond to institutional risks. This proposition is grounded in the e-government dataset, which emphasizes digital literacy, user attitudes, and administrative habits as elements of readiness (Kaiser & Gadár, 2023).

Proposition 2: Internal control strengthens public sector accountability through authorization, documentation, segregation of duties, monitoring, and procedural compliance. This proposition is supported by governance and audit datasets that emphasize disclosure, transparency, formal responsibility, and accountability mechanisms (Gooden & Mellon, 2025; Mansour et al., 2020).

Proposition 3: Digital readiness and internal control, when developed together, produce stronger accountability than either dimension alone. The corruption risk assessment dataset supports this proposition because integrated data can help identify risk, while control mechanisms are still needed for monitoring and follow-up (Vasconcelos & Cavique, 2022).

Proposition 4: Human-centered digital governance is needed so that digital systems do not simply automate routines, but also support accountability. This proposition is consistent with datasets that stress human resources, user readiness, and technological support in public sector reform (Alghizzawi, 2025; Kaiser & Gadár, 2023).

3.7 Theoretical Implications

This framework contributes to public sector accountability literature by connecting issues that are often examined separately: digital readiness, internal control, governance quality, and corruption risk. The paper suggests that accountability becomes stronger when human capability, organizational readiness, and control routines operate together.

The framework also treats digital readiness as a governance capability, not only a technical condition. The reviewed datasets describe readiness through literacy, technology acceptance, infrastructure, and organizational support. This paper links those elements to the ability of institutions to turn digital information into responsible administrative action.

Internal control also needs to be understood in a digital setting. Its traditional functions remain important, but digital transformation adds issues such as data reliability, cybersecurity, automated processes, and electronic records. Internal control should therefore be seen as an adaptive governance capability, not merely as a compliance checklist.

Methodologically, the paper shows how dataset articles can support conceptual development. Rather than producing new empirical data, the study connects datasets from e-government, public sector accounting, corporate governance, corruption risk assessment, audit quality, and governance indicators. The resulting propositions can later be tested

through surveys, SEM-PLS, comparative case studies, or longitudinal public sector research.

3.8 Practical Implications

For public organizations, the framework offers a practical reminder. Investment in digital infrastructure should be accompanied by training that improves digital competence, data literacy, and technology acceptance among public officials.

Public managers also need to build control into digital systems from the start. Authorization, documentation, monitoring, segregation of duties, and compliance checks should not be added only after the system is running. They should be considered part of system design.

Auditors and inspectorates can use the framework when assessing digital transformation readiness. The assessment should not stop at technology. It should also ask whether the control environment is strong enough to support accountability and whether staff can use digital information responsibly.

For policy makers, the framework suggests that digital reform should be evaluated not only by the number of platforms created, but also by the way those platforms support accountability. The questions are practical: who can access the system, who approves the data, who reviews the records, and how quickly risks can be followed up.

The framework is also relevant for governments that seek stronger public trust. Innovation matters, but trust also depends on responsible behavior, clear risk management, and transparent decisionmaking. By linking digital readiness with internal control, public institutions can develop governance systems that are more transparent, responsive, compliant, and resilient.

Table 3. Propositions and possible empirical indicators

Proposition	Possible indicators	Possible method
P1: Digital readiness strengthens accountability	Digital competence, data literacy, technology acceptance, institutional support	Survey of public officials; SEM-PLS; descriptive readiness index
P2: Internal control strengthens accountability	Authorization, documentation, segregation of duties, monitoring, compliance	Survey, internal audit checklist, or document review
P3: Digital readiness and internal control are complementary	Interaction between readiness and control quality; risk followup routines	Moderation analysis or comparative case study

Proposition	Possible indicators	Possible method
P4: Human-centered digital governance supports accountability	User capability, responsible data use, traceability, and risk responsiveness	Mixed-method study combining survey and interviews

3.9 Future Empirical Testing

The framework is open to comparative study. Public organizations in different institutional settings may show different levels of digital capacity, control discipline, and corruption risk. A comparative design would help clarify which parts of the framework are general and which parts depend on context.

Future studies may examine whether the link between digital readiness and accountability becomes stronger when internal control is well embedded in the organization. This would allow researchers to test whether digital readiness works mainly as a direct driver of accountability, or whether its effect depends on the quality of control mechanisms surrounding the digital system.

The proposed framework can be developed further through empirical testing in public organizations that already use digital systems. A survey design could measure readiness through user competence, data literacy, technology acceptance, and institutional support. Internal control could be measured through authorization, documentation, segregation of duties, monitoring, and compliance routines.

4. CONCLUSION

This conceptual paper develops a human-centered framework linking digital readiness and internal control to public sector accountability. The synthesis of dataset articles on e-government, public sector accounting readiness, corruption risk assessment, corporate governance, audit quality, and governance indicators shows that accountability in the digital era depends on more than technology.

Digital readiness helps public organizations use technology, interpret data, and recognize risk. Internal control keeps public processes authorized, documented, monitored, and compliant. When both elements develop together, they support public digital governance that is more accountable and more responsive to risk.

The paper shifts attention from technology-driven digitalization toward human-centered accountability. Public sector reform should ask not only whether digital systems are available, but also whether people, institutions, and control mechanisms are ready to use those systems responsibly.

This study is conceptual and does not empirically validate the proposed framework. The reviewed datasets also come from different institutional and national settings. Future research can examine the propositions through survey-based data, structural equation modeling, or comparative case studies across public sector organizations.

Although the framework is conceptual, it can help public organizations evaluate their digital governance capacity. The model encourages managers to see digital systems and internal control as one connected governance problem. A modern platform still needs competent users, reliable data, and clear control routines before it can support accountability.

The same logic applies to public sector reform more broadly. Digital transformation should not be judged only by the number of applications, dashboards, or online services introduced. It should also be judged by whether those systems help public officials explain decisions, document actions, identify risks, and respond to problems in a timely manner.

For future empirical work, the framework can be operationalized by developing survey indicators for digital readiness, internal control, and public accountability. Researchers may also test whether internal control strengthens the effect of digital readiness on accountability, or whether different institutional contexts produce different patterns. Such studies would help refine the framework and make it more useful for public sector policy and practice.

5. REFERENCES

- Alghizzawi, M. A. (2025). Dataset on the questionnaire-based survey of the readiness of government accountants to implement international public sector accounting standards (IPSAS). *Data in Brief*, 59, 111302. <https://doi.org/10.1016/j.dib.2025.111302>
- Al-Jundi, S. A. (2019). A survey dataset on determinants of administrative corruption. *Data in Brief*, 27, 104820. <https://doi.org/10.1016/j.dib.2019.104820>
- Al-Jundi, S. A., & Augustine, R. (2026). Survey dataset on key drivers of tax evasion. *Data in Brief*, 66, 112755. <https://doi.org/10.1016/j.dib.2026.112755>
- Arslan, M., & Alqatan, A. (2020). Corporate governance practices, barriers and drivers: A survey dataset. *Data in Brief*, 33, 106603. <https://doi.org/10.1016/j.dib.2020.106603>
- Gooden, E., & Mellon, M. (2025). Audit reporting standards data from experimental markets. *Data in Brief*, 60, 111602. <https://doi.org/10.1016/j.dib.2025.111602>
- Handoyo, S. (2023). Worldwide governance indicators: Cross country data set 2012-2022. *Data in Brief*, 51, 109814. <https://doi.org/10.1016/j.dib.2023.109814>
- Kaiser, T., & Gadár, L. (2023). Survey data on the attitudes towards digital technologies and the way of managing e-governmental tasks. *Data in Brief*, 46, 108871. <https://doi.org/10.1016/j.dib.2022.108871>

Mansour, M., Hashim, H. A., & Salleh, Z. (2020). Datasets for corporate governance index of

Jordanian non-financial sector firms. *Data in Brief*, 30, 105603.

<https://doi.org/10.1016/j.dib.2020.105603>

Rachmawati, N., & Yulianti, E. (2024). StatMetaQA: A dataset for closed domain question answering in Indonesian statistical metadata. *Data in Brief*, 57, 110816.

<https://doi.org/10.1016/j.dib.2024.110816>

Vasconcelos, M. O., & Cavique, L. (2022). Dataset for corruption risk assessment in a public administration. *Data in Brief*, 40, 107768.

<https://doi.org/10.1016/j.dib.2021.107768>