

Digital Transformation in Public and Private Organizations

Muhammad Islam¹

Fazeel Hayder Chohan²

¹ Civil Judge cum Judicial Magistrate (Lahore High Court, Lahore), Pakistan. E-Mail: sislam786@gmail.com

ORCID <https://orcid.org/0009-0003-6142-7070>

² Lecturer, NUST, Islamabad. E-Mail: fazeelhyder@gmail.com

ABSTRACT

This article reviews digital transformation in public and private organizations and asks what makes transformation different from simply introducing new digital tools. The discussion begins with the distinction between digitization, digitalization, and digital transformation because these terms are often used as if they mean the same thing. The article then considers organizational change, leadership, employee skills, technology adoption, cybersecurity, data governance, resistance, and innovation. It compares public and private organizations while recognizing that they are not measured or constrained in exactly the same way. The review also uses recent OECD and World Bank indicators to illustrate public-sector trends. These indicators are treated as evidence about institutional foundations, not as a complete measure of whether people actually experience better services. Digital transformation is broader than converting paper into digital information or placing an existing service online. The literature reviewed here supports a view of transformation as organizational change in which digital technologies alter processes, structures, capabilities, value creation, or relationships. The main argument is that technology is only one part of transformation. Meaningful transformation also requires changes in structures, routines, skills, governance, and measures of success.

ARTICLE HISTORY

Received **01-10-2025**
Accepted **20-12-2025**
Published **30-12-2025**

KEYWORDS

digital transformation;; digitalization; digital government; organizational change; technology adoption; data governance; cybersecurity;

CORRESPONDING AUTHOR

Fazeel Hayder Chohan
fazeelhyder@gmail.com

 <https://doi.org/10.68740/jjss15>

CC BY-NC 4.0 © 2026 The Author(s). Published by JuriSocial Research Center Private Limited. This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International Licence (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

Introduction

Digital transformation is now a common term in both academic writing and organizational plans. The problem is that the term is sometimes used for almost every technology project. A new website, a scanned archive, or an online form may be useful, but none of these automatically changes how an organization works. This makes the meaning of digital transformation an important starting point for research. Vial (2019), in a review of 282 studies, describes digital transformation as a process in which digital technologies create disruptions, organizations respond to them, and value-creation paths change. This definition places organizational change at the centre rather than treating technology as the final outcome.

The issue looks different in private and public organizations. Private firms face customers, competitors, investors, and changing markets. Public organizations also face changing expectations, but they must continue to provide services, follow legal mandates, protect equality, and operate within public budgets. Mergel et al. (2019) show that public administrators associate digital transformation with changes in services, processes, relationships, efficiency, interoperability, transparency, and citizen satisfaction. These differences mean that the same technology can produce different organizational problems in the two sectors. A private company may decide to close an unsuccessful digital service, while a public body may have to maintain access because the service is part of a legal or social obligation.

The article is designed as a critical review rather than an original survey or statistical study. It brings together established academic reviews, public-administration research, technology-adoption literature, and recent official measurements. The purpose is not to claim a new theory of digital transformation. Instead, it is to connect the main management issues that repeatedly appear in the literature and to explain why they matter in both public and private settings. Hanelt et al. (2021) show that the literature is broad and fragmented, while Wiener et al. (2025) more recently argue that digital transformation should be understood through interacting processes rather than as a single event. These studies provide a useful basis for the present review.

Three questions guide the discussion. First, how should digital transformation be distinguished from digitization and digitalization? Second, which organizational and management conditions most strongly affect the implementation of digital transformation in public and private organizations? Third, what can current international evidence tell us about the progress and limits of public-sector digital transformation? The article argues that the answers are connected: transformation becomes meaningful when technology is accompanied by changes in organizational routines, capabilities, governance, and service or business models.

The method is a structured critical review of selected academic and institutional sources. The core academic sources were chosen because they provide established definitions, review the wider literature, or examine organizational adoption and public-sector transformation. Official OECD and World Bank reports were used for current public-sector indicators, while NIST was used for cybersecurity governance. Sources were compared by theme rather than combined into a statistical meta-analysis. This approach has limits: it cannot establish causal effects across organizations, and the public-sector indices cannot be treated as measures of private-sector transformation. Those limits are kept visible throughout the article.

Meaning and Dimensions of Digital Transformation

There is no single definition of digital transformation that is accepted across all disciplines. Vial (2019) defines it as a process aimed at improving an entity through significant changes produced by combinations of information, computing, communication, and connectivity technologies. The important point is the scale of the organizational change. A project may introduce a useful digital tool without changing the basic way an organization creates value or delivers services. Hanelt et al. (2021) similarly

show that digital transformation is closely connected with organizational change, continuous adaptation, and wider digital ecosystems.

Vial (2019) also organizes the literature around several connected elements, including technologies, disruption, strategic responses, changes in value creation, structural change, organizational barriers, and outcomes. This framework is useful because it prevents digital transformation from becoming a list of fashionable technologies. Cloud computing, mobile platforms, analytics, the Internet of Things, and artificial intelligence may enable change, but the technology itself does not determine the organizational result. Wiener et al. (2025) develop this point further by treating digital transformation as a network of related processes and by identifying gaps in research on how those processes unfold over time.

Public-sector research adds another perspective. Mergel et al. (2019), based on expert interviews, found that public administrators commonly described digital transformation in terms of improving processes, services, relationships, efficiency, interoperability, transparency, and citizen satisfaction. This is important because public transformation is not simply a public version of private-sector disruption. The purpose of a government service includes public value, legal responsibility, continuity, and equal access. A transformation project therefore has to be assessed not only by whether it is technically successful, but also by whether it improves the service without creating new barriers.

Across both sectors, several dimensions appear repeatedly: strategy, technology, organizational structure, people, data, and relationships with external actors. OECD digital-government work treats governance, data, digital public infrastructure, and human-centred services as important foundations of public-sector transformation (OECD, 2024, 2026). The World Bank's GovTech Maturity Index similarly measures core government systems, online service delivery, digital citizen engagement, and enabling conditions such as strategy, institutions, laws, skills, and innovation policy (Vasconcelos et al., 2025). Private organizations add stronger emphasis on business models, competition, pricing, customer relationships, and investment. The common lesson is that technology needs organizational capacity around it.

Digital Transformation Versus Simple Digitization

Verhoef et al. (2021) distinguish three related stages. Digitization means converting analogue information into digital form. Digitalization means using digital technologies to change existing processes. Digital transformation goes further by changing the organization more broadly, including its business model, value creation, structures, or relationships. These distinctions are useful because they prevent every successful software installation from being described as transformation. A library that scans old records is digitizing. A library that lets users search, reserve, pay, and receive material through one integrated service is digitalizing its process. A library that develops a wider digital learning platform and changes how it delivers its services is closer to transformation.

Mergel et al. (2019) make a related point in the public sector. Putting a government form online does not necessarily change the underlying service. If citizens still have to print the form, sign it, and submit the same information again, the organization may have changed the format without changing the process. The distinction matters because organizational performance can be overstated when digital availability is treated as evidence of transformation.

A practical test is therefore useful. If the main result is a digital version of an existing activity, it is better described as digitization. If the process itself becomes different, the term digitalization is more appropriate. If the change affects organizational structures, value creation, service relationships, or the wider operating model, the stronger term digital transformation is justified. Not every project has to reach the last stage. The important point is to describe the stage honestly (Verhoef et al., 2021).

Organizational Change

Digital transformation is ultimately an organizational-change problem supported by technology. Digital services often cross departmental boundaries, while older organizations are usually arranged around separate functions. A citizen journey may involve identity, payment, records, complaints, and service delivery even though those activities belong to different units. Vial (2019) identifies structural change and organizational barriers as central parts of transformation, not as minor implementation issues.

Change is difficult for practical reasons. Legacy systems are often connected to legal requirements, accounting procedures, contracts, and staff routines. Employees have learned how to complete the old process and managers may be evaluated through measures designed for that process. In private firms, competitive pressure can make the cost of staying with the old model obvious. In public organizations, the pressure to change is mixed with legal duties, political priorities, budget limits, and the need for continuity. Mergel et al. (2019) also show that changing expectations among citizens can push governments to redesign services.

One important management choice is whether digital work remains mainly within an information-technology department or becomes a whole-organization responsibility. OECD research treats governance arrangements and coordination as part of the foundation of digital government (OECD, 2024, 2026). A digital unit that has advice but no authority over budgets or service design may produce good strategies that are difficult to implement. At the same time, concentrating every decision in one technical unit can create solutions that do not fit the legal or operational realities of frontline work.

The literature does not support the claim that one change model, such as top-down management, agile methods, or co-design, always produces the best result. What is more consistent is the need to change incentives, routines, responsibilities, and performance measures along with the technology (Hanelt et al., 2021; Vial, 2019). Otherwise, employees may simply place the new system on top of the old process. The organization becomes more digital in appearance without becoming substantially different in practice.

The difference between the technology timetable and the institutional timetable is also important. Technology products may change within months, while budgets, procurement arrangements, labour agreements, legal rules, and organizational responsibilities can take years to change. The COVID-19 period showed that institutions can move quickly when the pressure is exceptional, but emergency digital channels do not always become permanent reforms. Sustainable transformation requires the underlying rules, staffing, and responsibilities to be adjusted as well.

For this reason, organizational-change planning should include questions that are easy to overlook: Which roles will change? Which new skills and positions will be funded? Which old systems can actually be retired? Who has authority to stop duplicate projects? Which performance measures should be replaced? These questions may sound administrative, but they often determine whether a digital programme produces lasting organizational change.

Leadership

Leadership is frequently mentioned in digital-transformation research, but it is more useful to identify the decisions leaders actually have to make. Someone with sufficient authority must decide which processes will be changed, which data can be shared, which risks are acceptable, and which old channels can eventually be closed. These are organizational decisions, not simply technical decisions.

In private firms, leadership is often discussed in relation to strategy and competitive disruption (Vial, 2019; Verhoef et al., 2021). Managers may need to decide whether to improve the existing model, develop a platform, or create a new digital service. In public organizations, leadership is more strongly

connected with coordination and mandate because several ministries or agencies may have to work together without sharing a common profit-and-loss structure. OECD research therefore treats digital governance and institutional coordination as important parts of transformation capacity (OECD, 2024, 2026).

It is not necessary to treat digital leadership as a completely separate leadership theory. A more cautious interpretation is that digital projects expose familiar leadership problems in a new setting. Managers may fail to close an outdated channel, delay investment in data quality, or change priorities before a multi-year programme is completed. These are ordinary management problems, but digital transformation makes their effects more visible.

Leadership also involves communication between technical and non-technical groups. Technology teams may discuss systems, releases, and architecture, while senior managers focus on outcomes, costs, dates, and public or customer experience. Someone has to connect these perspectives. If a system is technically live but users still have to complete several unnecessary steps, a launch date alone does not show that transformation has succeeded.

Continuity is another part of leadership. Digital platforms often remain in use after the original project team has left. A programme therefore needs stable responsibilities, funding, governance rules, and institutional ownership. The broader OECD evidence on digital-government governance supports this point: institutional arrangements matter because digital transformation is not completed when a particular project manager leaves (OECD, 2026).

Employee Skills

Skills are important at several levels. Organizations need technical specialists to build and secure systems, but they also need people who understand the substantive work being changed. The World Bank includes digital skills among the enabling conditions in its GovTech framework, while Verhoef et al. (2021) emphasize organizational capabilities rather than software alone. Transformation therefore depends on the ability to use technology in real work, not simply on the number of licences purchased.

Training is a necessary response, but training by itself does not solve poor system design. If a new system makes a simple task harder, employees may learn to use it while continuing to rely on spreadsheets, email, or other informal workarounds. Skills policy should therefore be linked to job design and process redesign. Employees need to understand not only how to operate the system but also why the new process is better and what responsibility they have within it.

There is also an internal distribution issue. A small digital team may become a bottleneck, while frontline staff may feel that transformation is something being imposed on them. Mergel et al. (2019) place considerable attention on service relationships and the experiences of public administrators. A digital system will work differently depending on whether the people who use it every day have enough support, authority, and confidence to solve problems.

A practical skills strategy can be viewed at three levels. Specialists need the technical capacity to operate platforms and manage security. Managers need enough digital understanding to interpret performance information, risks, and vendor proposals. Frontline employees need to perform routine tasks and know when a case should be escalated. This broader approach is consistent with the emphasis that OECD and World Bank assessments place on digital skills as an institutional enabler (OECD, 2026; Vasconcelos et al., 2025).

Private organizations face a similar division between specialist digital teams and the wider workforce. Verhoef et al. (2021) argue that organizational structures and performance measures have to change with the digital business model. If employees are still rewarded only for the old sales channel, they have little reason to support the new one. In this sense, skills and incentives are connected rather than separate management issues.

Technology Adoption

Technology adoption research predates the current language of digital transformation. Venkatesh et al. (2003), through the Unified Theory of Acceptance and Use of Technology (UTAUT), brought together several earlier approaches and identified performance expectancy, effort expectancy, social influence, and facilitating conditions as important factors in technology use. These ideas remain useful because a system that is difficult to use or poorly supported may be rejected even when senior management considers it strategically important.

Rogers (2003) offers another useful perspective through diffusion of innovations. Relative advantage, compatibility, complexity, trialability, and observability can affect how an innovation spreads. Digital projects often encounter problems on exactly these points. A new process may not fit existing legal forms, may be difficult to test before full deployment, or may appear beneficial to senior management while creating extra work for the employee who has to use it.

Organizational adoption should also be separated from actual use. A ministry may formally adopt a system while local offices continue to use paper. A company may purchase analytics software while managers continue to make decisions mainly from experience. Transformation should therefore be evaluated through actual use, service outcomes, and changes in work practices rather than procurement alone (Venkatesh et al., 2003).

Cybersecurity

Greater digital dependence also creates greater cybersecurity exposure. This is not simply a technical problem because the success of a digital service depends on whether users and managers trust the system. NIST's Cybersecurity Framework 2.0 provides a common framework for organizations to identify, protect against, detect, respond to, and recover from cybersecurity risks, while adding a specific Govern function (NIST, 2024). This reinforces the idea that cybersecurity belongs within organizational governance rather than being treated as a final technical check.

Public and private organizations face different threat environments, but some risks overlap, including ransomware, identity theft, supply-chain compromise, and misuse by insiders. As more services and partners connect to common platforms, a single weakness can affect several processes. Digital integration can therefore improve efficiency while also concentrating risk. This trade-off needs to be considered during system design rather than only after an incident.

A common management weakness is to treat security as something that will be added after the main service is launched. NIST's CSF 2.0 is useful precisely because it places governance alongside the other cybersecurity functions. Leaders need to decide who owns risk, how suppliers will be managed, how incidents will be communicated, and what level of disruption the organization can tolerate (NIST, 2024).

Data Governance

Data is one of the basic infrastructures of digital transformation. A service may look simple to a user, but behind it there are questions about which organization owns a record, who may access it, how long it should be retained, and whether different systems can use the same information. OECD digital-government work treats data governance and digital public infrastructure as foundations for wider transformation (OECD, 2024, 2026).

Public and private organizations approach data from somewhat different starting points. Private firms may focus on customer relationships, analytics, commercial value, and liability. Public organizations must also consider legal authority, equality, public interest, transparency, and the risk of excessive surveillance. Both sectors need basic controls for data quality, definitions, access, retention,

and accountability. Without these controls, digital dashboards can create an appearance of precision without reliable underlying information.

Artificial intelligence makes these issues more important because automated systems depend on the quality and structure of their data. The 2025 World Bank GovTech update includes indicators related to ethical AI use and other emerging dimensions of digital government (Vasconcelos et al., 2025). This does not mean that the existence of an indicator solves the underlying problem. It shows instead that data governance and responsible technology use are becoming part of the broader institutional capacity needed for digital transformation.

Organizational Resistance

Resistance is often described as a negative attitude, but the reasons for resistance can be more practical. Employees may not see a clear advantage, may find the new system difficult to use, may worry about monitoring, or may believe that the change threatens their role. Rogers (2003) and Venkatesh et al. (2003) provide different theoretical explanations for these problems, while Vial (2019) places organizational barriers within the transformation process itself.

Resistance can also contain useful information. A frontline employee may object to a new process because it does not work for unusual cases that occur regularly in practice. If managers treat every objection as opposition to change, they may lose valuable knowledge about the service. The better approach is to ask whether the resistance reflects fear of loss, poor design, inadequate support, or a genuine problem with the proposed process.

Resistance can come from several parts of an organization. Middle managers may protect existing responsibilities, professional groups may be concerned about quality, and senior managers may continue funding parallel projects. These forms of resistance are not identical and should not be treated as a single cultural problem. The literature on digital transformation suggests that organizational barriers influence outcomes together with technology and strategy (Hanelt et al., 2021; Vial, 2019).

There is also a risk that organizations respond to resistance with training workshops without changing the underlying work. Employees may be asked to become more flexible even though the new process still requires duplicate information or unnecessary approvals. In such cases, resistance may be evidence that the redesign is incomplete. Adoption is more likely when the new process actually improves the work and when employees can see a reason to change.

Public consultation adds another dimension. Citizens who object to a digital-only service may be concerned about exclusion rather than resistant to technology. Private customers who stop using an application may be responding to a poor service journey rather than to a general fear of digital tools. Transformation programmes therefore need to distinguish between resistance to change and legitimate criticism of the proposed change.

Innovation

Innovation is both a reason for transformation and a possible result of it. Verhoef et al. (2021) place business-model innovation at the centre of the private-sector discussion. Digital technologies can make it possible to combine services, data, and channels in ways that were previously difficult. In public organizations, innovation is more closely tied to service improvement, such as reducing repeated requests for information, improving access, or coordinating services across agencies (Mergel et al., 2019).

The World Bank's 2025 GovTech findings include innovation policy among the enabling dimensions of public-sector digital maturity, while also showing that progress is uneven (Vasconcelos et al., 2025). This is a useful distinction. Having an innovation strategy is not the same as giving

organizations permission and resources to test a service, learn from failure, and scale successful experiments. Public organizations often face stronger reputational and accountability pressures than private firms, so innovation needs an appropriate risk-management approach.

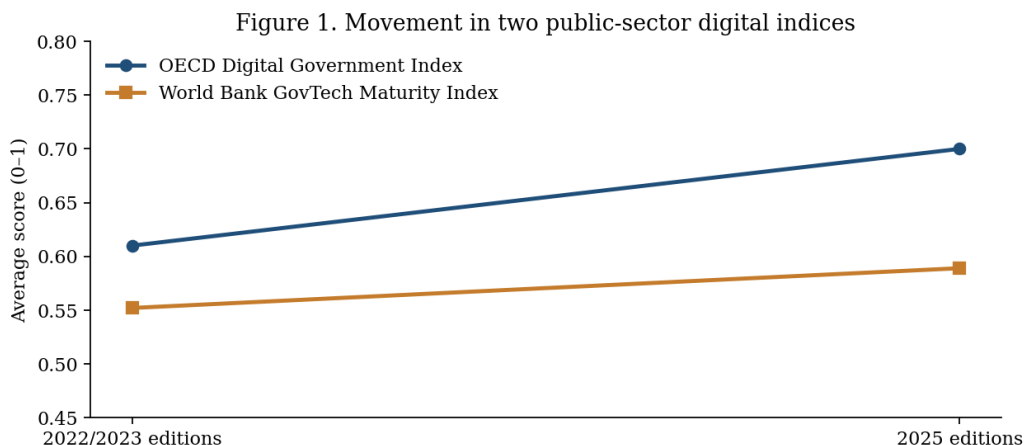
A more realistic approach is to connect innovation with controlled experimentation. Digital tools may reduce the cost of testing some service ideas, but failure can be more serious when an experiment involves sensitive data or essential public services. Sandboxes, phased pilots, flexible procurement, and clear evaluation criteria can help organizations learn without treating every experiment as a full-scale commitment.

Public Versus Private Sector Experiences

The same technologies can be used in both sectors, but the institutional setting is different. Private organizations are usually more directly disciplined by customers, competitors, investors, and financial performance. Public organizations must also account for law, political accountability, equality, continuity, and public trust. A failed login at a bank may be a customer-service problem; a failed login to a benefits system can prevent someone from accessing an essential service.

Mergel et al. (2019) show that changing private-sector digital services can raise citizens' expectations of government. Governments may therefore feel pressure to provide services that are as convenient as those offered by private firms. Verhoef et al. (2021), in contrast, focus on disruption, business models, and value creation in firms. The two literatures overlap on leadership, skills, structures, and capabilities, but the consequences of failure and the possibility of exit are different.

Measurement also differs. The OECD's 2025 Digital Government Index reports an OECD average of 0.70, up from 0.61 in the 2023 edition (OECD, 2024, 2026). The World Bank's 2025 GovTech Maturity Index reports a global average of 0.589, compared with 0.552 in 2022 (Vasconcelos et al., 2025). These figures are useful for describing public-sector trends, but the indices use different methods and populations and should not be treated as directly comparable scores. There is also no single official global index that provides an equivalent measure of private-sector digital transformation.



Sources: OECD DGI average 0.61 (2023) and 0.70 (2025); World Bank GTMI global average 0.552 (2022) and 0.589 (2025). The two indices are not directly comparable with each other.

Figure 1. Published average scores for the OECD Digital Government Index and World Bank GovTech Maturity Index across their 2023/2022 and 2025 editions. Note. The indices use different methods and coverage and are shown for trend illustration, not as directly comparable measures.

Table 1 summarizes the main public-private differences discussed in the literature. It is a conceptual synthesis rather than an empirical dataset. The categories are intended to show typical differences, not absolute rules. Particular organizations can fall between the two columns, especially state-owned enterprises, regulated private firms, and public organizations that operate through commercial partnerships.

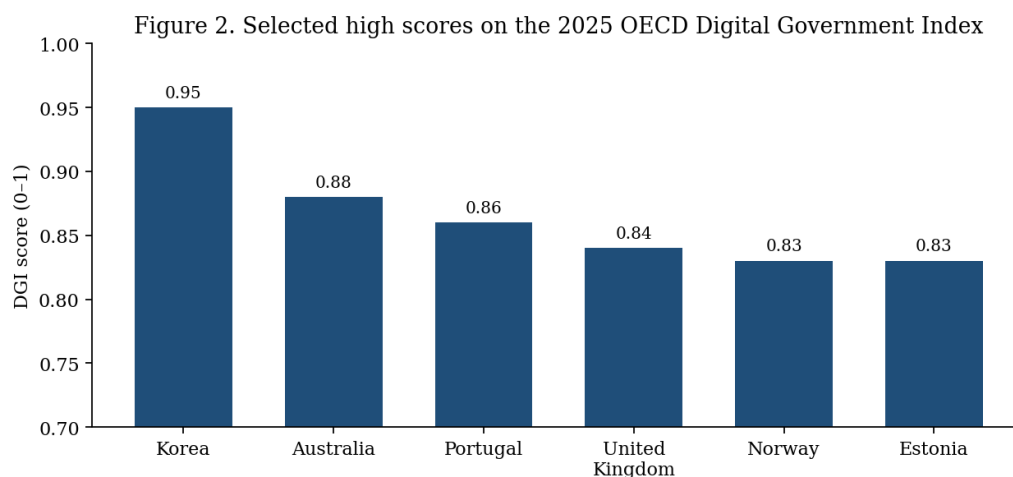
Table 1. Typical differences between digital transformation in public and private organizations (conceptual synthesis based on sources cited in the text).

Dimension	Public organizations	Private organizations
Primary purpose	Mandate, rights, service continuity, legitimacy.	Value creation, competition, customer retention.
What “transformation” often means	Joined-up services, once-only data, transparency, inclusion (Mergel et al., 2019; OECD, 2024).	Business-model and channel change, new digital offerings (Verhoef et al., 2021).
Exit option	Weak. Services usually cannot be abandoned.	Stronger. Products and channels can be retired.
Main constraints	Law, procurement, politics, equity, audit.	Capital, competition, brand risk, regulation in some sectors.
Data logic	Legal basis, purpose limitation, public-interest uses.	Customer insight, targeting, liability and trade secrets.
Leadership problem	Cross-government mandate and continuity.	Willingness to cannibalize old revenue.
Typical success metrics	Take-up, inclusion, time-to-service, trust, index scores.	Revenue, cost-to-serve, conversion, market share.
Failure mode	Digitized bureaucracy; exclusion of those offline.	Channel conflict; stranded legacy; security incident.

International Examples

International comparison is tempting and slightly dangerous. Index scores compress many things. They also help a review stay attached to published evidence instead of travel anecdotes.

The 2025 OECD Digital Government Index places Korea at 0.95, Australia at 0.88, Portugal at 0.86, the United Kingdom at 0.84, and Norway, Estonia, Ireland, and Denmark at 0.83 (OECD, 2026). These are composite scores for the enabling foundations of digital government, not direct measures of every citizen's experience. The OECD's 2025 assessment covers developments during 1 January 2023 to 31 December 2024, and the OECD average does not include Germany and the United States because 2025 data were not available for them.



Source: OECD (2026) reporting of the 2025 Digital Government Index. Korea 0.95; Australia 0.88; Portugal 0.86; United Kingdom 0.84; Norway and Estonia 0.83.

Figure 2. Selected high scores on the 2025 OECD Digital Government Index (OECD, 2026).

Estonia is often discussed in digital-government research because of its digital identity infrastructure and once-only approach to government data. Korea's high score is also important because it shows that strong digital-government capacity is not limited to small European states. The OECD results are best used as evidence of institutional foundations and policy capacity. They do not

establish that a country's digital services are equally accessible to every resident or that its broader political and administrative problems have disappeared (OECD, 2026).

Private-sector comparisons are more difficult because evidence is spread across company studies, industry surveys, and academic research rather than one global official index. This review therefore avoids using unverified corporate claims as international evidence. The more useful comparison is conceptual: in firms, transformation should be visible in business models, organizational capabilities, customer relationships, and performance measures, not simply in the introduction of an application (Verhoef et al., 2021).

Future Challenges

The first challenge is unequal organizational capacity. The World Bank's 2025 GTMI reports positive but uneven progress across 197 economies and a growing difference between the average scores of the more mature and less mature groups (Vasconcelos et al., 2025). This matters because international discussion can become too focused on countries with strong digital infrastructure while giving less attention to administrations that are still building basic systems, skills, and governance arrangements.

The second challenge is artificial intelligence. AI can improve service speed and decision support, but it can also scale errors and bias when it is used without appropriate controls. The inclusion of ethical-AI indicators in the 2025 GTMI shows that responsible use is becoming part of the public-sector digital agenda (Vasconcelos et al., 2025). Future research should therefore examine not only whether organizations adopt AI but also how they supervise it and how affected users can challenge harmful outcomes.

The third challenge is cybersecurity and third-party risk. More connected systems can create efficiency, but they can also concentrate the consequences of a security failure. NIST CSF 2.0 provides a governance-oriented framework for managing cybersecurity risk (NIST, 2024). The management challenge is to integrate security into the design and procurement stages rather than treating it as a final technical exercise.

The fourth challenge concerns legacy systems and procurement. Organizations often add new digital systems without being able to retire the old ones. This creates duplicate costs and can make employees maintain two processes at the same time. In public organizations, procurement arrangements may also make iterative service development difficult. More research is needed on how procurement, legal rules, and legacy infrastructure shape transformation over several years rather than only during the launch phase.

The fifth challenge is measurement. Official indices are useful because they provide comparable indicators, but they mainly capture institutional foundations. They do not fully show whether a person can actually complete a service easily. Private metrics can be closer to customer behaviour, but they may not capture exclusion or wider social effects. Future research should therefore combine institutional measures with evidence about actual use, accessibility, and outcomes.

The sixth challenge is human capacity. Skills, trust, workload, and fatigue influence whether new systems are actually used. The factors identified in UTAUT—performance expectations, effort, social influence, and facilitating conditions—remain relevant even when organizations use much newer technologies (Venkatesh et al., 2003). Transformation strategies should therefore consider the experience of ordinary users, not only the capability of specialist teams.

A seventh challenge is environmental and fiscal sustainability. Digital systems require devices, data centres, networks, and continuing vendor support. The 2025 GTMI includes green-technology policy among its newer indicators, showing that sustainability is becoming part of the digital-government discussion (Vasconcelos et al., 2025). The present review cannot quantify the environmental cost of

digital transformation, but it suggests that future research should examine these costs together with efficiency gains.

An eighth challenge is trust after failure. A serious data breach, unreliable automated decision, or long service outage can reduce confidence in a digital programme. Cybersecurity governance is therefore connected to institutional legitimacy, not only technical protection (NIST, 2024). Organizations need plans for explaining failures, correcting them, and restoring access when digital systems do not work.

A ninth challenge is dependence on major technology vendors. Both public and private organizations may rely on a small number of platform providers. This can improve technical capacity but may also increase switching costs and reduce organizational control. Existing digital-government indices capture many aspects of infrastructure and governance, but they do not fully describe vendor dependence. This is an area where management and public-policy research can add useful evidence.

Discussion

Taken together, the literature suggests that digital transformation is better understood as organizational change supported by digital technologies than as a technology upgrade. Vial (2019), Hanelt et al. (2021), and Wiener et al. (2025) all point, in different ways, to changes in structures, capabilities, processes, and organizational responses. The public-administration literature adds a strong focus on services, relationships, and institutional constraints (Mergel et al., 2019).

The management issues discussed in this article are closely connected. Weak leadership can leave old channels open. Weak skills can turn a new system into additional work. Weak adoption planning can produce formal implementation without actual use. Weak security and data governance can make integration risky. Resistance may then appear irrational even when it is pointing to a real design problem. Innovation is more likely to succeed when these basic conditions are addressed first.

The public-private comparison should remain cautious. Private organizations are not automatically more digitally transformed, and public organizations are not automatically behind. They operate under different objectives, constraints, and accountability systems. The available public indices show progress and uneven capacity, but they cannot be used to rank public and private organizations on one common scale (OECD, 2026; Vasconcelos et al., 2025).

The main research gap identified in this review is not another definition of digital transformation. The more useful gap concerns what happens after implementation. Existing reviews provide strong conceptual frameworks, while official indices provide broad measures of institutional capacity. There is less comparable evidence on how digital projects affect everyday work, service accessibility, employee experience, and long-term organizational change. Wiener et al. (2025) similarly identify the need for stronger process-oriented research and more attention to time and the interaction among transformation processes.

There is also a question of who is missing from successful transformation stories. High public-sector index scores tell us about policy and institutional foundations, but they say less about people with limited digital skills, unstable connectivity, disabilities, language barriers, or unusual administrative circumstances. The same concern applies inside private organizations to workers whose roles are changed by automation and to smaller suppliers that may struggle to meet the technical requirements of large platforms. These groups should be part of future research rather than being treated as secondary effects.

For private organizations, the parallel concern is whether transformation creates sustainable work and relationships as well as new revenue. Verhoef et al. (2021) emphasize business-model change and organizational capabilities, but those changes can also affect employees, suppliers, and customers. A

management-focused account should therefore examine not only whether a firm becomes more digital but also how the change is distributed across the people and organizations connected to it.

The review points to four practical directions for future research. First, studies should identify clearly whether they are examining digitization, digitalization, or transformation. Second, they should measure actual use and exclusion rather than only launch dates and procurement. Third, public and private cases should be compared using appropriate sector-specific measures. Fourth, security, data governance, skills, and organizational change should be studied as part of the transformation process rather than as separate technical issues.

Conclusion

Digital transformation is broader than converting paper into digital information or placing an existing service online. The literature reviewed here supports a view of transformation as organizational change in which digital technologies alter processes, structures, capabilities, value creation, or relationships (Vial, 2019; Hanelt et al., 2021; Verhoef et al., 2021). Public and private organizations use many of the same technologies, but their purposes, constraints, responsibilities, and measures of success are different.

The review also answers the second research question by showing that technology alone is not enough. Leadership, employee skills, actual technology adoption, cybersecurity, data governance, and the management of resistance all influence whether a digital project becomes lasting organizational change. The answer to the third question is more qualified. OECD and World Bank indicators show measurable progress in public-sector digital capacity, but they also show uneven development, and the indices do not measure every aspect of lived service experience (OECD, 2026; Vasconcelos et al., 2025).

The main contribution of this review is therefore a practical connection between issues that are often discussed separately. A transformation programme can have strong technology and still fail because the organization does not change its routines, skills, incentives, security arrangements, or data practices. The literature also suggests that the next stage of research should focus less on broad definitions and more on the process of implementation over time, including the experiences of users and employees.

Future studies could examine one public service and one private service in the same country and follow both over time. Such a design could test the digitization–digitalization–transformation distinction while also examining adoption, organizational change, inclusion, security, and outcomes. The present article is a review rather than an empirical study, so its purpose is to identify the concepts and management problems that such research should examine.

References

- Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>
- Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies*, 58(5), 1159–1197. <https://doi.org/10.1111/joms.12639>
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Organisation for Economic Co-operation and Development. (2024). 2023 OECD Digital Government Index: Results and key findings (OECD Public Governance Policy Papers No. 44). OECD Publishing. <https://doi.org/10.1787/1a89ed5e-en>

- Organisation for Economic Co-operation and Development. (2026). Digital Government Index and Open, Useful and Re-usable Data Index: 2025 results and key findings (OECD Working Papers on Public Governance No. 90). OECD Publishing. <https://doi.org/10.1787/6347ec74-en>
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- Vasconcelos, J. R., Dener, C., Nii-Aponsah, H., Blanco, C. V., Immonen, A. J., Nordlund, P., Siregar, F., & Song, Y. (2025). GovTech Maturity Index 2025: Tracking public sector digital transformation worldwide. World Bank Group.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. <https://doi.org/10.2307/30036540>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Wiener, M., Strahringer, S., & Kotlarsky, J. (2025). Where are the processes in IS research on digital transformation? A critical literature review and future research directions. *The Journal of Strategic Information Systems*, 34(2), 101900. <https://doi.org/10.1016/j.jsis.2025.101900>

Declarations

◆ Author Contributions	The author is responsible for the conception, literature review, analysis, drafting, revision, and final approval of this manuscript.
◆ Funding	No external funding was received for this research.
◆ Conflict of Interest	The author declares no conflict of interest relevant to this article.
◆ Data Availability Statement	This article is based on published academic and institutional sources. No original dataset was collected or generated for the study.
◆ Ethical Statement	Ethical approval was not required because the article does not involve human participants, interviews conducted by the author, or identifiable personal data.
◆ AI Use Disclosure	Generative AI tools were used during the preparation of the draft and/or for language assistance. The author remains responsible for the accuracy, verification, interpretation, citations, and final content of the manuscript.

Journal Policies *JuriSocial Journal of Social Sciences*

OPEN ACCESS & LICENCE

All articles are freely available on publication under CC BY-NC 4.0. Readers may share and adapt the work for non-commercial purposes with proper attribution.

PEER REVIEW

Every research article undergoes double-blind peer review by at least two independent reviewers.

PLAGIARISM POLICY

All submissions are screened with similarity-detection software; plagiarism in any form leads to rejection.

CORRECTIONS & RETRACTIONS

Errors are corrected through published corrigenda; retractions follow COPE guidelines.

PUBLICATION CHARGES

No article publishing fee charged.

COPYRIGHT

Authors retain copyright and grant JJSS the right of first publication.

PUBLICATION ETHICS

JJSS follows the Committee on Publication Ethics (COPE) Core Practices and guidelines.

GENERATIVE AI POLICY

AI tools cannot be listed as authors. Any substantive use must be disclosed; authors remain fully responsible for the content.

ARCHIVING & INDEXING

Content is preserved through [PKP Preservation Network / LOCKSS]. DOIs are registered with Crossref.

DISCLAIMER

The views expressed are those of the authors and do not necessarily reflect the views of the editors or the publisher.

Submissions & enquiries editor@jjss.jurisocial.org ◆ <https://socialsciences.jurisocial.org/>