HUMANIS
(Humanities, Management and Science Proceedings)

Vol. 6 • No. 1 • December 2025

Pege (Page) : 527 – 536

ISSN (*online*): 2746 - 4482
ISSN (*print*): 2746 - 2250

Master of Management Postgraduate Program
Jl. Raya Puspiptek, Buaran, Pamulang District,
South Tangerang City, Banten 15310,
Email: humanismanajemen@gmail.com

Special Issue:
ICMS 2025
Website. :
http://www.openjournal.unpam.ac.id/index.php/SNH

Facts and Trend of Digital Technology Infrastructure (Case: P.T. Mahdani Printing Artamedia's Enterprise Software)

Indah Ayu Widiyastuti, Istiqomah, Hanifah Dhia Nur Rohmah
Master of Management Postgraduate Program, University of Pamulang,
Jl. Raya Puspiptek,Gedung Vioktor, Tangerang Selatan, Banten 15310, Indonesia

indahdizka@gmail.com[1], istiqomahnila72@gmail.com[2] , Hanifah.nurrohmah10@gmail.com[3]

Abstract. The development of digital technology has driven significant transformation across various sectors, including the economy, education, and government. Digital technology infrastructure serves as a major foundation enabling broad connectivity, efficient data processing, and increasingly diverse digital services. This article examines the basic concepts, key components, as well as challenges and opportunities in developing digital technology infrastructure in Indonesia. The research approach used is a literature review of recent sources, including scientific journals, government reports, and industry publications. The findings indicate that although Indonesia has made notable progress in building its digital infrastructure, challenges such as access disparities between urban and rural areas, weak cybersecurity, and the need to improve human resource competencies remain key obstacles. These findings emphasize the importance of equitable, secure, and sustainable digital development strategies to support optimal national digital transformation.

Keywords: *Digital infrastructure, digital transformation, information technology, connectivity, technology policy.*

INTRODUCTION

The era of global digitalization requires every country to strengthen its digital technology infrastructure as a key pillar of knowledge-based economic growth. This infrastructure includes telecommunications networks, data centers, cloud computing, and cybersecurity systems. In Indonesia, accelerating digital transformation has become a national priority, as outlined in the Indonesia Digital Roadmap 2021–2024. However, various challenges such as limited network coverage, unequal access, and low digital literacy remain major issues that must be addressed. The rapid development of digital technology not only influences how companies conduct business processes but also transforms the structure of technological infrastructure that forms the foundation of organizational operations. One of the most crucial components in digital transformation is the digital technology infrastructure that supports the operational software used by companies. This infrastructure includes hardware, networks, data centers, cloud services, and cybersecurity systems that work in an integrated manner to ensure the smooth flow of information and business processes. For example, in the retail industry, the use of an inventory management system connected to real-time sales data greatly depends on adequate digital infrastructure to minimize errors and improve operational efficiency.

At the organizational level, software such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Human Resource Information Systems (HRIS), as well as production and logistics applications, require digital infrastructure that is stable, scalable, and secure. Without sufficient infrastructure, the implementation of such software systems will not be optimal and may even hinder operations, resulting in delayed data processing, service disruptions, and security risks that could affect business continuity. For instance, a company implementing an ERP system without a strong network infrastructure may face difficulties in quickly accessing data, which in turn slows down decision-making and affects overall performance. Digitalization within companies also increases the need for system integration, rapid data access, and analytical capabilities driven by big data and artificial intelligence. Therefore, companies are required to build infrastructure that not only meets current needs but can also adapt to rapid technological advancements. Common challenges include limited skilled human resources, high investment requirements, and increasingly complex security standards. For example, companies seeking to implement artificial intelligence–based solutions must ensure that they have sufficiently robust infrastructure to manage large volumes of data and the analytical complexity required.

Thus, a deep understanding of digital technology infrastructure and its role in supporting enterprise software is essential to ensure the effectiveness and sustainability of digital transformation. This study serves as a foundation for formulating infrastructure development strategies that can enhance corporate competitiveness in the digital era. By gaining a better understanding of how digital infrastructure functions and interacts with various systems and applications, companies can be better prepared to face existing challenges and leverage the opportunities offered by the digital era. In conclusion, strengthening digital technology infrastructure is not merely a necessity but a strategic step that is crucial for companies to survive and grow in an increasingly competitive business environment. By addressing existing challenges and utilizing technological advancements, companies can achieve a successful and sustainable digital transformation.

LITERATURE REVIEW

General

According to the OECD (2022), digital infrastructure includes technology systems that enable efficient data collection, storage, and exchange. Major components include broadband networks and 5G, data centers and cloud computing, the Internet of Things (IoT), and cybersecurity to ensure reliability and data privacy. Research from the Ministry of Communication and Information (2023) shows that the quality of digital infrastructure is directly proportional to the growth of the national digital economy. Development of digital infrastructure relies on several theoretical foundations. Information Systems Theory emphasizes the importance of alignment between technology, processes, and people as determinants of successful digital implementation. Communication Network Theory highlights network architecture as a vital element connecting devices and services for efficient information transfer. Distributed Computing Theory explains how computing resources can be shared and executed across multiple nodes to enhance performance and system reliability.

Telecommunication networks serve as the main foundation of digital infrastructure. Data centers support storage and processing of large-scale data and are increasingly adopting cloud-based models for flexibility and scalability. Cloud computing provides computing services through the internet and consists of IaaS, PaaS, and SaaS models. The digital ecosystem is further enhanced by IoT, enabling real-time device interconnectivity. Cybersecurity ensures continuity of digital infrastructure by protecting against hacking, data theft, and DDoS attacks. Digital infrastructure continues to evolve through innovations such as edge computing, artificial intelligence, quantum computing, and blockchain, which enhance the capability of managing larger data volumes and complex computational needs. Despite this progress, major challenges remain, including digital divides between urban and rural areas, increasing cybersecurity risks, costly infrastructure development, and regulatory or standardization gaps among stakeholders. The concept of Digital Technology Infrastructure (DTI) positions digital infrastructure as a foundation that enables organizations to develop, implement, and manage various digital systems effectively. This includes physical elements such as servers and network devices; software such as operating systems, middleware, APIs, and container platforms; cloud services; and data architecture elements such as data warehouses, data lakes, and ETL pipelines. Cybersecurity components like encryption, firewalls, identity management, and endpoint control play a critical role, supported by governance frameworks such as ITIL, COBIT, and ISO 27001.

In the context of company software, digital infrastructure supports core applications such as ERP SAP, CRM Salesforce, HRIS, and—in the case of this company—FileMaker as a microservices-based system. The role of FileMaker is analyzed based on how it functions as a core or supporting system and how it integrates with other systems through APIs, data exchange protocols (REST, SOAP, GraphQL), or middleware. System architecture determines whether the software is monolithic or microservices-based, and deployment models (on-premise, cloud, hybrid) influence scalability, costs, and regulatory compliance. Various frameworks such as IT Infrastructure Maturity Model, TOE (Technology–Organization–Environment), Enterprise Architecture (TOGAF, Zachman), and Resource-Based View (RBV) help analyze the strategic value and organizational impact of FileMaker implementation. Software implementation generally strengthens business processes, data consistency, operational efficiency, and security, though challenges arise such as integration complexity, limited network capabilities, lack of skilled IT personnel, high licensing costs, and stringent compliance requirements like GDPR or ISO 27001.

Weaknesses of Software in Company Operations

Although software offers many advantages, several weaknesses remain. Cost is often the main challenge, especially for enterprise-level systems with high licensing fees. Implementation, training, customization, and integration further increase overall expenses. Skills-related issues arise when employees must be trained to use new software and companies may become dependent on vendors. Security and privacy concerns are significant, particularly for cloud-based systems handling sensitive data. Operational disruptions may occur due to downtime, server overload, network issues, or bugs. User resistance also affects implementation success, especially among employees accustomed to manual processes or with low digital literacy. Software performance heavily depends on supporting infrastructure such as stable internet and adequate hardware. Integration challenges also arise, particularly with legacy systems due to differences in data formats, programming languages, or system architectures. Telecommunication networks form the backbone of digital infrastructure, allowing information to travel from one system to another seamlessly. Fiber-optic networks, satellite communications, and 5G mobile technology dramatically improve bandwidth, reduce latency, and support real-time communication. Alongside these networks, data centers serve as the primary facilities for storing, processing, and managing large-scale data flows. As organizations generate increasing amounts of data, traditional on-premises data centers are gradually shifting toward cloud-based models, which provide greater flexibility, elasticity, and cost efficiency. Cloud computing itself is categorized into several service models: Infrastructure as a Service (IaaS) offers virtualized hardware resources; Platform as a Service (PaaS) provides ready-to-use development environments; and Software as a Service (SaaS) delivers software applications directly through web interfaces. Together, these services reduce operational burdens and equip organizations with scalable capabilities.

The digital ecosystem becomes more dynamic with the advancement of IoT technologies, which enable physical devices to communicate autonomously. IoT systems support applications in manufacturing automation, smart transportation, agriculture, and healthcare monitoring. Cybersecurity is another critical component, ensuring continuity and resilience of digital infrastructure by safeguarding systems against cyberattacks such as ransomware, phishing, identity theft, and Distributed Denial of Service (DDoS) attacks. Ensuring confidentiality, integrity, and availability of data has become a major priority, especially as digital transactions increase exponentially. Digital infrastructure continues to evolve due to innovations in edge computing, artificial intelligence (AI), quantum computing, and blockchain. Edge computing places processing power closer to data sources to reduce latency and improve responsiveness. Artificial intelligence enhances predictive analytics, anomaly detection, and automated decision-making. Quantum computing, although still emerging, promises unprecedented computational speeds for optimization and encryption tasks. Blockchain introduces decentralized and transparent data management systems, making it valuable for supply chain tracking, financial transactions, and identity management. These innovations collectively strengthen the ability of organizations and governments to manage large and complex data environments.

Despite significant progress, various challenges persist. The most prominent issue is the digital divide between urban and rural areas, where disparities in access to stable internet services hinder inclusive growth. Cybersecurity risks are also escalating as digital adoption increases, with attackers exploiting vulnerabilities in networks, cloud systems, and IoT devices. Infrastructure development remains costly, requiring large investments in network expansion, data centers, and skilled personnel. Regulatory inconsistencies, lack of interoperability standards, and misalignment among stakeholders create additional barriers to cohesive digital ecosystem development. The concept of Digital Technology Infrastructure (DTI) positions digital infrastructure as a strategic foundation enabling organizations to design, deploy, and manage digital solutions effectively. DTI comprises physical hardware such as servers, routers, and storage systems; system software including operating systems, hypervisors, and middleware; cloud service models; and data architecture components such as data warehouses, data lakes, ETL/ELT pipelines, and API gateways. Cybersecurity technologies—encryption algorithms, multi-factor authentication, firewalls, identity and access management systems—support these structures by ensuring compliance with international governance frameworks such as ITIL, COBIT, and ISO 27001.

In organizational contexts, digital infrastructure supports software systems that manage core business operations. Enterprise Resource Planning (ERP) systems such as SAP streamline accounting, procurement, logistics, and inventory. Customer Relationship Management (CRM) applications like Salesforce enhance customer interaction, sales forecasting, and service management. Human Resource Information Systems (HRIS) manage employee data, payroll, and performance evaluation. In the context of this study, FileMaker serves as a microservices-based system supporting various operational needs. Its integration with other corporate systems, whether through REST APIs, SOAP protocols, GraphQL interfaces, or middleware platforms, determines its strategic role within the enterprise architecture. The system architecture—monolithic or microservices-based—also affects scalability, maintenance complexity, deployment efficiency, and cost. Deployment decisions, such as choosing between on-premise, cloud, or hybrid environments, further influence organizational flexibility and compliance with data protection regulations. Several frameworks—such as the IT Infrastructure Maturity Model, the Technology–Organization–Environment (TOE) framework, Enterprise Architecture models like TOGAF and Zachman, and the Resource-Based View (RBV)—provide analytical tools to assess the strategic importance, integration capabilities, and long-term value of FileMaker or any software implementation. These frameworks help determine capability readiness, digital transformation alignment, and contribution to competitive advantage.

Software implementation generally improves business processes, enhances data accuracy, supports informed decision-making, and increases operational efficiency. It strengthens organizational agility, reduces manual workloads, and promotes standardization across departments. However, several weaknesses may arise. High acquisition costs—especially for enterprise systems—can burden budgets, with additional expenses for customization, integration, training, and ongoing maintenance. Skills gaps may affect productivity, as employees must adapt to new systems while organizations depend heavily on vendors or external consultants. Security and privacy challenges are prevalent in cloud-based systems, particularly when handling sensitive personal or financial data. Technical disruptions such as downtime, bugs, and network instability can interrupt business continuity. User resistance also plays a role, especially among employees unfamiliar with digital tools or those who are comfortable with traditional manual workflows. Successful adoption requires effective change management strategies, continuous training, and strong leadership support. Integration barriers may emerge when modern applications interact with legacy systems that use outdated data formats or incompatible architectures. These issues complicate data synchronization, reduce system performance, and require additional middleware or redevelopment efforts.

Additional Literature Review (Extended Section)

The importance of digital infrastructure has grown significantly as organizations navigate an era of rapid technological change, global competition, and heightened customer expectations. Modern enterprises increasingly rely on digital systems not only to automate operational tasks but also to create new business models, enhance customer engagement, and improve decision-making accuracy. Scholars argue that digital infrastructure should be understood not as a static asset, but as a dynamic capability that evolves alongside organizational needs (Bharadwaj et al., 2013). This perspective emphasizes that digital maturity is achieved through continuous investment, integration, and adaptation to emerging technologies. As such, digital infrastructure forms the foundation upon which digital transformation initiatives are conceived, executed, and scaled.

Digital Platform Theory and Ecosystem Integration

Digital Platform Theory provides an essential foundation for understanding how modern organizations build interconnected technological environments. Digital platforms function as intermediaries that connect users, organizations, applications, and external systems through shared standards, interoperable services, and structured governance. Within these ecosystems, platforms do not simply enable transactions; they orchestrate interactions, facilitate data exchange, and establish rules that shape how participating entities create and capture value.the platform’s role by enabling customized microservices that link with larger enterprise systems. In today’s business environment, organizations increasingly operate within platform-based ecosystems where data flows seamlessly across various internal applications and external stakeholder systems. This interconnectedness is made possible through architectural principles such as modularity and loose coupling, which allow individual components to evolve independently without disrupting the entire system. Application Programming Interfaces (APIs) play a central role in this process by enabling enterprise tools to communicate efficiently and securely. Through API-driven integration, companies can synchronize customer data between CRM systems and e-commerce platforms, connect ERP modules with mobile applications, or embed specialized analytics engines into existing operational workflows.

Scholars emphasize that the effectiveness of digital platforms hinges on three core attributes: modularity, which allows subsystems to be updated or replaced without affecting the whole; openness, which encourages external developers, partners, or vendors to innovate on top of the platform; and governance, which maintains the balance between stability, scalability, and innovation (Tiwana, 2014). Strong governance ensures compliance with security standards, regulates access rights, and establishes protocols for managing data interoperability, all while supporting continuous innovation by ecosystem participants. These theoretical perspectives are particularly relevant when analyzing the role of customized software solutions such as FileMaker within broader enterprise ecosystems. As a low-code development platform, FileMaker enables organizations to build tailored applications and microservices that respond to unique operational needs. When integrated into larger enterprise architectures, these microservices act as complementary modules that enhance system functionality without requiring major reconfigurations of core platforms. FileMaker applications can serve as connectors that bridge data from on-premises databases to cloud services, automate workflow processes, or extend ERP and CRM capabilities through custom interfaces and data management tools. By supporting interoperability and extensibility, FileMaker contributes to the digital platform’s role as a dynamic ecosystem enabler. It empowers organizations to rapidly prototype solutions, integrate disparate data sources, and respond to evolving business demands—all while maintaining alignment with platform governance and security protocols. This illustrates how digital platform theory not only explains macro-level ecosystem behavior but also provides a lens for evaluating micro-level integration strategies within enterprise environments.

RESEARCH METHOD

This study adopts a case study research design to gain an in-depth understanding of how the implementation of FileMaker software influences digital infrastructure readiness, system integration, and organizational business processes. The case study approach is suitable because it allows for a comprehensive examination of complex real-world environments in which technology, users, workflows, and internal company policies interact dynamically. By focusing on a specific organizational context, this method enables the researcher to capture nuanced insights, including behavioral, technical, and managerial dimensions that cannot be fully explored through purely quantitative or experimental designs. To obtain a holistic understanding, a mixed-method approach is employed, combining qualitative and quantitative data collection techniques. The qualitative component includes in-depth interviews with key stakeholders such as IT managers, system developers, business analysts, and end users who interact with the FileMaker system on a daily basis. These interviews aim to identify challenges, user experiences, perceptions of system effectiveness, and alignment with existing digital infrastructure. Direct observation of software usage is also conducted to capture how FileMaker supports operational workflows, data processing activities, and coordination between departments. Additionally, internal documentation—such as Standard Operating Procedures (SOPs), system architecture diagrams, implementation guidelines, and system performance reports—is reviewed to provide structural insights into the organization’s digital ecosystem. The quantitative component consists of structured user surveys using measurement constructs adapted from established and validated models, including the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology (UTAUT), and the System Usability Scale (SUS). These instruments measure user acceptance, perceived ease of use, perceived usefulness, usability levels, and perceived performance improvements following software implementation. Quantitative data provide numerical evidence that complements the qualitative findings and strengthens the empirical grounding of the study.

Data analysis is conducted using both qualitative and quantitative techniques. Qualitative data are analyzed through thematic coding, allowing key themes, patterns, and relationships to emerge systematically from interview transcripts, observations, and documents. This inductive approach helps reveal underlying issues related to infrastructure readiness, integration challenges, user adaptation, and organizational support mechanisms. Quantitative data are analyzed using descriptive statistics to summarize user responses, identify distribution trends, and assess general levels of acceptance and usability across the organization. To enhance the reliability and validity of the findings, methodological triangulation is applied. This involves cross-verifying data obtained from interviews, observations, surveys, and internal documents. Triangulation ensures consistency, reduces potential bias, and strengthens the credibility of the conclusions drawn. Through this rigorous methodological framework, the study provides a comprehensive and evidence-based understanding of FileMaker’s role within the digital transformation landscape of the organization.

RESULTS AND DISCUSSION

General

The findings indicate that digital technology infrastructure plays a central and enabling role in ensuring the successful implementation of enterprise software solutions. A robust infrastructure—encompassing hardware, operating systems, network capacity, data architecture, cybersecurity mechanisms, and governance frameworks—forms the backbone that supports FileMaker’s optimal performance. Organizations with well-developed infrastructure are better equipped to leverage FileMaker for process automation, workflow customization, and seamless interaction with other enterprise systems. Furthermore, the presence of cloud computing platforms, Application Programming Interfaces (APIs), middleware tools, and system integration mechanisms significantly expands the scope of digital adoption and enhances interoperability across organizational units. The results also demonstrate that the implementation of enterprise software contributes directly to improvements in operational efficiency, data accuracy, task automation, collaboration, and data-driven decision-making. FileMaker enables users to digitize manual workflows, reduce repetitive administrative tasks, and centralize data into structured repositories. These capabilities align closely with established theoretical models such as the IT Infrastructure Maturity Model, which emphasizes the progression from basic technological readiness to advanced levels of integration and optimization. Similarly, the findings correspond to the

Technology–Organization–Environment (TOE) Framework, which explains how technological capabilities, organizational conditions, and environmental pressures collectively shape adoption outcomes. Organizations with strong digital infrastructure and supportive cultural environments tend to achieve higher levels of software utilization and innovation.

Despite these benefits, several challenges were identified during implementation. High initial investment costs—related to hardware upgrades, cloud subscriptions, and system customization—often limit the speed of digital transformation, particularly for small and medium-sized enterprises. Training and upskilling also emerge as critical needs, as effective utilization of FileMaker requires a combination of technical competencies, analytical skills, and user familiarity with digital workflows. Moreover, dependency on specialized technical expertise poses a risk when internal IT teams are limited or when knowledge transfer is insufficient. Security risks represent an additional challenge, particularly in cloud-based environments where data is stored, transmitted, and accessed across distributed networks. The findings highlight concerns related to access control, data privacy, and the need for continuous monitoring to prevent security breaches. These issues underscore the importance of comprehensive governance frameworks to regulate system usage, ensure compliance with industry standards, and mitigate operational risks. Overall, the results reinforce the conclusion that digital infrastructure maturity significantly influences the success of enterprise software adoption. When infrastructure, human capabilities, and governance structures are aligned, organizations can maximize the strategic value of FileMaker and other digital technologies, thereby enhancing competitiveness and supporting long-term digital transformation.

IT Governance, Compliance, and Organizational Control

Effective digital infrastructure management also requires robust IT governance. Frameworks such as COBIT 2019 emphasize strategic alignment, performance measurement, risk mitigation, and governance of enterprise IT assets. Governance ensures that technology investments align with organizational goals and comply with regulatory requirements such as GDPR, ISO 27001, HIPAA, or Indonesia's PDP Law. Compliance plays an increasingly central role in digital infrastructure planning because data privacy, ethical data usage, and cybersecurity policies directly affect system design and operational workflows. Research suggests that strong governance improves system reliability, reduces operational risks, and enhances user trust—especially in sectors such as finance, healthcare, and public administration.

Human–Technology Interaction and Digital Competence

From a human-centre perspective, the Human–Technology Interaction (HTI) framework explains how individuals interact with digital systems. User experience (UX), interface design, and digital literacy influence software adoption and overall system performance. Organizations must ensure that employees possess adequate digital competence, including skills related to data interpretation, cybersecurity awareness, and task automation. Digital infrastructure is effective only when users are able to leverage the technology to its fullest potential. Studies indicate that organizations with strong digital culture—characterized by openness to change, technology-driven innovation, and continuous learning—are more successful in adopting complex digital systems (Westerman et al., 2014).

Global Best Practices and Benchmarking in Digital Infrastructure

International benchmarks demonstrate how advanced digital infrastructure contributes to economic and organizational competitiveness. Countries such as South Korea, Singapore, and Finland prioritize nationwide high-speed connectivity, data center expansion, and digital government services. These countries invest heavily in edge computing nodes, 5G coverage, and cybersecurity command centers that monitor threats in real time. Their success illustrates the value of coordinated policies, public–private collaboration, and long-term digital roadmaps. These global experiences provide important lessons for organizations attempting to modernize their internal infrastructure: strategic planning, interoperability standards, and customer-centric designs are essential for maximizing the benefits of digital investments.

Sector-Specific Implications of Digital Infrastructure

In manufacturing, digital infrastructure facilitates smart factory operations, where IoT sensors, robotics, and predictive analytics enable real-time monitoring and quality control. Cloud-based systems allow manufacturers to synchronize supply chains, manage inventories more accurately, and reduce downtime through predictive maintenance. In retail, digital infrastructure enables omnichannel experiences, data-driven marketing, and personalized customer recommendations powered by machine learning algorithms. Meanwhile, in the financial sector, the reliability of digital infrastructure determines the security and availability of digital payments, online banking, and risk management systems. In organizational settings, digital infrastructure strengthens internal communication, supports remote work, and enhances data sharing across departments. The adoption of collaboration tools such as Microsoft 365, Google Workspace, Slack, or custom-built platforms depends heavily on stable networks, secure authentication systems, and well-designed backend architecture. As businesses increasingly move towards hybrid work models, the need for virtual private networks (VPNs), multi-factor authentication (MFA), and cloud security policies becomes even more critical.

Scalability, Interoperability, and System Lifecycle Management

Scalability is a crucial dimension of digital infrastructure, as organizations must adjust computational resources based on fluctuating workloads. Cloud elasticity enables businesses to allocate additional storage, processing power, or bandwidth during peak periods while reducing costs during low-demand cycles. System interoperability also ensures that data can move smoothly between old and new systems, reducing redundancy and inconsistencies. Poor interoperability often leads to data silos, inefficiencies, and increased operational risks. Lifecycle management is another important concept that ensures software and infrastructure remain up-to-date, secure, and reliable throughout their operational lifespan. This includes version upgrades, patch management, vulnerability scanning, performance monitoring, and end-of-life transition planning. Proper lifecycle management prevents compatibility issues and minimizes the likelihood of system failures.

Future Trends and Strategic Directions

Looking forward, digital infrastructure development will be shaped by several emerging trends. Advanced analytics, including big data and AI-driven insights, will be increasingly integrated into enterprise operations. Zero Trust Architecture (ZTA) is becoming the new standard for cybersecurity, replacing perimeter-based defenses with continuous verification mechanisms. Sustainable IT practices, such as green data centers, energy-efficient cooling systems, and renewable-powered networks, are gaining attention as organizations aim to reduce carbon footprints. Another important dimension of digital infrastructure is the organizational capability to manage data as a strategic asset. Data Management Theory emphasizes that high-quality data—accurate, consistent, timely, and accessible—forms the backbone of effective decision-making across all levels of an organization. With the rapid growth of enterprise data, companies are increasingly adopting data governance frameworks to regulate data usage, establish ownership, and implement standardized procedures for data quality assurance. These frameworks include components such as metadata management, data stewardship roles, and data lineage tracking, ensuring that information flowing through enterprise systems remains trustworthy and auditable. As organizations move toward analytics-driven decision-making, data lakes, data warehouses, and ETL/ELT pipelines become integral elements of digital infrastructure, supporting both operational processes and strategic business intelligence initiatives.

The rise of automation and digital workflows also underscores the role of Business Process Management (BPM) in shaping digital infrastructure adoption. BPM theory explains how organizations analyze, redesign, and optimize business processes to improve efficiency and reduce operational bottlenecks. Digital infrastructure supports BPM by enabling process automation through robotic process automation (RPA), enterprise workflow engines, and integrated applications that reduce manual workloads. Organizations that implement BPM supported by strong digital infrastructure often experience improvements in cycle times, customer satisfaction, and error reduction. This reinforces the idea that technological tools cannot deliver full benefits without parallel process redesign and continuous improvement practices. In addition, digital resilience has emerged as a key concept within contemporary literature. Digital resilience refers to an organization’s capability to maintain operations and recover quickly from disruptions caused by cyberattacks, system failures, network outages, or natural disasters. Modern digital infrastructure incorporates redundancy systems, disaster recovery (DR) sites, backup solutions, and high availability (HA) architectures to ensure business continuity. Cloud service providers typically offer multi-region availability zones, automated failover mechanisms, and real-time monitoring dashboards to detect anomalies early. Research suggests that organizations with resilient digital infrastructure demonstrate higher operational reliability, reduced downtime costs, and stronger customer trust.

The role of leadership also receives growing attention in digital infrastructure literature. Digital leadership theories highlight the importance of leaders who can articulate a clear digital vision, promote innovation, encourage cross-functional collaboration, and foster a culture of experimentation. Leaders who understand the strategic value of digital infrastructure are better equipped to prioritize investments, allocate resources effectively, and drive digital transformation initiatives across departments. Studies show that leadership support is one of the strongest predictors of successful technology adoption, particularly in environments where employees may resist change or lack digital literacy. Finally, literature increasingly focuses on the socio-economic implications of digital infrastructure adoption. On a macro level, digital infrastructure enhances national competitiveness by improving public services, supporting digital entrepreneurship, and facilitating cross-border trade. On a micro level, it empowers organizations to adopt new business models such as e-commerce, remote work systems, data monetization, and digital platforms that connect suppliers, partners, and customers. However, scholars caution that without inclusive policies and broad-based access, digitalization may widen inequalities. Thus, the development of digital infrastructure must be accompanied by capacity-building programs, digital literacy initiatives, and regulatory frameworks that encourage innovation while protecting users.

CONCLUSION

Digital technology infrastructure constitutes a fundamental pillar for enabling and sustaining corporate digital transformation. This infrastructure encompasses physical components, enterprise software environments, data architecture, cloud computing platforms, governance structures, and cybersecurity frameworks. Together, these elements form an integrated digital ecosystem that supports the effective and sustainable adoption of enterprise software solutions. Without a solid infrastructure foundation, digital initiatives are likely to face operational constraints, reduced system performance, and heightened security vulnerabilities. The findings of this study reaffirm the relevance of several theoretical perspectives—Information Systems Theory, Network Communication Theory, Distributed Computing Theory, IT Infrastructure Maturity, the Technology–Organization–Environment (TOE) Framework, Enterprise Architecture principles, and the Resource-Based View (RBV). Collectively, these perspectives highlight that the success of any software implementation depends on achieving alignment between technological capabilities, organizational structures, and external business environments. Effective software adoption requires seamless integration with the existing infrastructure to ensure gains in efficiency, data accuracy, workflow automation, collaboration, and evidence-based decision-making.

Moreover, the study concludes that enterprise software can serve as a strategic enabler of digital transformation when supported by mature technological infrastructure, competent human resources, and an adaptive organizational culture. When employees possess the necessary skills and the organization embraces a culture of innovation, software can evolve beyond a simple operational tool into a catalyst that enhances organizational agility, competitiveness, and strategic responsiveness. However, several ongoing challenges—such as technological disparities, security vulnerabilities, integration complexity, data governance issues, and significant financial investments—must be addressed through comprehensive and proactive management strategies. Therefore, software implementation should not be viewed in isolation but understood as an integral component of a broader digital system. Its success is determined by the quality and readiness of the digital infrastructure, the organization's capacity for integration, and the preparedness of its people and processes. When these factors are aligned, strong digital infrastructure positions software as a strategic asset that drives superior performance, strengthens competitive advantage, and supports holistic, long-term digital transformation across the organization.

REFERENCE

Ministry of Communication and Information Technology. (2023). National Digital Transformation Report. Jakarta: Kominfo.

OECD. (2022). Digital Economy Outlook 2022. Paris: OECD Publishing.

World Bank. (2023). Digital Infrastructure in Developing Countries. Washington, D.C.: World Bank.

Setiawan, A., & Rahmawati, N. (2021). *Analysis of Digital Infrastructure in Indonesia*. Journal of Information and Communication Technology, 15(2), 45–58.

Fauzan, R. Y., Reyan, M., & Adha, D. (2025). Improving Digital Infrastructure: Assisting with Internet Service Activation at SMAN 3 Payakumbuh. 4(2), 6–10.

Hoshmand, M. O., & Ratnawati, S. (2023). Information Technology Infrastructure Security Analysis in Facing Cybersecurity Threats. 5(2), 679–686.

Wahyuanto, E., Taufiqi, M. A., Azizah, N., & Maryam, N. S. (2025). Utilizing Digital Technology to Improve Village Administration. 03(03), 359–363.

Ministry of Communication and Information Technology of Indonesia. (2023). *Indonesia digital infrastructure development report.* Kementerian Komunikasi dan Informatika Republik Indonesia.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next-generation strategy. *MIS Quarterly, 37*(2), 471–482.

Tiwana, A. (2014). *Platform ecosystems: Aligning architecture, governance, and strategy.* Morgan Kaufmann.Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into business transformation.* Harvard Business Review Press.

Marques, J., Ferreira, J., & Ferreira, F. (2020). Digital transformation in organizations: A systematic literature review. *Journal of Business Research, 123*, 567–580.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things: security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.