

REVIEW ARTICLE

A Systematic Synthesis of Data Governance and Cybersecurity on Trust and Acceptance of Digital Government in Thailand

Anaphat Nongkhoo*, Cholpassorn Sitthiwarongchai, Wutipong Janmuangthai

College of Innovation and Management, Suan Sunandha Rajabhat University, Dusit, Bangkok 10300 Thailand

* Corresponding author: anaphat.no@ssru.ac.th

Received: 21 March 2026 / Revised: 30 April 2026 / Accepted: 30 April 2026

Abstract. This review article presents a systematic synthesis of the structural relationship between data governance and cybersecurity and examines their collective influence on public trust and the acceptance of digital government services in Thailand. Using a qualitative Systematic Literature Review (SLR) of global and domestic scholarly works published between 2017 and 2026, the study explores the complex balance between technological advancement and societal confidence. The findings reveal a critical paradox: while Thailand is actively pursuing its ambition to become one of the top 40 digital governments by 2027, persistent cyber threats and data breaches continue to undermine public trust. The synthesis suggests that data governance provides the institutional framework for transparency and data quality, whereas cybersecurity establishes the technical foundation for risk mitigation. When integrated, these two pillars enable what is referred to as “technical verifiability,” which functions as a key mechanism that encourages citizens to move from basic awareness toward meaningful acceptance of digital technologies. Policy recommendations highlight the need to transition from fragmented “data silos” to an integrated national data architecture. By adopting Privacy-Enhancing Technologies (PETs) and promoting a stronger culture of institutional accountability, the Thai government can move beyond the mere deployment of digital systems toward building the enduring digital trust required for a sustainable digital future.

Keywords: Cybersecurity, Data Governance, Digital Government, Digital Trust, Technology Acceptance, Technical Verifiability

1. Introduction

In the contemporary global landscape, the evolution of digital government has extended beyond administrative convenience and has become an important indicator of national competitiveness and modern governance capacity. The United Nations *E-Government*

Survey 2024 highlights a significant global movement toward digital transformation as a pathway to achieving inclusivity and sustainable development. Within this broader transformation, the global digital economy is projected to reach approximately USD 16 trillion in 2024, indicating that digital economic activities are expanding approximately 2.5 times faster than traditional economic sectors. As a result, governments around the world are increasingly required to strengthen their digital infrastructure in order to remain resilient within an increasingly complex and dynamic environment.

For Thailand, the transition toward a digital government has been positioned as a key national priority, formally articulated in the Digital Government Development Plan (2023–2027). The Thai government has established an ambitious target: to rank among the top 40 countries in the global E-Government Development Index (EGDI) by 2027. This strategic direction is closely aligned with the 20-Year National Strategy and the 13th National Economic and Social Development Plan, both of which envision a more agile and digitally enabled public administration capable of supporting the BCG Economic Model through inclusive access to public services.

However, the acceleration of digital transformation also introduces significant challenges, particularly in relation to cybersecurity risks and the protection of personal data. Recent statistics from 2025–2026 indicate a substantial increase in cyber intrusion attempts and sophisticated fraud incidents, resulting in cumulative financial losses exceeding 98,000 million THB. Beyond financial damages, these

incidents undermine the level of digital trust that citizens place in public institutions. While regional leaders such as Singapore have achieved digital trust levels of approximately 59%, Thailand continues to face challenges in strengthening institutional confidence despite the existence of legal frameworks such as the Personal Data Protection Act (PDPA) , B.E. 2562 (2019) and the Cybersecurity Act, B.E. 2562 (2019).

This study therefore provides a systematic synthesis of data governance and cybersecurity as two critical foundations of a trustworthy digital government ecosystem. By examining the intersection between policy frameworks and technological mechanisms, this research aims to explore how Thailand can develop an institutional environment in which digital technologies are not only implemented but also broadly accepted and trusted by citizens.

2. Conceptual Framework and Methodology

The objective of this research is to synthesize the critical dimensions of data governance and cybersecurity within the Thai public sector and to examine their influence on digital trust and technology acceptance. The following sections outline the theoretical foundations and the systematic approach employed in this study.

2.1 Conceptual Framework: Systemic Determinants and Outcomes

The conceptual framework of this study posits that data governance and cybersecurity constitute fundamental prerequisites for establishing a reliable digital government ecosystem. While data governance provides policy-oriented oversight emphasizing transparency, accountability, and regulatory compliance, cybersecurity functions as the technical safeguard that ensures data integrity, confidentiality, and system resilience in accordance with international standards such as the NIST Cybersecurity Framework.

Together, these structural dimensions influence citizens' perceived risk, which in turn plays a crucial role in shaping the level of digital trust in government systems.

The research framework is organized into three primary components.

- **Systemic Determinants (Inputs).** This dimension includes data governance, which ensures systematic data management through transparency, accountability, and legal compliance, and cybersecurity, which focuses on technical protection mechanisms and institutional response capabilities, including the establishment of Cyber Security Operations Centers (CSOC) to monitor and respond to cyber incidents.
- **Trust and Acceptance (Outcomes).** In this dimension, digital trust refers to the public's expectation that government digital systems will protect personal data, safeguard individual rights, and operate in a responsible manner. Such trust subsequently contributes to digital government acceptance, which is reflected in citizens' willingness to use digital services and participate in data integration initiatives.
- **Technical Verifiability.** This element functions as a bridge between systemic determinants and social outcomes. It refers to the ability of digital systems to provide verifiable technical evidence regarding security, transparency, and accountability throughout the lifecycle of digital government operations.

2.2 Review Methodology

This study adopts a Systematic Literature Review (SLR) methodology to collect and synthesize relevant evidence from policy documents, academic publications, and institutional reports published between 2017 and 2026.

The review encompasses three primary categories of information.

- **National Policy and Regulatory Documents.** This includes an analysis of strategic frameworks, legal instruments, and operational standards issued by major Thai government agencies, including the Digital Government Development Agency (DGA), the National Cyber

Security Agency (NCSA), and the Personal Data Protection Committee (PDPC).

- International Institutional Reports. The review also incorporates analytical reports and global indicators published by international organizations, including the United Nations (UN), the World Economic Forum (WEF), and the Organization for Economic Co-operation and Development (OECD).
- Scholarly Literature. A systematic search was conducted in peer-reviewed academic journals, both domestic and international, focusing on studies related to digital governance, cybersecurity, institutional trust, and technology acceptance.

3. Implementation of Data Governance and Cybersecurity in Thailand's Digital Government

The success of digital government initiatives is closely linked to the level of trust and acceptance among citizens. This section examines the implementation of data governance and cybersecurity within the Thai public sector, with particular attention to the legal frameworks and operational developments that shape the national digital ecosystem.

3.1 Strategic Policy Frameworks and the Digital Landscape

Thailand has positioned data governance and cybersecurity as central pillars of its national digital transformation agenda. These priorities are embedded within several high-level strategic frameworks.

- 20-Year National Strategy. This national strategy envisions the development of a digital government ecosystem characterized by seamless data integration, transparency, and institutional accountability. The strategy emphasizes the importance of strong data governance mechanisms and cybersecurity measures to safeguard critical national infrastructure.
- Digital Government Development Plan (2023–2027). This plan outlines strategic directions for government agencies to

adopt standardized Data Governance Frameworks while strengthening cyber resilience through centralized digital platforms and advanced cybersecurity mechanisms.

- National Security Policy (2023–2027). This policy framework aims to strengthen national capacity in preventing cyber threats by elevating security standards for Critical Information Infrastructure (CII) and improving national mechanisms for responding to cyber-related crimes.

3.2 Key Initiatives in Data Governance

Data governance in the Thai public sector refers to the systematic management of data through clearly defined rights, responsibilities, and institutional mechanisms to ensure data accuracy, privacy protection, and secure interoperability. Several important legal and operational developments illustrate the advancement of data governance in Thailand.

The landscape of digital governance and security in Thailand is defined by several key legislative and regulatory instruments, as summarized in Table 1.

- Regulatory Frameworks. The enactment of the Personal Data Protection Act (PDPA) B.E. 2562 (2019) together with the issuance of data management standards by the Digital Government Development Agency (DGA) has established an important regulatory foundation for public sector data governance, particularly in relation to data classification, metadata standards, and responsible data sharing.
- Data Cataloguing and Interoperability. The Government Data Catalogue, coordinated by the National Statistical Office, currently integrates more than 20,210 datasets from 302 government agencies. In addition, the national Open Data platform (data.go.th) provides public access to more than 34,000 datasets, supporting transparency and enabling the creation of social and economic value from government data.

- **Operational Readiness.** Findings from the 2025 Digital Government Readiness Survey indicate that approximately 77% of department-level government agencies have reached an intermediate stage of data-driven organizational maturity. Within this group, high priority has been placed on data access control (84%) and data accuracy management (99%), reflecting increasing institutional awareness of data governance practices.

3.3 Cybersecurity Implementation and Threat Management

Cybersecurity functions as a critical technical safeguard for maintaining institutional trust in digital government systems. In Thailand, the National Cyber Security Agency (NCSA) is responsible for coordinating national cybersecurity standards and responding to emerging cyber threats.

- **Legal Compliance.** The Cybersecurity Act B.E. 2562 (2019) provides the legal framework that requires government agencies and operators of Critical Information Infrastructure (CII) to implement preventive, detective, and responsive cybersecurity measures in alignment with international standards such as the NIST Cybersecurity Framework.
- **Incident Response.** In 2025, the national cyber response center detected more than 200 million compromised credentials, highlighting the increasing scale of cyber threats. These developments have reinforced the need for stronger national capabilities in incident response, digital forensics, and threat intelligence to protect government digital infrastructure.

3.4 Public Trust and Digital Acceptance Trends

Despite the robust legal framework established by the PDPA and the Cybersecurity Act, a critical paradox emerges within Thailand's

digital landscape. While the Thailand Digital Outlook 2025 report indicates that public confidence in national digital policies has reached approximately 99%, this confidence does not necessarily translate into behavioral trust. In practice, the willingness of citizens to share personal data online declined to 42.94% in 2025. This paradox suggests that although citizens recognize the efficiency and benefits of digital government infrastructure, concerns regarding data privacy risks and increasingly sophisticated online fraud continue to limit full behavioral acceptance of digital government services. Such concerns may be influenced by the increasing scale of cyber incidents, including the detection of more than 200 million compromised credentials during the same period.

4. Analysis of Cybersecurity and Data Governance on Digital Government Trust and Acceptance

This section synthesizes findings from 28 scholarly publications and institutional reports published between 2017 and 2026, consisting of 14 domestic and 14 international sources. The analysis organizes the evidence into four analytical pillars: infrastructure and security, data governance, trust drivers, and dimensions of acceptance.

A comprehensive synthesis of the 28 selected scholarly publications and institutional reports, categorized by their primary analytical pillars, is presented in Table 2.

4.1 Analysis of Cybersecurity Dimensions

The systematic review indicates that perceived risk remains a critical determinant influencing citizens' adoption of public digital services. Concerns related to personal data protection and the risk of cyberattacks continue to act as major barriers to citizen participation in digital government platforms.

Table 1. Key Legal and Regulatory Frameworks for Data Governance and Cybersecurity in Thailand

Legislation / Standard	Key Summary
Personal Data Protection Act (PDPA) B.E. 2562 (2019)	Establishes standards for data collection, processing, and protection to ensure public confidence in data privacy.
Cybersecurity Act B.E. 2562 (2019)	Defines policies and measures for government and Critical Information Infrastructure (CII) to prevent and respond to cyber threats.
Government Data Governance Standard (V1.0 & Revised)	Defines rights and responsibilities in data management, covering lifecycle processes and success metrics.
Government Data Cataloging Standard (DGA 3/2564)	Provides guidelines for agencies to create data catalogs and metadata consistent with national governance frameworks.
Framework for Cybersecurity Practices for Government Agencies (2021)	Establishes NIST-based standards for identification, protection, detection, response, and recovery.
Standard for Website Security for Government and CII (2025)	Sets minimum technical and governance requirements for official digital platforms.

Table 2. Systematic Synthesis of Cybersecurity and Data Governance on Digital Trust and Acceptance.

No.	Source (Author & Year)	Cybersecurity			Data Governance			Trust Drivers			Use and Acceptance		
		Risk Management	Security-Enhancing Technologies	System Reliability	Data Governance	Privacy and Transparency	Regulatory Compliance	Institutional Integrity	Responsiveness	Digital Social Contract	Usage Level	Adoption Barriers	Digital Literacy
1	NCSA (2026)		X	X	X		X		X	X	X	X	X
2	Chanjaras (2025)	X	X			X	X	X	X		X	X	
3	DGA (2025)		X	X	X		X		X		X	X	X
4	Elayah (2025)				X	X		X	X		X	X	X
5	Kaowisut & Thongchana (2025)		X	X	X	X		X	X		X	X	
6	OECD/ADB (2025)			X	X	X		X	X		X		
7	Preecha (2025)	X	X					X				X	

Table 2. Systematic Synthesis of Cybersecurity and Data Governance on Digital Trust and Acceptance (continuous).

No.	Source (Author & Year)	Cybersecurity			Data Governance			Trust Drivers			Use and Acceptance		
		Risk Management	Security-Enhancing Technologies	System Reliability	Data Governance	Privacy and Transparency	Regulatory Compliance	Institutional Integrity	Responsiveness	Digital Social Contract	Usage Level	Adoption Barriers	Digital Literacy
8	PwC (2025)	X	X	X	X	X						X	X
9	Tadsadornkulpat (2025)			X	X	X	X	X	X			X	X
10	Aleisa (2024)		X	X		X		X	X		X	X	X
11	Chakrothai (2024)	X	X				X						X
12	Ciancarini et al. (2024)		X	X	X				X		X		
13	Desrochers (2024)		X	X	X	X	X	X		X			
14	Hasan et al. (2024)		X	X		X	X	X	X		X	X	X
15	Kehabal (2024)	X	X					X				X	X
16	Rajan (2024)	X	X	X	X		X						X
17	Zyoud & Lutfi (2024)	X	X	X	X	X						X	X
18	Lao-rat (2022)		X		X						X	X	
19	Nakonsong & Jamratphan (2022)		X	X	X	X		X	X		X		X
20	World Bank Group (2022)		X	X	X	X	X		X		X		
21	World Economic Forum (2022)	X	X		X	X		X		X		X	
22	Wylde et al. (2022)	X	X		X	X	X	X		X		X	
23	Brezzi et al. (2021)			X		X		X	X	X			
24	Kunchonchai (2021)				X	X						X	X

Table 2. Systematic Synthesis of Cybersecurity and Data Governance on Digital Trust and Acceptance (continuous).

No.	Source (Author & Year)	Cybersecurity			Data Governance			Trust Drivers			Use and Acceptance		
		Risk Management	Security-Enhancing Technologies	System Reliability	Data Governance	Privacy and Transparency	Regulatory Compliance	Institutional Integrity	Responsiveness	Digital Social Contract	Usage Level	Adoption Barriers	Digital Literacy
25	OECD (2020)			X	X	X		X	X		X		
26	Songittisuk (2019)				X				X			X	X
27	Yonghuay & Tabtieng (2019)			X	X						X	X	
28	Sirirattana (2017)			X	X		X	X	X			X	X

- **Global and Domestic Perspectives.** International research—particularly studies conducted in countries such as Saudi Arabia—highlights the integration of cybersecurity with Digital Intelligence and sociocultural factors as essential components of digital government adoption. In contrast, Thai studies tend to focus on specific demographic groups, including urban professionals and academic personnel, while emphasizing the role of emerging technologies such as Artificial Intelligence (AI) and Blockchain in strengthening technical verifiability
- **Risk Mitigation Mechanisms.** Evidence from the literature suggests that government cybersecurity preparedness—including technical capacity, regulatory maturity, and institutional coordination—plays a significant role in reducing perceived risk and discouraging avoidance behavior toward digital government services.
- **The Trust Gap.** Despite technological advancements, approximately 86% of the Thai population continues to express concern regarding online fraud and data leakage. This finding highlights a persistent gap between

technological deployment and the level of trust perceived by citizens.

4.2 Data Governance and Administrative Transparency

Data governance is increasingly recognized as a structural foundation for developing an efficient and trustworthy digital government.

- **Interoperability and Big Data Integration.** Effective data governance functions as a key mechanism for reducing data silos, thereby enabling interoperability among government agencies and strengthening the government’s capacity to deliver integrated public services.
- **The Privacy–Transparency Paradox.** Although Open Government Data initiatives promote transparency and enhance positive public perceptions of government institutions, their success depends heavily on robust data privacy protection. International frameworks, particularly those proposed by the World Economic Forum (WEF), emphasize that digital trust can only be sustained when citizens are confident that their data is managed responsibly and securely.

- **Accountability through Institutional Compliance.** In the Thai context, legal frameworks such as the Personal Data Protection Act (PDPA) and the Cybersecurity Act provide the baseline for institutional accountability. However, international governance frameworks increasingly emphasize the importance of moving beyond compliance-based trust toward ethical accountability, which is supported by transparent technical verification mechanisms.

4.3 Drivers of Public Trust and Behavioral Acceptance

The synthesis suggests that digital trust is fundamentally rooted in institutional competence and demonstrable transparency, which together shape citizens' perceptions of reliability and accountability in digital government systems.

- **Institutional Competence and Integrity.** Frameworks proposed by international organizations, such as the OECD and the WEF, identify reliability and integrity in data governance as primary drivers of digital trust. In the Thai context, although formal institutional frameworks are established, trust formation still relies heavily on legal enforcement mechanisms rather than the "technical verifiability" observed in more mature digital ecosystems.
- **Human Capital and Cultural Drivers.** A noticeable divergence appears in the strategies for fostering digital adoption. International studies often emphasize the role of citizens' Digital Intelligence (DQ) as a long-term driver of innovation acceptance. In contrast, Thai literature—as synthesized in Table 2—tends to prioritize the digital literacy of government officials. This suggests that the expertise, professionalism, and transparency of public sector personnel play a central role in shaping citizens' trust and willingness to adopt digital government services.

Building on these findings, this divergence reflects a broader strategic gap in the development of digital trust. While current efforts in Thailand have focused primarily on strengthening institutional capacity and service delivery mechanisms, comparatively less emphasis has been placed on empowering citizens to independently assess and manage digital risks. This imbalance suggests that the development of sustainable digital trust requires a more integrated approach that simultaneously strengthens both institutional credibility and citizen-level digital competence.

5. Policy Recommendations for Cultivating Digital Trust and Acceptance in Thailand

Based on the systematic synthesis of both domestic and international research, this section proposes a set of strategic policy recommendations aimed at strengthening a digital trust ecosystem in Thailand. These recommendations emphasize the integration of data governance as the structural foundation of value creation, supported by cybersecurity as a critical mechanism for safeguarding individual rights and institutional integrity.

5.1 Strategic Data Governance and Architectural Integration

To address the current limitations in administrative coordination and service efficiency, the Thai government should consider the following strategic directions.

- **Integration of National Data Architecture.** The government should gradually transition from fragmented data silos toward an integrated national data architecture supported by standardized interoperability protocols. Such integration would enhance cross-agency data exchange and improve the overall efficiency of public sector decision-making.
- **Enhancement of Proactive Public Services.** By leveraging integrated government data, public agencies can develop

proactive and citizen-centric services that anticipate public needs and deliver services more efficiently. This approach would strengthen the perceived value of digital government and reinforce citizens' confidence in public sector competence.

5.2 Strengthening Security and Privacy through Technical Verifiability

Digital trust must ultimately be grounded in verifiable technical mechanisms, rather than relying solely on regulatory compliance. Several policy directions are therefore recommended.

- Deployment of Advanced Cyber Defense Technologies. Government agencies should incorporate advanced technologies, including Artificial Intelligence (AI), to enhance early threat detection capabilities and improve responses to increasingly sophisticated cyber threats.
- Adoption of Privacy-Enhancing Technologies (PETs). The implementation of Privacy-Enhancing Technologies (PETs) and robust anonymization techniques within Open Government Data initiatives can help balance the dual objectives of administrative transparency and personal data protection.
- Transition toward Technical Verifiability. Policy frameworks should gradually move beyond a purely compliance-based approach toward a governance model in which security and data management practices are technically verifiable and transparent to the public.

5.3 Institutional Accountability and Proactive Human Capital Development

Human factors remain a central determinant in the development of digital trust within the public sector

- Strengthening Institutional Accountability. The government should institutionalize clear mechanisms for remediation, transparency, and compensation in

cases of data breaches or system failures. Moving beyond the minimum legal requirements of the Personal Data Protection Act (PDPA) and the Cybersecurity Act—enforced by the National Cyber Security Agency (NCSA)—would significantly reduce citizens' perceived risk and enhance long-term confidence in public institutions.

- Enhancing Digital Competence among Public Officials. Continuous investment in specialized training for public sector personnel is essential to strengthen expertise in data governance, data ethics, and cybersecurity standards. This capacity-building effort is critical for improving institutional integrity and ensuring that digital government services are delivered with high levels of security and accountability.
- Promoting Digital Intelligence among Citizens. National initiatives should focus on elevating citizens' Digital Intelligence (DQ), moving beyond basic digital literacy toward comprehensive cybersecurity awareness. Empowering individuals to protect their personal data and identify sophisticated online fraud will ultimately contribute to reducing the high levels of digital apprehension identified in this study.

6. Conclusion

Thailand's pursuit of a top-40 global digital government ranking represents not only a technological transformation but also a critical institutional challenge centered on public trust. Although Thailand has established significant legal and strategic frameworks for digital governance, a notable trust gap remains, driven by persistent cyber threats and concerns regarding personal data protection.

The findings of this study suggest that sustainable digital government adoption depends on the integration of robust data governance structures and resilient cybersecurity systems. Strengthening these two pillars can create a governance environment in which

digital systems are not only operationally effective but also socially trusted.

However, the findings also highlight a critical paradox—where high levels of policy confidence coexist with relatively low willingness to share personal data. This suggests that legal compliance alone is insufficient to fully establish citizen trust.

By addressing this paradox, the Thai government must move beyond compliance-based approaches toward a model grounded in technical verifiability and institutional accountability. Such a model, characterized by both operational transparency and verifiable system security, is essential for fostering a digital ecosystem that is not only technologically advanced but also meaningfully accepted by citizens.

References

- Aleisa N (2024) Digital governance and algorithmic transparency: Enhancing public trust through standardized security communication. *International Journal of Information Management*, 74: 102712
- Brezzi M, González S, Nguyen D, Prats M (2021) An updated OECD framework on drivers of trust in public institutions to meet current and future challenges. *OECD Working Papers on Public Governance*, 48
- Chakrothai N (2024) Factors affecting the awareness and use of cybersecurity technology according to the NCSC announcement. Master's thesis, Thammasat University
- Chanjaras P (2025) The role of the Thai government in regulating cybercrime: A mixed-methods study on socio-economic impacts in Bangkok. *Political Science and Public Administration Journal*, 16: 23–45
- Ciancarini P, Giancarlo R, Grimaudo G (2024) Digital transformation in the public administrations: A guided tour for computer scientists. *IEEE Access*, 12: 22841–22865
- Committee on Digital Government Development (2020) Announcement of the Digital Government Development Committee on government data governance. *Royal Gazette*, 137: 47–68
- Desrochers PR (2024) Access to information and privacy: Practical approaches for public service reform. *Canadian Public Administration*, 67: 102–118
- Digital Government Development Agency (2023) Thailand digital government development plan 2023–2027. Digital Government Development Agency
- Digital Government Development Agency (2025) Report on the results of the 2025 digital government readiness survey of government agencies (summary). Digital Government Development Agency
- Elayah M (2025) Transformative pathways in Qatar's e-government: Integrating societal engagement and NGO partnerships for sustainable digital governance. *Public Administration and Development*
- Forrester Research (2024) Global digital economy forecast, 2023 to 2028. Forrester Research
- Hasan A, Alenazy AA, Habib S, Husain S (2024) Examining the drivers and barriers to adoption of e-government services in Saudi Arabia. *Journal of Information and Data Technology Management*, 1: 139–160
- Kaeowisut S, Thongchana P (2025) Digital government and driving the Thai public sector in the digital age: Trends and challenges. *Journal of Narathiwat Rajanagarindra University Humanities and Social Sciences*, 13: 284–301
- Lehabal S (2024) Factors affecting the acceptance of the use of cybersecurity technology with artificial intelligence. Master's thesis, Thammasat University
- Kunchonchai P (2021) Factors affecting the effectiveness of data governance in Thai government agencies. *Journal of Information Technology and Management*, 7: 45–58

- Lao-rat C (2022) Models for digital organization transformation. *Payap University Journal*, 32: 173–187
- Nakonsong P, Jamratphan V (2022) Digital government transformation and future digital governance. *Journal of the Thai Association for Public Administration (Special Issue)*: 1–17
- National Cyber Security Commission (2026) Strategic plan for national cybersecurity 2024–2027. National Cyber Security Commission
- National Institute of Standards and Technology (2024) The NIST cybersecurity framework (CSF) 2.0. US Department of Commerce
- National Statistical Office (2026) GD catalog: Government data catalogue system. National Statistical Office
- Office of the National Economic and Social Development Council (2022) The 13th national economic and social development plan (2023–2027). Office of the National Economic and Social Development Council
- OECD (2020) The OECD digital government policy framework: Six dimensions of a digital government. *OECD Public Governance Policy Papers*, 2
- Preecha J (2025) Cybersecurity and public trust in digital governance: Focusing on citizen trust. *ICOSSH*, 2: 26–37
- Rajan R (2024) A modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Journal of Information Security and Applications*, 81: 103715
- Sirirattana W (2017) Governance: Powering the civil service 4.0. *Proceedings of the 4th National Academic Conference*: 160–168
- Songittisuk S (2019) Factors affecting the intention to use digital government services. *Journal of Business Administration*, 42: 12–28
- Tadsadornkulpat M (2025) Governance in the digital age: Challenges and opportunities for Thai public administration. *Journal of Social Studies, Religion and Culture*, 6: 388–401
- Thales (2025) 2025 Thales digital trust index: Understanding how digital experiences affect consumer trust. Thales
- United Nations Department of Economic and Social Affairs (2024) United Nations e-government survey 2024: Accelerating digital transformation for sustainable development with the addendum on artificial intelligence. United Nations
- World Bank Group (2022) Interoperability: Towards a data-driven public sector. World Bank Group
- World Economic Forum (2022) Earning digital trust: Decision-making for trustworthy technologies. World Economic Forum
- Wylde V, Rawindaran N, Lawrence J, Balasubramanian R, Prakash E, Jayal A, Khan I, Hewage C, Platts J (2022) Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, 3: 127
- Yonghuay S, Tabtieng T (2019) Digital trust and technology acceptance: A case study of government e-services. *Journal of Digital Science and Innovation*, 2: 89–104
- Zyoud SH, Lutfi A (2024) Global research trends in digital governance: A bibliometric analysis. *Governance*, 37: 456–478