世界互联网大会 World Internet Conference

中国式现代化研究院 INSTITUTE OF CHINESE PATH TO MODERNIZATION

Outcomes of World Internet Conference Think Tank Cooperation Program

Report on the Evaluation Indicator Framework of Digital-intelligence Government Governance

Authoring Unit

Nankai University Institute of Chinese Path to Modernization

Nankai University Research Center for Cyber Society Governance

APRIL 2026


世界互联网大会
World Internet
Conference


中国式现代化发展研究院
INSTITUTE OF CHINESE PATH TO MODERNIZATION

Writing Group

Leader

Fang Wang — Professor, School of Information and Communication, Nankai University; Director, Center for Network Society Governance, Nankai University

Key members

Meiquan Wang — Doctoral Student, School of Information and Communication, Nankai University

Xuekun Zhu — Doctoral Student, School of Information and Communication, Nankai University

Xinyue Zhang — Doctoral Student, School of Information and Communication, Nankai University

Email: 1120231398@mail.nankai.edu.cn

Foreword

With artificial intelligence as a representative of the new generation of digital technologies, global society is rapidly entering a more intelligent stage of development. AI is increasingly regarded as a key driver of a new wave of technological transformation and governance change. As AI technologies continue to mature and strategies for Digital-intelligence governance advance, algorithmic models, computing infrastructure, and data resources are increasingly integrated into social governance and public service delivery. At the international level, the United Nations has incorporated digital public infrastructure and AI governance into the global cooperation framework through the Global Digital Compact. The European Union has successively introduced the Digital Decade Policy Programme 2030 and the Artificial Intelligence Act, while international organizations such as the OECD and the World Bank continue to promote policy frameworks related to data governance, GovTech development, and digital transformation of the public sector. Against this backdrop, major economies around the world are exploring institutional arrangements and governance practices for applying emerging technologies in government governance, and governance practices are gradually evolving from traditional digital government development toward Digital-intelligence governance.

However, as Digital-intelligence transformation accelerates, government governance capabilities face a set of emerging systemic challenges. First, a significant time gap persists between technological innovation and institutional adaptation. As algorithmic systems become embedded in decision-making, regulation, and public service processes, mechanisms for transparency, accountability, and human oversight must be strengthened in parallel. Second, the nature of governance risks is becoming more complex. Issues once centered on data sharing and privacy protection are now extending to challenges such as model interpretability, algorithmic bias, and the credibility of AI-generated content, placing higher demands on governance reliability and legitimacy. Third, countries differ substantially in digital infrastructure, institutional capacity, and the depth of technology adoption, resulting in uneven governance capability structures that may affect policy implementation and exacerbate digital divides. Most existing digital government evaluation systems focus primarily on the level of online services or the breadth of technology deployment, making it difficult to fully capture the actual state of government governance in an emerging intelligent society.

Against this background, this report proposes an Evaluation Indicator Framework of Digital-intelligence Government Governance. Centered on the identification of governance capabilities, the framework is structured around four primary dimensions: Digital-intelligence Social Governance, Digital-intelligence Public Service Delivery, Institutional and Infrastructure Support, and Digital-intelligence Public Participation. The framework systematically characterizes the capability structure and operational state of governments undergoing Digital-intelligence transformation. It provides a comparable and adaptable tool for assessing governance capabilities and offers a structured reference framework to countries seeking to advance digital government development in the context of an emerging intelligent society.

Contents

Ⅰ、Global Trends in Digital-intelligence Governance

（Ⅰ）The Evolution of Digital Government Toward Intelligent Governance

The development of digital government worldwide shows clear stage-based characteristics. Assessments of 193 United Nations member states indicate that the coverage of digital public services continues to expand, while significant differences remain in infrastructure, data governance capability, and institutional support. As a result, the digital transformation process remains uneven across countries [1]. This suggests that the evolution of digital government is not a linear transition but a gradual process shaped by different development foundations.

In the early stage, the primary focus lies in the digitization of administrative processes and the online provision of government services. Governments improve accessibility and administrative efficiency by establishing unified portals, electronic filing systems, and online service platforms. At this stage, digital technologies mainly serve as tools to optimize existing administrative processes. The United Nations evaluates e-government development through the Online Service Index, Telecommunication Infrastructure Index, and Human Capital Index, emphasizing that these three elements jointly form the foundation of digital government. Similarly, the World Bank's GovTech Maturity Index (GTMI) identifies "core government systems and shared digital infrastructure" as key evaluation areas, noting that the robustness of foundational systems directly affects subsequent integration capabilities[2]. At this stage, goverance structures do not fundamentally change, and improvements are mainly reflected in service delivery and administrative efficiency.

As digital infrastructure improves, government operations enter a new phase characterized by data integration and data sharing. The OECD argues that data should be treated as a strategic asset of the public sector and that institutional arrangements should promote cross-agency sharing and reuse of data to support policy design, service improvement, and performance evaluation [3]. The 2023 OECD Digital Government Index further identifies the "Data-driven public sector" as a key dimension, highlighting the importance of data governance rules, interoperability mechanisms, and data quality management [3]. In this phase, government decision-making and public service delivery increasingly rely on data monitoring and analytical tools. Transparency and measurability improve, while ultimate outcomes responsibility remains with human administrative actors.

In recent years, the maturity of artificial intelligence technologies has led some countries to explore AI-assisted applications in specific governance scenarios. Applications such as risk identification, trend forecasting, resource allocation, and intelligent customer services are gradually expanding, while generally emphasizing support for rather than replacement of human decision-making. The G7 Toolkit for Artificial Intelligence in the Public Sector, jointly released by the OECD and UNESCO, notes that when AI is integrated into government systems, institutional and capacity development must be strengthened simultaneously. The public sector must establish governance frameworks that ensure safety, reliability, and accountability, translating ethical principles into operational rules [4]. Globally, intelligent applications remain unevenly distributed and largely scenario-specific, and their development is closely linked to existing levels of data governance capacity and institutional maturity.

[1] United Nations Department of Economic and Social Affairs. UN E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development – With the addendum on Artificial Intelligence[R]. New York: United Nations, 2024.
[2] World Bank. GovTech Maturity Index (GTMI): The State of Public Sector Digital Transformation[R]. Washington, D.C.: World Bank, 2022.
[3] OECD. 2023 OECD Digital Government Index: Results and Key Findings[R]. Paris: OECD Publishing, 2024.
[4] OECD/UNESCO. G7 Toolkit for Artificial Intelligence in the Public Sector[R]. Paris: OECD Publishing, 2024.

(II) Institutional Approaches of International Organizations and Major Economies

A notable feature of current international practices in Digital-intelligence governance is that digitalization is no longer treated as a single technological reform. Instead, institutional tools are increasingly used to reshape the organizational arrangements and responsibility structures of government operations. This institutional shift has gradually moved Digital-intelligence governance from policy initiatives toward a stage in which rules, evaluation mechanisms, and implementation systems operate in parallel.

At the level of international organizations, the United Nations has integrated digital issues into the global governance system through agenda coordination. The Global Digital Compact explicitly places digital cooperation, data governance, and AI governance on the agenda of multilateral cooperation[1]. This arrangement does not directly prescribe technical standards; rather, it generates sustained policy pressure through political commitments and multilateral consensus. As a result, issues such as the digital divide, capability gaps, and risks associated with artificial intelligence have become long-term topics of international negotiation. Meanwhile, the periodic publication of the UN E-Government Survey provides a continuous monitoring tool, allowing differences in development levels and governance capacities to be systematically measured. In essence, the UN approach links Digital-intelligence governance with both development agendas and rights-based agendas, creating sustained institutional attention.

The institutional innovation of the OECD lies in conceptualizing digital government development as a governance capability framework that can be compared and

Table 1 Major Institutional Instruments of the United Nations

Institutional Instrument	Document / Policy	Year	Institutional Focus	Implementation Approach
UN E-Government Survey	UN E-Government Survey	Biennial	Development gaps and governance capacity assessment	Global monitoring
Global Digital Compact	Global Digital Compact	2024	Multilateral framework for digital cooperation and AI governance	Adopted at UN Summit
Pact for the Future	Pact for the Future	2024	Integration of digital issues into the global governance agenda	Political commitment
AI Advisory Body Report	Governing AI for Humanity	2024	Global AI governance initiatives	Advisory mechanism
Integration of SDGs and Digital Transformation	Digital for SDGs Initiative	Ongoing	Digital development and sustainable development	Development framework

[1] United Nations. Global Digital Compact[R/OL]. 2024.

evaluated across countries. Its Digital Government Policy Framework identifies six dimensions, including digital-by-design, a data-driven public sector, and government as a platform[1]. The key significance of this framework is that it shifts the focus of digital transformation from whether individual departmental projects are online to whether governments have established mechanisms for coordination, data sharing, and the allocation of responsibilities. When participating in assessments and peer reviews, member countries are therefore required not only to report progress in technological development but also to explain arrangements for institutional coordination and data governance. In this way, Digital-intelligence governance becomes embedded within broader public management reforms.

The World Bank advances digital transformation primarily through maturity assessments and project-based support, breaking reform into phased and implementable tasks. The GovTech Maturity Index covers nearly 200 economies and aims to identify structural gaps in government capabilities across core systems, online service delivery, citizen engagement, and institutional support[2]. Unlike a simple ranking exercise, the index is used to support policy dialogue and financing decisions, thereby translating assessment results directly into reform priorities. In recent years, the World Bank has further proposed the concept of Digital Public Infrastructure (DPI), emphasizing that digital identity systems, payment platforms, and data exchange mecha-

Table 2 Major Institutional Instruments of the OECD

Institutional Instrument	Document / Policy	Year	Institutional Focus	Implementation Approach
Recommendation on Digital Government Strategies	Recommendation of the Council on Digital Government Strategies	2014	Whole-of-government digital transformation principles, coordination, and capacity building	Council recommendation guiding member state policy alignment
Data-Driven Public Sector Report	The Path to Becoming a Data-Driven Public Sector	2019	Data as a strategic asset for the public sector	Policy guidance
OECD AI Principles	OECD Principles on Artificial Intelligence	2019	Trustworthy AI, accountability, and transparency	Principles adopted by member countries
Digital Government Policy Framework (DGPF)	OECD Digital Government Policy Framework	2020	Six-dimensional governance capability structure (digital-by-design, data-driven government, etc.)	Framework-based assessment and peer review
Digital Government Index (DGI)	OECD Digital Government Index	2023 / 2025	Quantified comparison of digital government maturity	Indicator-based measurement
G7 AI Toolkit (with UNESCO)	G7 Toolkit for Artificial Intelligence in the Public Sector	2024	AI risk management in the public sector	Practical policy toolkit

[1] OECD. The OECD Digital Government Policy Framework: Six dimensions of a Digital Government[R]. Paris: OECD Publishing, 2020.
[2] World Bank. GovTech Maturity Index, 2022 Update[R]. Washington, D.C.: World Bank, 2022.

nisms constitute the foundational architecture of digital service delivery[1].

Table 3 Major Institutional Instruments of the World Bank

Institutional Instrument	Document / Policy	Year	Institutional Focus	Implementation Approach
GovTech Maturity Index (GTMI)	GovTech Maturity Index	2020 / 2022 / 2025	Maturity-based diagnostic assessment of digital government development	Indicator-based evaluation
GovTech Global Partnership (GGP)	GovTech Global Partnership	Ongoing	Policy dialogue and capacity building for digital government reform	Program and project support
Digital Public Infrastructure Framework	Digital Public Infrastructure (DPI) Approach	2024 / 2025	Digital identity, digital payments, and data exchange systems	Foundational infrastructure framework

The European Union has adopted a coordination path driven by legal and regulatory frameworks. The Digital Decade Policy Programme 2030 establishes common targets and monitoring mechanisms, providing member states with a shared progress framework. Building on this foundation, the Interoperable Europe Act clarifies the responsibilities of member states in the design of cross-border digital public services and data exchange, while establishing coordination and evaluation mechanisms[2], Through legislative instruments, the EU further defines the implementation mechanisms and cooperation requirements for public sector interoperability, bringing related objectives into an institutionalized stage of implementation. As a result, interoperability is elevated from a technical standards issue to a legal obligation.

Table 4 Major Institutional Instruments of the European Union

Institutional Instrument	Document / Policy	Year	Institutional Focus	Implementation Approach
Digital Decade Policy Programme	Digital Decade Policy Programme 2030	2022	Targets for digital public services and digital transformation	Monitoring and coordination mechanism
Data Governance Ac	Data Governance Act	2022	intermediaries and data-sharing mechanisms	Regulatory framework

[1] World Bank Group. Digital Public Infrastructure and Development: A World Bank Group Approach[R]. 2025.
[2] European Parliament and the Council. Regulation (EU) 2024/903 (Interoperable Europe Act)[S]. 2024.

Institutional Instrument	Document / Policy	Year	Institutional Focus	Implementation Approach
Data Act	Data Act	2023	Data access and data usage rights	Legislative regulation
Interoperable Europe Act	Interoperable Europe Act	2024	Cross-border interoperability of public services	Legal obligation
Artificial Intelligence Act	Artificial Intelligence Act (AI Act)	2024	Risk-based regulation of artificial intelligence systems	Unified regulatory framework
European Digital Identity Framework	eIDAS Regulation (revised)	2014 / 2024 revision	Cross-border electronic identification and trust services	Legal framework

The institutional pathway of the United States is characterized by embedding digital service experience and data governance capabilities into compliance requirements through legislation and administrative regulations. The 21st Century Integrated Digital Experience Act requires federal agencies to improve the quality of websites and digital services, and authorizes the Office of Management and Budget to issue implementation guidance, thereby making improvements in user experience a statutory responsibility[1]. At the same time, the Foundations for Evidence-Based Policymaking Act establishes an institutional framework for federal data management and open data, making the use of data to improve policymaking a cross-agency obligation[2]. In the area of AI risk governance, the National Institute of Standards and Technology (NIST) has issued the AI Risk Management Framework (AI RMF 1.0), providing a unified risk management structure for both public sector institutions and enterprises[3]. This pathway emphasizes the combination of legal instruments and technical standards to stabilize the responsibility boundaries of Digital-intelligence governance.

Table 5 Major Institutional Instruments of the United States

Institutional Instrument	Document / Policy	Year	Institutional Focus	Implementation Approach
21st Century IDEA Act	21st Century Integrated Digital Experience Act (Public Law 115-336)	2018	Digital service experience and modernization of federal websites	Federal legislation
Evidence Act	Foundations for Evidence-Based Policymaking Act (Public Law 115-435)	2019	Data governance and evidence-based policymaking capacity	Federal legislation

[1] United States Congress. 21st Century Integrated Digital Experience Act (Public Law 115-336)[S]. 2018.
[2] United States Congress. Foundations for Evidence-Based Policymaking Act (Public Law 115-435)[S]. 2019.
[3] NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0)[R]. 2023.

Institutional Instrument	Document / Policy	Year	Institutional Focus	Implementation Approach
Federal Data Strategy	Federal Data Strategy	2020	Data asset management and federal data governance	Strategic framework
NIST AI Risk Management Framework	Artificial Intelligence Risk Management Framework (AI RMF 1.0)	2023	AI risk management structure	Technical standard
Executive Order 14110	Executive Order on Safe Secure, and Trustworthy Artificial Intelligence	2023	Safe and trustworthy AI governance	Executive order
OMB AI Guidance (M-24-10)	OMB Memorandum M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of AI	2024	Federal AI governance and oversight	Administrative guidance

In many Asia-Pacific countries, integration capacity is strengthened through central coordination mechanisms and national-level implementation programs. As the intelligent society continues to evolve, China's policy orientation places greater emphasis on the coordination between technological development and governance reform. Through initiatives such as national AI programs, standardization guidelines for the intelligent society, and regulations on government data sharing, China promotes the application of intelligent technologies alongside improvements in foundational data governance and market-oriented data allocation mechanisms.

Singapore's Digital Government Blueprint proposes the use of shared digital platforms and a unified digital identity system to support cross-agency service integration, emphasizing centralized capability development to reduce duplicated system construction[1], Japan's Digital Agency has released the Priority Plan for the Advancement of a Digital Society, which sets cross-ministerial reform tasks and timelines through annual priority plans, with cabinet approval used to strengthen implementation authority [2]. Taken together, these practices point to a common governance logic: digital transformation requires sustained coordination in organizational structures and implementation mechanisms, rather than relying solely on technological innovation.

[1] Government of Singapore. Digital Government Blueprint[R]. 2020.
[2] Digital Agency (Japan). Priority Plan for the Advancement of a Digital Society[R]. 2025.

Table 6 Major Institutional Instruments in Asia–Pacific Countries

Country	Institutional Instrument Type	Policy / Document	Year	Institutional Focus	Implementation Approach
	National Strategic Plan	Overall Layout Plan for the Development of Digital China	2023	Integrated development of digital government, digital infrastructure, and data resource systems	Central strategic planningand coordinated implementation
	Administrative Regulation	Regulation on the Sharing of Government Data	2025	National integrated governmentbig data system, data-sharing responsibilities, and security boundaries	State Council regulation
China	Data Institutional Reform	Key Tasks for Building Basic Data Institutions and Better Leveraging Data Elements (2025)	2025	Data property rights, authorization mechanisms, and data circulation	Annual policy agendaof the National Data Administration
	National AI Initiative	Opinions on Deepening the Implementation of the “AI+” Action	2025	Integration of artificial intelligence into government and governance systems	State Council special initiative
	Standardization Framework	Standardization Guidelines for the Development and Governance of the Intelligent Society (2025 Edition)	2025	Standards for intelligent application scenarios and social impact assessment indicators	National standardization guidance
	National Blueprint	Digital Government Blueprint	2020	Shared digital capabilitie and user-centric service integration	National strategic blueprint
Singapore	National Digital Strategy	Smart Nation Initiative	Ongoing	Digital infrastructure and smart city development	Coordinated by the Prime Minister’ s Office
	Digital Identity System	National Digital Identity (NDI)	2018	Unified digital identity authentication and authorization system	National digital platform
Japan	Institutional Reform	Establishment of the Digital Agency	2021	Cross-ministerial coordination of digital transformation	Cabinet-level institution
	National Policy Plan	Priority Plan for the Advancement of a Digital Society (2025 Edition)	2025	Annual priorities and cross-ministerial digital reform	Cabinet-approved national plan
		.....			

International organizations and major economies have adopted three complementary institutional approaches. These include shaping policy directions through evaluation frameworks, clarifying responsibility boundaries through legal and regulatory rules, and promoting phased capability development through implementation programs and maturity assessment tools. These approaches indicate that Digital-intelligence governance has moved beyond the stage of technological deployment and entered a phase of continuous institutional adjustment. The central challenge is no longer the adoption of new technologies, but how to establish stable and sustainable operational mechanisms within existing administrative systems.

(III) Common Trends in the Development of Digital-intelligence Governance

The development of Digital-intelligence governance is not merely the renewal of technological tools, but a transformation in the operating logic of governance structures. The transition from the digital stage to the Digital-intelligence stage is characterized not by the increase in the number of systems, but by the restructuring of institutional arrangements and operational modes. In the early phase of digital government, information systems mainly served functions such as process optimization and efficiency improvement. Their role was to embed technical solutions into existing administrative structures and modify existing procedures. In the current stage, however, institutional frameworks built around data sharing, interoperability rules, and algorithm governance are increasingly reshaping the ways in which administrative systems themselves operate.

This structural shift is first reflected in changes in the allocation of responsibilities. The deployment of Digital-intelligence systems is no longer treated as a purely technical decision, but is increasingly incorporated into compliance review and risk assessment frameworks. The focus of governance is shifting from ex-post supervision to ex-ante review, and from accountability for operational outcomes to the prior design of institutional conditions. The digital decision-making process itself has become a matter requiring justification, documentation, and continuous evaluation. As a result, responsibility moves forward from the implementation stage to the design stage, and the logic and sequencing of governance is adjusted accordingly.

The institutional position of data within governance structures has significantly risen. Data is no longer treated merely as a subsidiary resource of individual departments. Instead, an independent institutional framework is gradually forming around issues such as ownership definition, access rules, data-sharing obligations, and security responsibilities. Data is increasingly treated as an object of governance that requires dedicated rules for allocation, sharing, and accountability. This shift implies that part of administrative authority is reorganized within data governance frameworks, and the boundaries between government departments increasingly shift from technical interfaces to institutional boundaries.

The evaluation of public services is undergoing transformation. In the early stage of digitalization, emphasis was placed on system coverage and the launch of online service channels. In the Digital-intelligence stage, however, evaluation increasingly focuses on operational quality, service consistency, and process verifiability. Digital services are no longer supplementary functions but basic operational conditions, and service experience

and responsiveness are gradually incorporated into compliance requirements. Governance evaluation therefore shifts from a construction-oriented approach to a performance-oriented one. At the same time, the introduction of artificial intelligence raises institutional requirements for transparency, explainability, and security. Technological authority is no longer based solely on administrative discretion but is incorporated into continuous supervision and risk control frameworks. Digital-intelligence governance thus presents a clear characteristic: the expansion of technological capabilities occurs simultaneously with the strengthening of institutional constraints, together forming a new operational structure.

At the same time, inclusiveness is gradually becoming an important component of the institutional structure of Digital-intelligence governance. Within this framework, issues such as fairness, accessibility, and diverse participation are receiving increasing attention. Inclusiveness is no longer only a development goal or policy slogan, but is increasingly translated into institutional design and operational rules. The deployment of technology, data collection practices, and modes of public service delivery must respond institutionally to differences in social conditions and capability structures. This transformation does not manifest as a single policy measure but as a structural adjustment in governance values. While pursuing efficiency and capability expansion, governance systems increasingly incorporate fairness and universality as inherent conditions of institutional operation.

II、Challenges Facing Digital-intelligence Government Governance

(Ⅰ) Alignment Between the Technical Infrastructure and Data Systems

As platform architectures become largely established, the focus of digital government development is gradually shifting toward the alignment of foundational technological infrastructure with evolving governance needs. Fragmented legacy systems, inconsistent data standards, and limited visibility over technology assets and associated risks create persistent pressures on the large-scale deployment of data-driven governance and artificial intelligence applications. In this context, some innovative projects are able to operate effectively in specific scenarios, yet when extended across departments or regions, they often encounter rising costs and increasing coordination complexity, leading to differentiated expansion pathways.

In countries where public audit evidence is relatively comprehensive, legacy systems are widely regarded as a key structural constraint on the expansion of data and AI capabilities in the public sector. The United Kingdom has reported that many critical public services still rely on legacy technologies developed decades ago, with the proportion of legacy systems in central government departments estimated at about 28% in 2024. In sectors such as policing and the National Health Service (NHS), the share of legacy systems varies more widely, in some cases reaching 60–70%[1]. The review further notes that legacy systems not only increase maintenance costs but also reduce service reliability and expand the attack surface. Similarly, a 2025 review by the U.S. Government Accountability Office (GAO) on federal legacy IT modernization highlights that a large share of federal IT spending continues to be devoted to operating and maintaining existing systems. These legacy systems are costly

[1] Department for Science, Innovation and Technology; Government Digital Service. State of Digital Government Review[R/OL]. London: GOV.UK, 2025-01-21[2026-02-12].https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review

and more vulnerable to cybersecurity risks, while modernization efforts remain an ongoing process of adjustment[1]. One of the core challenges associated with legacy systems is the lack of transparency regarding assets and technical knowledge. Legacy infrastructures often lack maintenance documentation, rely on increasingly scarce technical skills, and are not centrally recorded. As a result, organizations face difficulties in comprehensively assessing system availability, compatibility, and security conditions, which in turn generates long-term operational pressure on budgets and personnel allocation.

Another manifestation of the mismatch between technical infrastructures and data systems is that data may exist but remain unusable. Comprehensive studies on public sector data governance indicate that existing frameworks often operate under conditions of institutional fragmentation, dispersed data ownership, inconsistent standards, and ambiguous regulatory responsibilities. These factors limit the effective management and reuse of data as a strategic asset[2][3]. Fragmented data assets increase the cost of integration, reduce the efficiency of data sharing, and weaken trust foundations, ultimately constraining the large-scale application of data-driven analysis and intelligent tools in policy-making and public service optimization.

Similarly, OECD empirical analyses on the strategic use of AI in government show that many public sector AI projects are constrained by limited access to high-quality and shareable data, as well as insufficient cross-agency data-sharing mechanisms. In practice, these constraints slow the transition of AI systems from pilot experimentation to large-scale deployment and place greater demands on consistent data governance across institutions[4].

(II) Institutional Accommodation of Intelligent Technologies in Governance Processes

After intelligent systems enter public decision-making and service processes, evaluation frameworks, responsibility allocation, and oversight mechanisms in some economies remain under continuous development, which to some extent affects the pace of large-scale deployment. Several international assessments indicate that although the number of public sector AI projects continues to increase, many still remain at the stages of exploration, pilot testing, or limited deployment, and pathways toward scaling remain unstable. Governments commonly face difficulties in establishing consistent measurement standards when promoting AI applications, lacking unified indicators to evaluate cost savings, service improvements, or risk management outcomes. This situation raises higher requirements for decisions on sustained investment and broader deployment[5]. In the absence of comparable and verifiable evaluation systems, AI projects often remain localized experiments, and scaling pathways tend to progress in stages[6].

When algorithms participate in administrative decision-making, the identification of responsible actors

[1] U.S. Government Accountability Office. Agencies Need to Plan for Modernizing Critical Decades-Old Legacy IT Systems (GAO-25-107795) [R/OL]. 2025-07-17[2026-02-12].https://files.gao.gov/reports/GAO-25-107795/index.html
[2] OECD. Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions[R/OL]. Paris: OECD Publishing, 2025-09-18[2026-02-26].https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html.
[3] OECD. The Path to Becoming a DataDriven Public Sector[R/OL]. Paris:OECD Publishing, 2019-11-28[2026-02-27].https://www.oecd.org/en/publications/the-path-to-becoming-a-Datadriven-public-sector_059814a7-en.html.
[4] OECD. “Implementation Challenges that Hinder the Strategic Use of AI in Government” [EB/OL]. 2025-09-18[2026-02-12]. https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report/implementation-challenges-that-hinder-the-strategic-use-of-ai-in-government_05cfe2bb.html
[5] OECD. Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions[R/OL]. Paris: OECD Publishing, 2025-09-18[2026-02-27].https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html.
[6] United Nations System. United Nations System White Paper on AI Governance: An Analysis of the UN System’ s Institutional Models, Functions, and Existing International Normative Frameworks Applicable to AI Governance[R/OL]. New York: United

becomes more complex. Decision outcomes may be influenced by multiple factors, including data sources, model design, and human review. In such contexts, responsibility allocation becomes increasingly complicated. The European Data Protection Board has noted that when public institutions use algorithmic systems, they must clearly define the responsibilities of data controllers and processors and ensure traceable decision pathways; otherwise, requirements for legality and accountability may not be satisfied[1]. Similarly, the European Union emphasizes that high-risk AI systems must include mechanisms for traceability and human oversight[2]. Where responsibility boundaries and human-machine role divisions remain unclear, some institutions adopt more cautious strategies when applying AI in high-impact decision contexts, resulting in a gradual approach to expanding applications.

The effective operation of intelligent technologies also depends on data quality, process redesign, and personnel capabilities. The International Monetary Fund notes that as governments advance digital and intelligent reforms, the complexity of organizational capacity building becomes increasingly evident, particularly in the coordination between data governance capabilities and cross-agency mechanisms [3]. In addition, the World Bank finds that in many public sector digital transformation initiatives, the introduction of new technologies without parallel process redesign and personnel training often results in limited efficiency gains or even new administrative burdens[4]. These observations indicate that the institutionalization of intelligent systems depends not only on model feasibility but also on their alignment with institutional absorption capacity. When organizational structures and capability development remain in transition, the institutional integration of intelligent systems typically proceeds in a gradual manner.

(III) Transformation of Risk Structures in Digital-intelligence Governance

When data and models become important inputs for public governance, the structure of risks begins to exhibit multidimensional characteristics. The first category is availability risk, which arises when cyberattacks or system failures interrupt critical services and affect the continuity of public administration and public service delivery[5]. The second category is integrity risk, referring to situations in which data or content is corrupted, manipulated, or affected by systemic bias and subsequently enters decision-making processes[6]. The third category is traceability risk, which emerges when multi-source data, algorithmic components, and external vendors jointly participate in governance systems. In such contexts, the complexity of responsibility attribution and evidence reconstruction increases significantly, requiring clearer institutional arrangements to support accountability chains[7]. This structural shift indicates

[1] European Data Protection Board (EDPB). Guidelines on automated decision-making and profiling for the purposes of Regulation 2016/679[EB/OL]. Brussels, 2023[2026-02-12]. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en
[2] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)[S/OL]. Brussels: Official Journal of the European Union, 2024-07-12[2026-02-27].https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
[3] International Monetary Fund. Transforming Public Finance through GovTech[R/OL]. Washington, D.C.: IMF, 2023-09-06[2026-02-27]. https://www.imf.org/en/publications/staff-discussion-notes/issues/2023/09/06/transforming-public-finance-through-govtech-535765
[4] World Bank. GovTech Maturity Index 2025: Tracking Public Sector Digital Transformation Worldwide[R/OL]. Washington, D.C.: World Bank,2025-12-17[2026-02-27].https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099121725193511608.
[5] International Organization for Standardization. Information technology—Security techniques—Information security management systems—Requirements: ISO/IEC 27001:2022[S]. Geneva: ISO, 2022.
[6] International Organization for Standardization. Information technology—Security techniques—Information security risk management: ISO/IEC 27005:2022[S]. Geneva: ISO, 2022.
[7] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0)[R]. Gaithersburg: NIST, 2023.

that risk governance is gradually moving beyond the improvement of data quality alone toward a broader focus on ensuring service continuity and establishing auditable mechanisms throughout the entire governance process.

In recent years, pressures on cyber resilience in the public sector have increased globally. Public administrative systems and critical infrastructures in multiple countries have experienced ransomware attacks and other cyber incidents, making service continuity and information security central concerns. In the European Union, sectors such as public administration, transport, finance, and digital infrastructure have been incorporated into stricter cybersecurity and information security obligation frameworks. These frameworks emphasize cross-border coordination and the protection of critical services[1]. In the United States, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) promotes the establishment of a unified reporting mechanism for major cyber incidents, requiring critical entities to report incidents within specified timeframes and disclose ransom payments when applicable[2]. These developments illustrate a broader institutional trend toward improving risk visibility and response mechanisms for critical infrastructure.

The widespread adoption of generative artificial intelligence further reshapes the risk landscape. When training data, retrieval corpora, or external knowledge bases contain unreliable or manipulated information, model outputs may carry implicit biases. When such outputs are directly used in document drafting, analytical assessments, or decision-support processes, errors may shift from reference information to governance inputs. In this context, risk management is gradually evolving from single-point control toward full-process arrangements that cover data sources, the use of model outputs, continuous monitoring, and incident response mechanisms. The AI Risk Management Framework released by the U.S. National Institute of Standards and Technology proposes a structured approach centered on governance, risk identification, measurement, and risk management, providing an operational pathway for embedding risk control throughout the lifecycle of AI systems in the public sector[3].

When AI systems are embedded in public sector operational processes, transparency, traceability, and explainability increasingly become essential conditions for institutional operation. Risks no longer arise solely from technical misjudgments but also from potential rights violations, amplified biases, and the erosion of public trust caused by opaque decision processes. As a result, public oversight institutions and citizens increasingly demand greater transparency and clearer accountability structures. The ISO/IEC 42001 Artificial Intelligence Management System Standard proposes the establishment of systematic management and documentation mechanisms to enhance transparency, reliability, and traceability[4]. In public sector contexts, this implies that responsibility chains must be embedded within technological chains, ensuring that data sources, model versions, system calls, and references can be reconstructed, thereby supporting continuous oversight and institutional accountability.

[1] Directive (EU) 2022/2555. NIS2 Directive, Article 23 Reporting obligations [EB/OL].(2022-12-27)[2026-02-12].https://nis2resources.eu/directive-2022-2555-nis2/article-23/
[2] Cybersecurity and Infrastructure Security Agency (CISA). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) [EB/OL].[2026-02-12].https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia?os=wtmb5utkcxk5refappamp_kit%3D1
[3] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0)[EB/OL]. (2023-01-26)[2026-02-12].https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10
[4] International Organization for Standardization. ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system[S]. 2023.

(IV) Diverging Accessibility in Digital-intelligence Public Services

In the context of Digital-intelligence transformation, public service systems widely pursue process optimization and efficiency improvement through online and intelligent service channels. As digital channels become embedded in service delivery processes, the focus of attention gradually shifts from whether digital entry points exist to whether services effectively reach groups that face disadvantages in accessing public services. The accessibility issue is therefore moving from coverage indicators toward questions of actual accessibility, increasingly intersecting with the expansion of AI applications.

Global connectivity gaps remain a key structural variable affecting the advancement of Digital-intelligence public services. The United Nations Broadband Commission reports that approximately one-third of the world's population still lacks internet access, with higher risks of disconnection in low-income countries and among vulnerable groups[1]. This indicates that before discussing the intelligent transformation of digital public services, connectivity conditions themselves remain a fundamental determinant of accessibility.

On this basis, artificial intelligence may further influence service disparities in structural ways. OECD policy analysis on the use of AI in government notes that public sector AI systems may amplify existing digital divides due to data bias, capability differences, or algorithm design issues, thereby worsening disadvantages for vulnerable populations[2]. Relevant policy documents further emphasize that governments should incorporate inclusiveness and fairness into risk assessment frameworks when deploying AI, rather than treating them solely as social welfare issues[3]. These developments suggest that accessibility is increasingly emerging as a key variable in Digital-intelligence governance structures, alongside data security and system stability.

As public service systems continue to shift toward online channels, the weakening of offline service capacity has become a structural concern in several countries. Evaluations of digital government transformation in multiple jurisdictions note that if resource allocation and performance assessment rely excessively on digital channels, offline service counters, telephone support, and community service networks may be reduced. This may increase the cost of accessing services for individuals with limited digital skills or unstable internet connectivity. The UK National Audit Office has emphasized that when governments promote digital-by-default strategies, alternative service channels must remain accessible; otherwise, vulnerable groups may face difficulties obtaining essential public services[4]. Similar discussions appear in European Union policy documents on digital inclusion, which highlight the importance of maintaining multi-channel service provision to ensure fairness[5].

The focus of digital public service evaluation is therefore gradually shifting from coverage indicators toward actual accessibility. Connectivity conditions, capability structures, and service channel arrangements together determine whether services truly reach their intended users. As artificial intelligence becomes further embedded in public sector operations, if accessibility consider-

[1] Broadband Commission for Sustainable Development. The State of Broadband 2024: Leveraging AI for Universal Connectivity [R]. Geneva: ITU & UNESCO, 2024.
[2] OECD. AI and the Future of Social Protection in OECD Countries[R/OL]. Paris: OECD Publishing, 2025-06-19[2026-02-27].https://www.oecd.org/en/publications/ai-and-the-future-of-social-protection-in-oecd-countries_7b245f7e-en.html.
[3] OECD. AI in the Public Sector: Opportunities and Challenges [R]. Paris: OECD Publishing, 2023.
[4] National Audit Office (UK). Digital Transformation in Government: Addressing the Barriers to Success [R]. London: NAO, 2023.
[5] European Commission. 2030 Digital Compass: the European way for the Digital Decade [R]. Brussels: European Commission, 2021.

ations are not incorporated into institutional arrangements and risk management frameworks, existing inequalities may persist under new technological conditions. Consequently, governance frameworks need to incorporate accessibility into institutional design and risk governance through connectivity support, capability development, and diversified service provision, ensuring that Digital-intelligence transformation does not weaken the fairness foundations of public services.

III、Structure of the Evaluation Indicator Framework for Digital-intelligence Government Governance

The challenges facing current governance systems are not concentrated in a single technological domain but unfold along the structure of governance operations. The degree of alignment between technical infrastructure and data systems constitutes the basic conditions for governance operation. The clarity of institutional absorption and responsibility allocation determines whether intelligent technologies can be embedded into core administrative processes. On this basis, the accumulation of new risk forms makes security and trustworthiness key variables for stable governance operations. At the same time, differences in public service provision and participation structures translate these capability gaps into concrete public experiences.

As governance divergence increasingly manifests as differences in capability structures, evaluation frameworks also need to shift toward a capability-oriented logic. The construction and refinement of the indicator framework are therefore developed in response to these structural changes in governance operations. The framework is organized around four key capability dimensions within governance systems: social governance responsiveness, public service operational capability, institutional and infrastructural support capability, and public participation integration capability. By structuring these four capability areas, the indicator framework integrates diverse governance outcomes into a unified analytical structure.

(I)Principles for Indicator Construction

The construction of the indicator framework follows four principles: relevance, value orientation, operability, and adaptability. Indicators are selected and designed to reflect evaluation objectives, evaluation subjects, and the evolving requirements of governance development, thereby forming an evaluation indicator framework for Digital-intelligence Government Governance that aligns with global development trends.

Relevance principle. Indicators should correspond to specific evaluation objects and objectives, accurately describing the characteristics of the system under evaluation. They should cover essential aspects of the evaluation subject while also reflecting its distinctive attributes. Selected indicators should therefore be able to clearly distinguish the evaluated system from other governance contexts.

Value-orientation principle. The ultimate objective of government governance is the realization of social value. Indicator design should therefore align with global development trends and support sustainable economic and social development. Priority should be given to improving public service quality, optimizing the business environment, and strengthening ecological protection. Accordingly, the indicator framework emphasizes enhancing Digital-intelligence Government Governance capabilities while advancing overall governance performance.

Operability principle. Each indicator must be observable and measurable, with clearly defined calculation methods and identifiable data sources. Indicator design should minimize risks of data manipulation or distortion and rely as far as possible on publicly accessible and

objective data. Considering the cost and feasibility of data collection, indicators should generally be easy to collect and should not impose excessive observation costs.

Adaptability principle. A comprehensive evaluation indicator framework should remain relatively stable within a given evaluation period. At the same time, as governance environments evolve and evaluation objectives change, the framework should be dynamically adjusted to respond to new governance conditions and emerging policy needs.

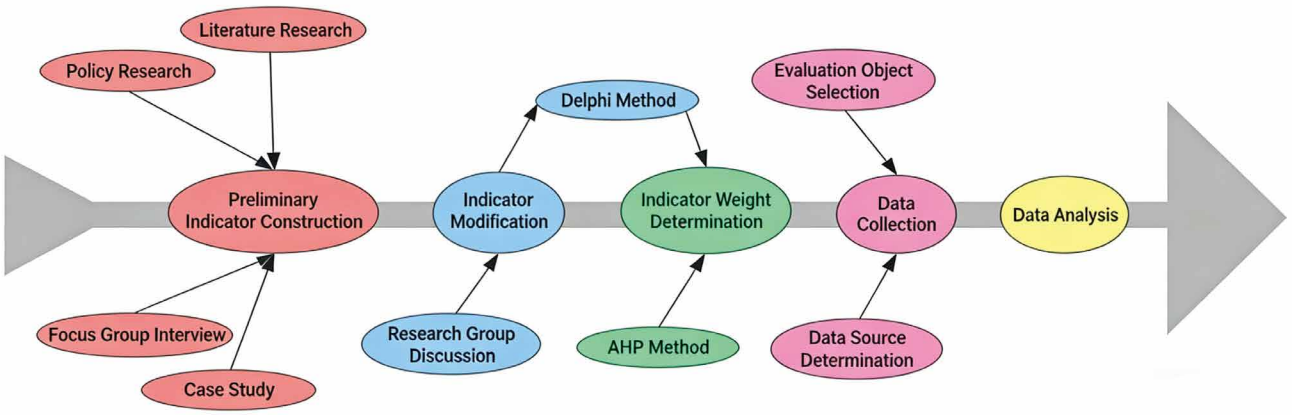

Figure 1 Research Framework

The research framework is illustrated in Figure 1. First, the Value-Focused Thinking (VFT) method is applied to conduct a content analysis of major global policy documents, extracting key policy objectives and implementation instruments as the basis for candidate indicators. To construct a comprehensive and operational evaluation indicator framework for government governance, extensive research and data collection are conducted. First, relevant studies and materials on digital government and government data are collected from both domestic and international sources. These materials include academic journal articles, conference papers, government reports, and reports from consulting organizations. Second, the collected literature and materials are systematically analyzed and synthesized. Considerations include indicator selection, classification, and weighting, with the aim of identifying candidate secondary and tertiary indicators. Finally, case analysis is used to refine the candidate indicators through additions and adjustments. Experts in relevant fields are invited to evaluate and review the proposed indicators, leading to the development of a digital government evaluation indicator framework that is both comprehensive and practically applicable.

(II)Evolution of the Digital-intelligence Government Governance Indicator Framework from 2019 to 2023

To respond to complex governance contexts and evolving policy objectives, the indicator framework for Digital-intelligence Government Governance has undergone continuous refinement from 2019 to 2023. Guided by the internal logic of Digital-intelligence governance, a series of updates and adjustments have been made to reflect key developments such as the expansion of the digital economy, rapid advances in artificial intelligence technologies, the global COVID-19 pandemic, and the pressures of post-pandemic economic recovery. These adjustments highlight the changing priorities and trends in government governance across different periods.

The addition and removal of indicators follow strict selection criteria and evaluation procedures. Newly introduced indicators are primarily determined based on policy orientation, technological development trends, societal needs, and data availability. Indicators are removed when policy objectives have been achieved, technologies become outdated, or governance environments change. Each annual adjustment is discussed and reviewed through multiple rounds of consultation with experts in government governance. Figure 2 summarizes the dynamic evolution of the indicator framework over the five-year period.

The evaluation theme in 2019 was “Big Data and Government Governance Effectiveness” .The framework focused on assessing government performance and capability, covering four dimensions: governance performance, governance capability, institutional support,

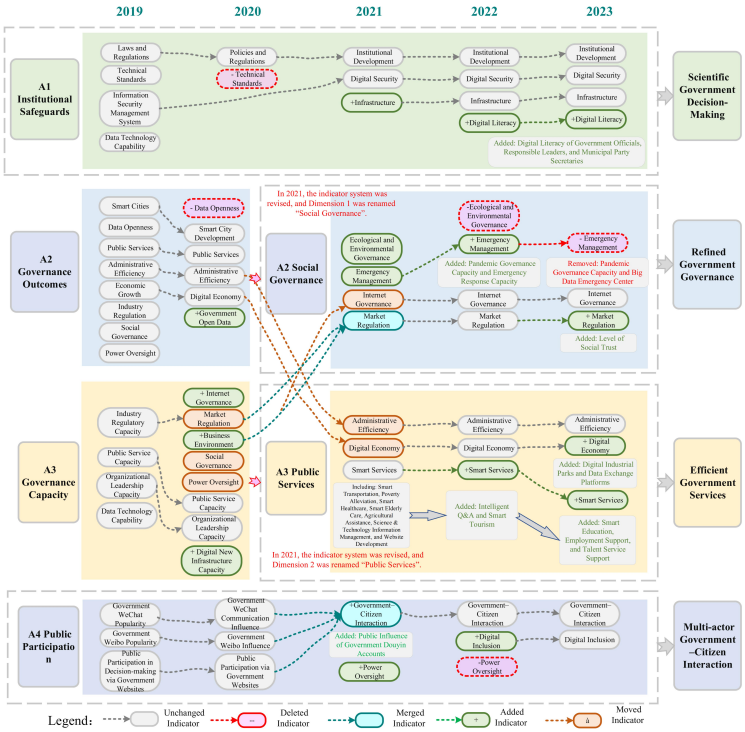

Figure 2. Evolution of the Indicator Framework for Digitally Empowered Government Governance, 2019–2023

and public participation.

In 2020, revisions and supplements were made to the dimensions of governance outcomes and governance capability, highlighting the importance of Digital-intelligence development in areas such as the digital economy, business environment optimization, and new digital infrastructure development. Newly added indicators emphasized the role of digital technologies in governance, capturing government responses to public health emergencies and strategies for promoting technological innovation. These adjustments ensured that the framework could reflect changes in policy priorities and technological developments in a timely manner.

In 2021, the framework underwent structural adjustment. The original dimensions of governance performance and governance capability were removed and replaced by the dimensions of social governance and public service delivery, reducing the emphasis on efficiency evaluation and highlighting the service and governance functions of government. In addition, considering the challenges posed by the COVID-19 pandemic, indicators related to emergency management were introduced to assess the capacity of local governments to use digital technologies to manage pandemic risks.

In 2022, the indicator framework was further adjusted to capture governance performance under the complex global pandemic environment. Indicators related to policy objectives that had been achieved, such as poverty alleviation, were removed. To respond to post-pandemic governance challenges, indicators on pandemic governance capability were added to measure the resilience of cities in addressing public health crises. Indicators no longer aligned with current policy priorities, such as ecological governance, were also removed to maintain consistency with policy orientations. At the same time, with the rapid development of large-scale AI models, new indicators such as intelligent government Q&A services were introduced to reflect emerging technological trends. In response to post-pandemic economic recovery needs, tourism-related indicators were also added to assess the recovery of service industries and reflect renewed attention to economic revitalization.

In 2023, the indicator framework underwent further important adjustments to address new challenges and opportunities in the post-pandemic period. The framework placed greater emphasis on economic recovery, the development of artificial intelligence, and enhanced social inclusiveness and care. Emergency governance indicators related to the pandemic were removed, while indicators on market regulation and the digital economy were added to assess government capacity to stabilize economic environments and promote economic recovery.

In addition, in response to rising employment pressures following the pandemic, indicators related to education, employment security, and talent services were introduced to evaluate government capacity to support employment and career development through digital means, reflecting increased attention to social welfare and livelihood issues.

(III) The 2025 Indicator Framework for Digital-intelligence Government Governance

Between 2023 and 2025, digital government worldwide has entered a stage in which operational quality and risk management become as important as functional expansion. As online service systems gradually mature, the

key issue faced by public sectors is no longer simply system construction or service coverage. Instead, governments must ensure stable operation under complex conditions, improve responsiveness, and address the new risks and opportunities associated with intelligent technologies.

Against this background, the 2025 indicator framework introduces a systematic restructuring of the previous model. It incorporates elements such as governance responsiveness, intelligent service provision, computing and security infrastructure, and multi-channel public participation into the core evaluation scope. While moderately reducing the overall number of indicators (by approximately 10%), the revised framework shifts the evaluation logic from construction-oriented measurement toward performance-oriented assessment, and from physical counts toward algorithm-based metrics. In this way, the framework provides a more precise analytical tool and institutional support for assessing the modernization level of digital government.

Dimension A: Digital-intelligence Social Governance

Social governance is a central domain in digital government transformation. Its level of digitalization directly influences the government's capacity to maintain public order, respond to risk events, and sustain public trust. As digital technologies become deeply embedded in public management processes, social governance is evolving from a domain of administrative execution toward an operational system supported by data resources, intelligent analytics, and real-time feedback mechanisms. The evaluation of social governance capability therefore involves both the government's ability to coordinate and respond in risk situations and the quality of interaction and trust between government and society.

From the perspective of evaluation logic, this dimension measures three core capabilities. The first is risk identification and emergency response capability, referring to whether governments can rapidly assess situations, mobilize resources, and implement effective responses when public risks or emergencies arise. The second is public trust and governance reputation, reflecting the social evaluation of government performance and the perceived outcomes of governance in a digital communication environment. The third is information communication and feedback mechanisms, which capture the ability of governments to respond to public concerns, address misinformation, and maintain information order in open information environments. Together, these three capabilities constitute the operational foundation of digital social governance systems.

In recent years, the technological environment of global social governance has undergone significant transformation. Emergency management systems are gradually shifting from models centered on physical infrastructure and organizational structures toward integrated operational systems characterized by data integration, risk prediction, and intelligent coordination. Artificial intelligence and data analytics technologies are increasingly used to enhance risk monitoring and resource allocation efficiency, reducing the explanatory power of evaluation approaches based solely on the scale of infrastructure construction. At the same time, in highly networked information environments, the speed of public opinion dissemination has increased significantly, and public perception has become more influential in governance stability. Government performance in responsiveness and information transparency therefore becomes a key observation variable.

Based on these developments, the indicator framework optimizes the social governance dimension. Indicators that previously focused on post-event outcomes or infrastructure construction are reduced, while greater emphasis is placed on responsiveness, system operational capability, and social feedback performance. For example, simple event-count indicators and passive response indicators are adjusted into rapid response capability metrics to better capture the dynamic performance of governance processes. Indicators related to intelligent emergency systems are introduced to measure the integration of data and algorithms in risk management. In addition, governance reputation and public feedback indicators are included to reflect the perceived effectiveness of governance from the societal perspective. Meanwhile, construction-oriented indicators with limited differentiation or universal adoption are consolidated or removed in order to enhance the comparative value of the framework.

Dimension B: Digital-intelligence Public Service Delivery

Public services constitute the most direct institutional interface between digital government and the public. Their operational quality directly influences how citizens perceive the outcomes of digital transformation. In a Digital-intelligence governance environment, public services not only perform basic administrative functions but also represent a key domain where technological applications intersect with institutional performance. Accordingly, the evaluation of this dimension reflects both the efficiency of government operations and the impact of technological integration on service delivery models and quality structures.

From the perspective of evaluation logic, this dimension focuses on three core aspects. The first is service provision efficiency and accessibility, referring to whether governments use digital and intelligent technologies to optimize procedures, shorten processing time, and reduce the cost of obtaining services. The second is response quality and professional competence, which examines whether government responses to public demands demonstrate completeness of information, problem-solving capacity, and transparency in explanation, rather than merely emphasizing response speed. The third is the breadth and structural extensibility of service coverage, reflecting whether digital technologies support the expansion of public services into areas such as innovation protection, professional regulation, and support for emerging industries. Together, these three aspects constitute the core structure of Digital-intelligence public service delivery.

In recent years, public sectors around the world have increasingly introduced automation tools and artificial intelligence systems to improve both internal administrative efficiency and frontline service responsiveness. Generative artificial intelligence and intelligent support systems are being applied in scenarios such as document processing, policy interpretation, and consultation responses. In this context, evaluation priorities are gradually shifting toward service quality, professional standards, and the actual effectiveness of problem resolution.

At the same time, as technological deployment becomes increasingly widespread, some early indicators oriented toward infrastructure or project construction are gradually losing their differentiating value. Once foundational systems become widely established, their mere existence no longer provides meaningful explanatory power. In contrast, factors such as the professionalization of service content, the quality of responses, cross-regional coordination capacity, and the depth of

intelligent support tool adoption better reflect the real operational state of digital public services. Therefore, the indicator framework introduces structural adjustments within the public service dimension, strengthening quality-oriented and operational indicators while reducing or consolidating construction-oriented indicators with limited dynamic variation.

Specifically, new indicators are introduced to measure response quality, enabling a more accurate assessment of the government's professional capacity in complex problem contexts. Indicators related to intelligent office systems and automated assistance tools are also incorporated to observe the extent to which artificial intelligence is embedded in internal administrative operations. In addition, indicators for specialized service domains are expanded to capture the ability of digital government to extend services into areas such as innovation protection and industrial development support. Meanwhile, indicators that have long remained static, lack annual variation, or merely reflect completed infrastructure construction are consolidated or removed in order to enhance the framework's comparative value and dynamic explanatory capacity.

Dimension C: Institutional and Infrastructure Support

Digital infrastructure and institutional safeguards constitute the foundational conditions for the operation of digital government. Their level of maturity directly affects the stability, security, and sustainability of governance systems. As data and algorithms become deeply embedded in public sector operations, support capacity is no longer reflected solely in the availability of technical resources, but also in the adaptability of institutional arrangements and the continuous development of organizational capabilities.

From the perspective of evaluation logic, this dimension is structured around four aspects: infrastructure capacity, security governance capacity, institutional responsiveness, and organizational digital capability. Infrastructure capacity refers to computing resources, data processing environments, and platform support conditions, which provide the necessary foundation for data-driven governance and algorithmic applications. Security governance capacity encompasses data protection, system safeguards, and risk response mechanisms, serving as the key guarantee for stable digital operations. Institutional responsiveness reflects whether governments are able to formulate clear and operational policy and regulatory arrangements for emerging technologies, forming the institutional basis for the legality and standardization of technological applications. Organizational digital capability refers to the extent to which the overall personnel structure and skill composition within the public sector can adapt to digital technologies, representing a practical condition for technology implementation and institutional execution. Together, these four capacities constitute the underlying support structure of digital government operations.

In recent years, the global development of artificial intelligence, large-scale models, and data infrastructure has accelerated significantly. Public sectors have shown increasing demand for high-performance computing resources and integrated data capabilities, making computing capacity and platform integration important indicators of digital government maturity. At the same time, many countries have strengthened regulatory requirements in cybersecurity and data protection. Frequent incidents of data breaches and system attacks have transformed information security from a purely technical issue into a governance concern, making security capability a core prerequisite for the trustworthy operation of digital government. At the institutional

level, governments around the world have issued policy frameworks and risk management guidelines for artificial intelligence and data governance, emphasizing transparency, traceability, and accountability mechanisms. Institutional responsiveness is therefore no longer measured by the number of policies issued, but by whether policies can effectively align with technological practices. Meanwhile, as digital technologies become more widely applied, evaluation has gradually shifted from assessing the capabilities of individual leaders to examining the overall digital capacity of organizations, with greater attention to workforce skill structures and continuous training mechanisms as indicators of sustainable institutional support.

Based on these developments, the indicator framework introduces structural adjustments within the support and safeguard dimension. Indicators related to computing capacity and data infrastructure are strengthened to better reflect the operational conditions required for high-intensity data processing environments in the public sector. An indicator for AI governance policy frameworks is introduced to measure the institutional capacity to regulate emerging technologies. In addition, data security incident indicators are incorporated to observe the effectiveness of security governance in practice. At the same time, indicators that merely reflect institutional establishment or the number of policy documents are consolidated, thereby enhancing the comparative value and explanatory power of the framework.

Dimension D: Digital-intelligence Public Participation

Public participation constitutes an important component of the digital government system. Its operational condition directly influences government transparency, the level of social collaboration, and the formation of institutional trust. In the digital environment, citizens are no longer merely recipients of public policies; instead, they participate in information expression, opinion feedback, and issue deliberation through multiple digital channels. The maturity of digital participation mechanisms therefore reflects both the openness of government and the inclusiveness and interactivity of governance structures.

From the perspective of evaluation logic, this dimension focuses on three aspects. The first is government digital communication and public interaction capacity, referring to whether governments can maintain stable and continuous communication with the public through multi-channel dissemination systems and respond to societal concerns in a timely manner. The second is the integration level of public service interaction mechanisms, which reflects whether citizens have clear, unified, and sustainable access pathways when obtaining information or submitting requests. The third is citizens'digital experience and accessibility, measuring whether interaction processes are convenient, whether feedback mechanisms are accurate, and whether different social groups are able to participate on an equal basis. Together, these three aspects form the structural foundation of public participation capacity.

In recent years, the global digital communication environment has undergone significant transformation. Multi-platform communication and diversified content formats have become the norm, making traditional indicators based on a single communication channel insufficient for capturing the real dynamics of public interaction. At the same time, public institutions have gradually integrated fragmented consultation, complaint, and feedback channels by establishing unified access systems or multi-channel integration mechanisms, thereby improving the convenience of public participation. From

a technological perspective, intelligent customer service systems and automated response tools are increasingly being introduced into public service interaction scenarios in order to enhance response efficiency and address large-scale consultation demands.

Against this background, the indicator framework introduces structural adjustments to the public participation dimension. Communication capacity indicators shift from measuring single channels to evaluating the degree of multi-channel interaction integration, emphasizing cross-platform data integration and the breadth of interaction. Public service interaction indicators move beyond simple opinion collection functions toward comprehensive access and feedback mechanisms, reflecting the level of integration and sustainability of service entry points. In addition, intelligent interaction capability indicators are introduced to assess the government's capacity to maintain response efficiency and consistency in large-scale interaction environments. Construction-oriented indicators that lack consistent measurement standards or exhibit limited variation are consolidated in order to enhance the comparative value of the framework.

Through the discussion and analysis of these indicators, the original indicator system is further refined and optimized. Ultimately, the Digital-intelligence Government Governance Evaluation Index is constructed with four primary dimensions, fourteen secondary indicators, and forty-two tertiary indicators, as illustrated in Figure 3.

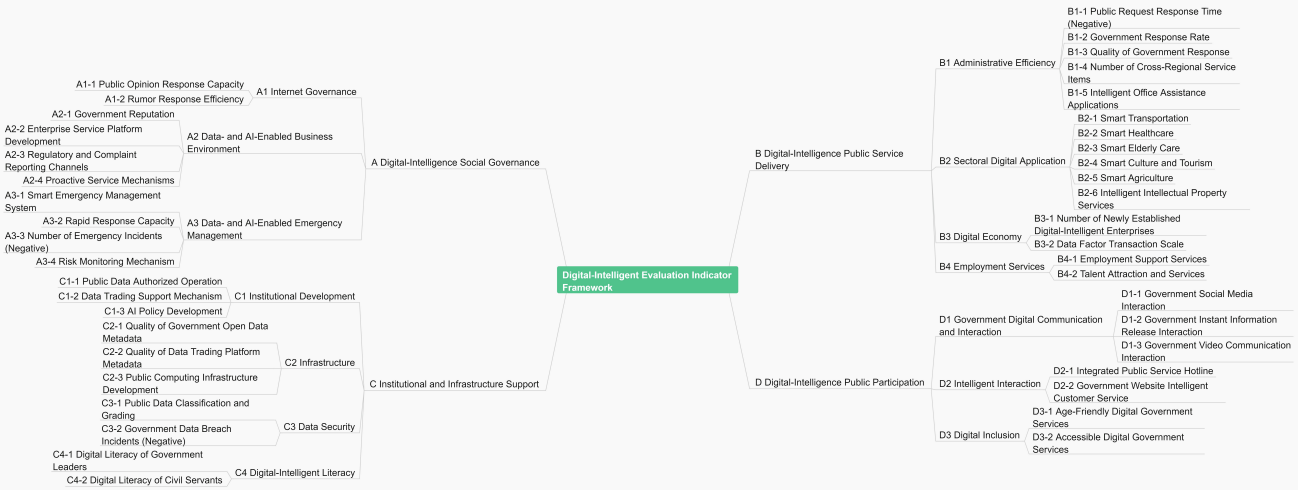

Figure 3. The 2025 Evaluation Index System for Digital-intelligence Government Governance

The weights of the indicators in the 2025 index framework were primarily determined using the Delphi method. A panel of 17 experts was invited to evaluate the importance of each indicator through three rounds of scoring. The results from each round were processed using a structured approach, and the final weights of the indicators were calculated based on the experts' scores in the final round, forming a preliminary weighting scheme.

On this basis, the weights were further adjusted in accordance with the current stage of development of Digital-intelligence government governance and the objectives of the evaluation framework. The final weights for indicators at each level were then established, as shown in Table 7.

Table 7 Weights of the Indicator Framework

Code	Primary Indicator	Weight	Code	Secondary Indicator	Weight	Code	Tertiary Indicator	Weight
A	Digital-intelligence Social Governance	30.00%	A1	Internet Governance	7.50%	A1-1	Public Opinion Response Capacity	4.500%
					7.50%	A1-2	Rumor Response Efficiency	3.000%
			A2	Digital-intelligence Business Environment	12.00%	A2-1	Government Reputation	3.600%
					12.00%	A2-2	Enterprise Service Platform Development	3.000%
					12.00%	A2-3	Regulatory and Complaint Reporting Channels	3.000%
					12.00%	A2-4	Proactive Service Mechanisms	2.400%
			A3	Digital-intelligence Emergency Management	10.50%	A3-1	Smart Emergency Management System	2.625%
					10.50%	A3-2	Rapid Response Capacity	3.150%
					10.50%	A3-3	Number of Emergency Incidents (Negative)	2.625%
					10.50%	A3-4	Risk Monitoring Mechanism	2.100%
B	Digital-intelligence Public Service Delivery	35.00%	B1	Administrative Efficiency	9.45%	B1-1	Public Request Response Time (Negative)	1.701%
					9.45%	B1-2	Government Response Rate	1.607%

Code	Primary Indicator	Weight	Code	Secondary Indicator	Weight	Code	Tertiary Indicator	Weight
B	Digital-intelligence Public Service Delivery	35.00%	B1	Administrative Efficiency	9.45%	B1-3	Quality of Government Response	1.890%
					9.45%	B1-4	Number of Cross-Regional Service Items	2.835%
					9.45%	B1-5	Intelligent Office Assistance Applications	1.418%
			B2	Sectoral Digital Empowerment	12.95%	B2-1	Smart Transportation	2.590%
					12.95%	B2-2	Smart Healthcare	2.590%
					12.95%	B2-3	Smart Elderly Care	1.943%
					12.95%	B2-4	Smart Culture and Tourism	1.943%
					12.95%	B2-5	Smart Agriculture	1.943%
					12.95%	B2-6	Intelligent Intellectual Property Services	1.943%
			B3	Digital Economy	5.95%	B3-1	Number of Newly Established Digital-intelligence Enterprises	2.975%
					5.95%	B3-2	Data Factor Transaction Scale	2.975%
			B4	Employment Services	6.65%	B4-1	Employment Support Services	3.325%
					6.65%	B4-2	Talent Attraction and Services	3.325%

Code	Primary Indicator	Weight	Code	Secondary Indicator	Weight	Code	Tertiary Indicator	Weight
C	Institutional and Infrastructure Support	20.00%	C1	Institutional Development	6.00%	C1-1	Public Data Authorized Operation	1.800%
					6.00%	C1-2	Data Trading Support Mechanism	2.100%
					6.00%	C1-3	AI Policy Development	2.100%
			C2	Infrastructure	6.00%	C2-1	Quality of Government Open Data Metadata	1.800%
					6.00%	C2-2	Quality of Data Trading Platform Metadata	1.800%
					6.00%	C2-3	Public Computing Infrastructure Development	2.400%
			C3	Data Security	4.00%	C3-1	Public Data Classification and Grading	2.400%
					4.00%	C3-2	Government Data Breach Incidents (Negative)	1.600%
			C4	Digital-intelligence Literacy	4.00%	C4-1	Digital Literacy of Government Leaders	3.200%
					4.00%	C4-2	Digital Literacy of Civil Servants	0.800%
D	Digital-intelligence Public Participation	15.00%	D1	Government Digital Communication and Interaction	4.50%	D1-1	Government Social Media Interaction	1.575%
					4.50%	D1-2	Government Instant Information Release Interaction	1.350%
					4.50%	D1-3	Government Video Communication Interaction	1.575%

Code	Primary Indicator	Weight	Code	Secondary Indicator	Weight	Code	Tertiary Indicator	Weight
D	Digital-intelligence Public Participation	15.00%	D2	Intelligent Interaction	5.25%	D2-1	Integrated Public Service Hotline	2.625%
					5.25%	D2-2	Government Website Intelligent Customer Service	2.625%
			D3	Digital Inclusion	5.25%	D3-1	Age-Friendly Digital Government Services	3.150%
					5.25%	D3-2	Accessible Digital Government Services	2.100%

IV、International Reference and Structural Adaptation of the Indicator Framework

（Ⅰ）International Reference of the Indicator Framework

International digital government evaluation frameworks generally follow three major orientations. The first focuses on the degree of service digitalization, examining indicators such as online service coverage, cross-departmental integration, and the development of e-participation channels. The second emphasizes institutional and policy completeness, highlighting the establishment of data governance rules, open data regimes, and legal frameworks. The third adopts a maturity-based approach, assessing the level of digital government development through staged classifications.

Although these frameworks differ in their analytical approaches, they largely converge around several common structural themes. These include development stages and maturity logic, service provision and user experience, institutional and infrastructure support, cross-departmental integration capacity, and risk and security safeguards. In practical evaluation processes, these orientations often share a set of cross-framework indicators embedded in dimensions such as service assessment, public interaction, and enabling conditions. These indicators also reflect a growing emphasis on inclusiveness, addressing the needs of populations with limited connectivity, individuals with constrained digital capabilities, and other groups facing barriers to access. In doing so, they enable evaluation frameworks to identify variations in digital-intelligent service accessibility across social groups.

This structural approach had strong distinguishing power during the early stages of digitalization. However, as an increasing number of countries have completed the construction of foundational portals, online service systems, and institutional frameworks, evaluation approaches centered on the existence of functions or institutions have gradually lost their ability to capture

differences in operational performance. Under such circumstances, if evaluation remains focused primarily on functional coverage statistics, it becomes difficult to distinguish the operational differences among governance systems.

To address this limitation, the present indicator framework shifts the evaluation focus from the existence of systems to operational capacity. Its core distinction does not lie in the number of systems or policies, but in four categories of governance capacity. The social governance dimension examines the government's ability to respond, coordinate, and manage complex societal situations. The public service dimension evaluates the professionalism, continuity, and problem-solving quality of service provision. The institutional and infrastructure support dimension focuses on infrastructure conditions, data governance arrangements, security safeguards, and institutional adaptation capacity. The public participation dimension assesses interaction mechanisms, the quality of service reach, and the level of digital inclusion. In this framework, evaluation shifts away from infrastructure itself toward governance capacity, and away from mere presence toward actual performance.

Table 8 International Reference of the Digital-intelligence Government Governance Indicator Framework

Dominant Approach	Reference Dimension	Typical Approach of Major International Evaluation Frameworks	Structural Orientation of This Indicator Framework
Maturity-Based Approach	Evaluation Unit	Based on the implementation status of functions	Based on operational capacity performance
	Development Logic	Describes development stages through maturity classification	Describes governance operation through capability structures
Service Digitalization Approach	Service Evaluation	Focuses on service launch and coverage	Focuses on response quality and problem-solving capacity
	Government Platforms	Emphasizes system integration and platform completeness	Emphasizes cross-regional coordination and proactive service mechanisms
	Digital Participation	Measures the number of channels and degree of openness	Measures interaction depth and multi-channel integration capacity
Institutional Completeness Approach	Risk and Security	Mostly treated as enabling conditions	Incorporated as core operational constraints and negative indicators
	Infrastructure	Emphasizes construction level and institutional completeness	Emphasizes computing support, security resilience, and operational effectiveness
	Technology Integration	Focuses on technology deployment and policy existence	Focuses on the degree of integration of intelligent tools into governance processes

Dominant Approach	Reference Dimension	Typical Approach of Major International Evaluation Frameworks	Structural Orientation of This Indicator Framework
Cross-Dimensional Observation Variable	Service Accessibility and Group Inclusion	Embedded in existing dimensions through whether services are reachable and usable, whether citizens actually adopt them, and how capability differences affect access	Incorporated into the operational capacity structure to assess differences in service access and sustained use across social groups

Compared with function-coverage-oriented frameworks, the present indicator framework introduces structural differences in three respects. First, it shifts the focus from static existence to dynamic processes, emphasizing response speed, risk control, and the capacity for sustained operation. Second, it moves from isolated functional indicators to structural interconnections, examining the coupling relationships among different governance capacities rather than treating indicators as independent variables. Third, it transitions from construction scale to operational resilience, incorporating security capacity, computing resources, and risk management into the core dimensions rather than treating them as peripheral support conditions.

At the same time, public interaction and digital inclusion are integrated into the operational capacity structure. As a result, differences in governance performance are reflected not only in system stability but also in the reach of services and their actual accessibility to different groups.

This structural difference does not represent a simple replacement of existing frameworks, but rather corresponds to changes in the stage of digital government development. As digital government enters a phase characterized by data-driven governance and the integration of artificial intelligence, operational risks and system stability emerge as new sources of differentiation among governance systems. The significance of this indicator framework, therefore, lies not in expanding the list of digital functions, but in adjusting the analytical perspective through which governance performance is observed.

(II) Transferability Across Institutional Contexts

In cross-national comparisons, digital government evaluation is often directly influenced by differences in institutional structures. Variations in administrative hierarchies, fiscal decentralization, legal frameworks for public data, information disclosure regimes, and the procurement and operation models of digital technologies can all affect the availability and comparability of indicators. Therefore, whether an indicator framework can be applied across different institutional environments largely depends on whether its structural logic is grounded in governance scenarios that commonly exist across countries.

The framework proposed in this report provides a capacity-identification structure. It characterizes key capability domains in Digital-intelligence governance through a stable hierarchical structure while leaving room for adjustments at the levels of indicator content and measurement methods in different institutional

environments. This structured—rather than template-based—design allows the framework to maintain analytical consistency while enabling application and comparison across diverse institutional settings.

The structural foundation of the framework does not rely on specific administrative systems or policy instruments. Instead, it is organized around four governance scenarios that commonly emerge in the operation of Digital-intelligence governance: social governance, public service delivery and problem response, public infrastructure and institutional support, and public interaction and accessibility arrangements. Regardless of the organizational form adopted by governments, these scenarios constitute fundamental units of digital governance operations and therefore possess practical relevance across different institutional environments. This scenario-based structural design—rather than one based on institutional labels—forms the basis for the framework' s transferability.

At the level of practical application, the transferability of the framework is mainly reflected in three aspects. First, indicator content can be adapted. For example, the indicator "response time to public requests" may correspond to hotline systems, online petition platforms, or integrated service portals in different countries. Similarly, "data breach incidents" can be measured according to national cybersecurity reporting systems or regulatory disclosure rules. What the indicator captures is not the specific platform itself, but the efficiency or outcome reflected in its operation.Second, the weighting structure can be adjusted. Depending on policy priorities or stages of governance development, the relative importance of dimensions such as social governance, public service delivery, or public participation can be recalibrated to reflect local policy agendas. Third, data sources and measurement methods can be localized. Administrative records, open government data, third-party monitoring data, or survey data may all serve as alternative data sources. As long as the conceptual meaning of the indicators remains consistent, methodological adjustments can be made accordingly.

It should be emphasized that structural transferability does not imply simple replication. Institutional boundaries, legal requirements, and data availability may directly influence how indicators are implemented. For example, strict restrictions on personal data disclosure in some countries may limit algorithm-based measurement of response quality or interaction intensity. In highly decentralized governance systems, the statistical scope of indicators related to cross-regional coordination may also need to be redefined. Therefore, the transferability of the framework is based on the principle of "stable structure, adaptable content, and adjustable methods," rather than the direct replication of indicator definitions.


世界互联网大会
World Internet
Conference


中国式现代化发展研究院
INSTITUTE OF CHINESE PATH TO MODERNIZATION