PUBLIC ADMINISTRATION 4.0: LEVERAGING DIGITAL TOOLS FOR EFFECTIVE GOVERNANCE

Monograph

Public Administration 4.0: Leveraging Digital Tools for Effective Governance

Estonia, 2025

International databases and directories indexing publications:

- CrossRef (DOI: 10.36690);
- Google Scholar;
- National Library of Estonia;
- The ESTER e-catalog;

Recommended for publishing by the Academic Council of the Scientific Center of Innovative Research (№4 of 26.09.2025)

ISBN 978-9916-9389-0-4 (pdf)

Public Administration 4.0: Leveraging Digital Tools for Effective Governance *(2025).* Monograph. In O. Akimov (Ed.), Scientific Center of Innovative Research. Estonia. 262 p. https://doi.org/10.36690/PUBADM

The monograph examines a core challenge of contemporary state development, namely the transition to Public Administration 4.0 in digitalized and security sensitive governance environments. In the context of hybrid service delivery, platform expansion, and the growing use of AI, public institutions must increase efficiency while preserving legality, accountability, and public trust. The book offers an integrated analysis of digital public governance by combining conceptual foundations and international models with practical implementation issues, including interoperability and data governance. It pays particular attention to risk based supervision, anti fraud policy, and the digitalization of accounting and reporting as instruments of economic security and administrative integrity. The monograph also situates digital transformation within broader security architectures, including national, economic, and energy policy contexts, showing that modernization must be aligned with resilience and continuity requirements.

The monograph is intended for researchers and graduate students in public administration and public policy, as well as for civil servants, public sector managers, supervisory and audit professionals, and policymakers engaged in digital transformation and economic security. Overall, it contributes a coherent framework and applied guidance for scaling digital government responsibly through transparency, inclusion, cybersecurity, and effective oversight.

Table of Contents

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Introduction

The monograph "*Public Administration 4.0: Leveraging Digital Tools for Effective Governance*" examines how public institutions can redesign governance capacity under conditions of rapid digitalization, expanding data flows, and the growing use of AI in public services. It proceeds from the assumption that contemporary digital transformation is not limited to automation of procedures, because it also reshapes institutional design, accountability, and the legitimacy of administrative decisions. In this context, the practical value of digital government depends on interoperability, lawful data reuse, and trust infrastructure, which together enable integrated service delivery and reduce repetitive administrative requests. At the same time, scaling digital services increases systemic exposure to governance risks, including model risk, cybersecurity vulnerabilities, and unequal access, which requires public administration to treat safeguards as a core element of performance rather than as a secondary compliance layer. These premises position Public Administration 4.0 as a governance paradigm that combines user centric service design with resilient institutional mechanisms and measurable public value outcomes.

A central analytical focus of the monograph is that digital transformation simultaneously strengthens administrative capacity and raises the cost of error, since decisions are increasingly mediated by platforms, analytics, and AI supported triage. This is particularly visible in the domain of public governance of digital accounting and reporting, where the quality of data, the reliability of identifiers, and the design of reporting pipelines directly influence fraud exposure, supervisory effectiveness, and economic security. Therefore, risk based supervision and anti fraud policy are treated as institutional capabilities that align law, data governance, analytics, and accountability into an integrated decision cycle, with attention to proportionality, fairness, and administrative burden reduction. The monograph also situates digital governance within broader security architectures, recognizing that national security challenges, economic resilience, and energy policy turbulence intensify the need for evidence grounded and interoperable public administration. In this

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

sense, digital tools are interpreted not as neutral technologies, but as governance instruments whose effectiveness depends on institutional coordination, oversight mechanisms, and the capacity to learn through monitoring and evaluation.

Structurally, the monograph is organized into three chapters that develop a coherent trajectory from conceptual foundations to sectoral governance instruments and security relevant applications.

Chapter 1 "*Digital Public Governance: Conceptual Frameworks, International Models and AI Driven Public Services*", systematizes the conceptual evolution of digital public administration, compares international practices and transfer mechanisms, and analyses how AI can enhance the efficiency and quality of public services under defined accountability constraints.

Chapter 2 "*Public Governance of Digital Accounting and Reporting: Risk-Based Supervision, Anti-Fraud Policy and Economic Security*", develops a governance perspective on digital supervision instruments, the digitalization of accounting and reporting in Ukraine, and the quality risks of digital reporting alongside precautions and oversight mechanisms.

Chapter 3 "*Public Administration in the Architecture of Security: National, Economic, and Energy Policy Contexts*", connects digital governance with the realities of national security under full scale invasion, the modernization of economic security instruments, and the evidence base of public governance in energy policy, including the Visegrád Group context. The monograph is intended for scholars, policymakers, public sector leaders, and practitioners who need an integrated framework that links digital public service modernization with risk governance, anti fraud capacity, and security oriented policy coherence.

The monograph is designed for researchers in public administration, public policy, and digital governance, as well as for civil servants and managers responsible for institutional reform, service delivery modernization, and regulatory design. It is also relevant for supervisory and control bodies, public finance and audit professionals, and specialists engaged in digital accounting, reporting governance, and anti fraud policy, because these domains increasingly depend on data quality, interoperable registers, and enforceable accountability procedures. For national and sectoral

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

policy communities, including those working in economic security, cybersecurity, and energy governance, the monograph offers a consolidated perspective on how digital transformation changes risk profiles and coordination requirements in multi level administrative systems. For graduate students and early career professionals, it provides an analytically consistent entry point into Public Administration 4.0 as a governance paradigm that integrates institutional design, legal safeguards, and implementation capacity. Across these audiences, the monograph is intended to support both conceptual understanding and applied decision making by linking policy frameworks with operational instruments, including risk based supervision, integrity controls, and evidence informed service design.

The book's internal logic emphasises that digitalization is successful when it improves public value and administrative reliability simultaneously, rather than when it only increases the volume of digital transactions. In this sense, the contribution of the monograph consists in treating digital tools as instruments of governance that must be embedded in institutional responsibility, measurable outcomes, and rights respecting administrative routines. A further contribution lies in connecting digital public services with the governance of reporting, fraud prevention, and security architectures, thereby demonstrating that digital government maturity is inseparable from resilience and economic security objectives.

The directions for further research derived from the monograph's problem field concern, first, the development of measurable indicators for assessing the effectiveness of AI enabled solutions in the public sector, with attention to service targeting, administrative burden reduction, and error costs under real operational constraints. Second, future studies should deepen the analysis of ethical and human rights implications of algorithmic governance, particularly in domains where automated support may influence eligibility decisions, enforcement priorities, or the distribution of public resources. Third, longitudinal research is needed to evaluate how AI adoption changes accountability chains, transparency practices, and democratic participation, including the

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

institutional consequences of increased reliance on predictive analytics and platform mediated coordination.

Comparative research across jurisdictions and administrative traditions remains methodologically important, because digital governance models are shaped by legal interoperability, institutional trust arrangements, and implementation capacity, which differ substantially even among countries that adopt similar technologies. In addition, the monograph's focus on risk based supervision and digital reporting suggests a research agenda on data governance quality, auditability of reporting pipelines, and the design of oversight mechanisms that can detect manipulation while remaining proportionate and procedurally fair. Finally, the security oriented perspective of the third chapter motivates further work on the governance of critical infrastructures, including energy policy, where digital coordination, continuity planning, and crisis learning mechanisms increasingly define the practical effectiveness of public administration. In aggregate, these directions position Public Administration 4.0 as a field in which administrative modernization must be evaluated through institutional effects, not only through technical deployment, and where innovation is defensible when it strengthens legality, trust, inclusion, and resilience at the same time.

Chief editor of the monograph
Prof., Dr., Oleksandr Akimov

https://doi.org/10.36690/PUBADM
ISBN 978-9916-9389-0-4 (pdf)

Chapter 1
Digital Public Governance: Conceptual Frameworks, International Models and AI Driven Public Services

https://doi.org/10.36690/PUBADM
ISBN 978-9916-9389-0-4 (pdf)

Section 1.1. Digitalization of Public Administration: Conceptual Foundations, Institutional Change, and Implementation Policy

Oleksandr Akimov[1], Liudmyla Akimova[2]

[1]*Doctor of Sciences in Public Administration, Professor, Honored Economist of Ukraine, Professor, Scientific and Methodological Centre of Personnel Policy of the Ministry of Defence of Ukraine, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-9557-2276*

[2]*Doctor of Sciences in Public Administration, Professor, Honored Education Worker of Ukraine, Professor of the Department of Labor Resources and Entrepreneurship, National University of Water and Environmental Engineering, Rivne, Ukraine; ORCID: https://orcid.org/0000-0002-2747-2775*

Citation:
Akimov, O. & Akimova, L. (2025). Digitalization of Public Administration: Conceptual Foundations, Institutional Change, and Implementation Policy. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 9–31). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-9-31

Abstract. *Public administration digitalization has progressed from technology focused automation to governance centered transformation, where digital tools reshape institutional design, integrated service delivery, and accountability. Contemporary models stress interoperability, lawful data reuse, and trust infrastructure as prerequisites for sustainable scaling, while value based approaches frame digital public services through rights protection, inclusion, and resilience. The goal of this study is to systematize the evolutionary phases of public administration digitalization and to compare the conceptual foundations of digital government in EU countries and Ukraine, emphasizing institutional change and implementation policy. The study applies qualitative policy synthesis and comparative institutional reasoning, organizing key policy narratives into a phase typology and a milestone based comparison interpreted through governance architecture, sequencing, and capacity building. The findings identify five phases: informatization, e government, digital government, platform and ecosystem government, and value based resilient digital government. Across these phases, the dominant logic shifts from agency centric efficiency to whole of government coordination and data enabled public value creation, which increases the importance of legal, organizational, and data governance alignment. The EU pathway is marked by shared principles and coordinated commitments that prioritize user centricity, the once only principle, and target driven steering supported by monitoring mechanisms. Ukraine demonstrates accelerated implementation through a unified service ecosystem and interoperability infrastructure that enable data reuse and reduce repetitive administrative requests, while remaining embedded in a broader public administration reform agenda. The results suggest that sustainable digitalization requires co development of institutional design, legal interoperability, and trust infrastructure alongside service expansion, with performance management focused on outcomes, inclusion, and resilience rather than output counts.*

Keywords: *digital government; public administration digitalization; e-government; interoperability; once only principle; government as a platform; digital identity; trust infrastructure; value based governance; institutional change; policy implementation; monitoring and evaluation.*

ISBN 978-9916-9389-0-4 (pdf)

1. The evolution of public administration digitalization. The evolution of public administration digitalization reflects a gradual shift from technology-led automation toward governance-led transformation, where digital tools are embedded in institutional design, service delivery, and accountability. In the earliest stage, often described as informatization, public organizations prioritized internal efficiency through computerization of clerical tasks, document management, and the creation of isolated databases. This stage improved administrative throughput but rarely changed the logic of public service provision, because information systems were typically agency-centric, fragmented, and weakly connected to policy outcomes. A second stage, associated with e-government, moved beyond internal automation to online information provision and transactional services, enabling citizens and businesses to submit forms and requests electronically. The key limitation of this stage was that it frequently digitized existing procedures "as is," thereby transferring complexity into digital channels rather than redesigning processes around user journeys and life events.

A third stage, frequently labeled digital government, emphasizes integrated service delivery, cross-organizational coordination, and data reuse as a governance capability. International policy frameworks increasingly describe digital government as an organizational and policy transformation rather than an IT program, with leadership, whole-of-government coordination, and a data-driven public sector as foundational conditions (OECD, 2014).

In the European Union, this transition was operationalized through the EU eGovernment Action Plan 2016 to 2020, which advanced principles such as "digital by default," "once-only," openness, and interoperability as shared commitments that should guide modernization and reduce administrative burden (European Commission, 2016).

The Tallinn Declaration later reinforced this direction as a ministerial-level political commitment, prioritizing user-centricity, the once-only principle, and trust-based approaches for high-quality digital public services (European Commission, 2017).

From the late 2010s onward, a platform and ecosystem perspective gained prominence, where digital public administration is understood as a coordinated set of shared building blocks such as digital identity, interoperability layers, data governance, and reusable components that enable consistent services across agencies and, in the EU context, across borders. This logic aligns with the broader interoperability agenda promoted through the European Interoperability Framework, which treats

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

interoperability as multidimensional, encompassing legal, organizational, semantic, and technical alignment rather than mere system integration.

At the same time, global assessments increasingly frame digital government as a contributor to sustainable development, institutional effectiveness, and resilience, not only as an efficiency instrument, as reflected in the UN E-Government Survey's emphasis on inclusive digital government and resilient infrastructure investment.

A further, distinctly contemporary phase can be characterized as value-based and resilient digital government, where the normative dimension becomes explicit. The Berlin Declaration links digital public services to European values, fundamental rights, inclusion, and trust, thereby strengthening the expectation that digital transformation must protect rights and legitimacy rather than merely expand functionality (European Commission, 2020).

In parallel, the EU's Digital Decade Policy Programme 2030 institutionalizes a target-driven approach to digital transformation, establishing measurable objectives and monitoring mechanisms across dimensions that include the digitalization of public services (European Parliament and Council of the European Union, 2022). Across OECD analytical frameworks, this phase is frequently described through principles such as "digital by design," "government as a platform," "user-driven," and "proactiveness," which together capture the move from digitized transactions toward anticipatory, integrated, and data-enabled public value creation.

Ukraine's trajectory illustrates an accelerated and highly visible evolution that combines rapid service scaling with infrastructure for interoperability. The establishment of a dedicated institutional center for digital transformation enabled a coordinated strategy of building a unified service ecosystem, with Diia serving as a citizen-facing entry point that unites digital documents with public services across mobile and web channels (Ministry of Digital Transformation of Ukraine, 2025). In parallel, the Trembita system operationalizes interagency data exchange, enabling authorities to reuse data and reduce repetitive requests to citizens, which is conceptually consistent with the once-only logic emphasized in EU frameworks even when implemented under different national labels (EU4Digital, 2025). Importantly, Ukraine's evolution is also embedded in a broader modernization agenda, where the Public Administration Reform Strategy 2022 to 2025 frames the objective of building a capable service and digital state with safeguards for citizens' rights (Cabinet of Ministers of Ukraine, 2021). Taken together, the EU and Ukraine experiences suggest

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

that digitalization evolves most sustainably when institutional design, legal interoperability, and trust infrastructure co-develop alongside service expansion, rather than being treated as sequential or purely technical tasks.

Table 1.1 introduces a structured typology of the evolution of public administration digitalization, focusing on the dominant governance logic and the primary outputs in each phase.

Table 1.1. Evolutionary Phases of Public Administration Digitalization: Governance Logic, Instruments, and Outputs

Evolutionary phase	Dominant governance logic	Typical instruments	Primary outputs and limitations
Informatization and internal automation	Administrative efficiency within agencies	Office automation, registries, document systems	Faster internal processing, but siloed data and weak service integration
E-government and online transactions	Channel shift toward electronic interaction	Web portals, e-forms, basic online services	Wider access to procedures, but frequent "digitization of bureaucracy" without redesign
Digital government and integrated services	Whole-of-government coordination and data reuse	Interoperability frameworks, shared platforms, data governance	End-to-end services and reduced duplication, but requires institutional coordination and standards (OECD, 2014)
Platform and ecosystem government	Reusable building blocks and cross-domain alignment	Digital identity, interoperability layers, APIs, common components	Scalable service ecosystems and cross-border readiness in the EU context (EIF)
Value-based and resilient digital government	Rights, inclusion, trust, and resilience as baseline requirements	Value-based principles, targets, monitoring, cybersecurity-by-design	Digital services as public value infrastructure, constrained by rights and accountability (Berlin Declaration; Digital Decade)

Sources: systematized by the authors based on (OECD, 2014; United Nations Department of Economic and Social Affairs, 2024; European Commission, 2017; European Commission, 2020)

The progression shows a consistent shift from agency-centric automation toward cross-institutional governance capabilities, where legal and organizational alignment becomes as decisive as technology.

Table 1.2 summarizes key policy milestones that shaped the EU trajectory and situates Ukraine's accelerated pathway within comparable governance logics of user-centricity, interoperability, and trust.

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Table 1.2. Policy and Institutional Milestones of Digital Government: Comparative Overview of the EU and Ukraine

Jurisdiction	Milestone	Core emphasis for evolution	Why it matters for the "next stage"
EU	EU eGovernment Action Plan 2016–2020	Digital by default, once-only, interoperability and openness	Defines shared principles and legitimizes process redesign beyond channel digitization
	Tallinn Declaration (2017)	User-centricity, once-only, trust and quality of services	Converts principles into a political commitment among ministers and accelerates coordinated adoption
	Berlin Declaration (2020)	Value-based digital government, fundamental rights, trust	Embeds normative constraints and democratic legitimacy into digital transformation governance
	Digital Decade Policy Programme 2030 (2022)	Targets, monitoring, coordinated policy cycles	Institutionalizes measurable goals and policy steering for digital public services
Ukraine	Diia ecosystem	Unified access to documents and services, user-centric scaling	Creates a recognizable service-state interface and accelerates citizen adoption
	Trembita interoperability system	Secure interagency data exchange and reuse	Enables integrated services and reduces repetitive administrative requests
	Public Administration Reform Strategy 2022–2025	Service and digital state, rights safeguards, institutional capability	Anchors digitalization in administrative reform and institutional capacity building

Sources: systematized by the authors based on (European Commission, 2016; European Commission, 2017; European Commission, 2020; European Parliament and Council of the European Union, 2022; Cabinet of Ministers of Ukraine, 2021; Ministry of Digital Transformation of Ukraine, 2025; State Enterprise DIIA, 2025)

Across contexts, the decisive milestones are those that convert digitalization from projects into governance commitments, because they define principles, allocate institutional responsibility, and build trust infrastructure for scale.

2. Conceptual foundations in EU countries and Ukraine: a comparative perspective. Conceptual foundations of public administration digitalization can be defined as an integrated set of normative principles, governance arrangements, and enabling infrastructures that determine how digital tools reshape state capacity, service quality, and administrative legitimacy. This framing matters because "digitalization" is not synonymous with deploying information systems, rather it refers to a deliberate reconfiguration of public administration around data flows, interoperable processes, and user oriented service outcomes (OECD, 2014). In this sense, the conceptual core of digital government rests on three interdependent layers: a value layer (why transformation is pursued and what constraints apply), a governance layer (who coordinates decisions and how

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

accountability is ensured), and an infrastructure layer (which technical and organizational building blocks make integration feasible). The European Union has operationalized these layers through a combination of policy principles, harmonized legal instruments, and shared frameworks designed to enable cross border functionality, administrative burden reduction, and rights based governance (European Commission, 2016; European Commission, 2017). The Ukrainian pathway has pursued comparable principles but under different contextual drivers, emphasizing rapid service scaling, strong central coordination, and infrastructure for interagency exchange to support integrated services (Ministry of Digital Transformation of Ukraine, n.d.; Cabinet of Ministers of Ukraine, 2021). A comparative approach is therefore most informative when it moves beyond listing initiatives and instead examines how principles are translated into institutional mechanisms and enforceable rules. The key analytical premise is that similar principles can produce different outcomes depending on sequencing, legal constraints, and the degree of coordination capacity available. Consequently, the comparison below focuses on conceptual pillars that shape digitalization as governance, not as technology adoption.

Value and principles as the normative foundation. In the EU, digital government is increasingly anchored in a value based understanding of public service provision, where convenience and efficiency must be balanced with legitimacy, inclusion, and fundamental rights. Principles such as user centricity, transparency, and trustworthiness are not treated as optional quality attributes, but as governance commitments that structure design choices and accountability expectations (European Commission, 2017; European Commission, 2020). User centricity in this conceptualization implies that service design begins with life events and user journeys rather than administrative boundaries, which encourages simplification, pre filled forms, and coherent multi agency delivery. A related principle is the reduction of administrative burden, which is operationalized through the "once only" idea, meaning administrations should reuse data that is already available rather than repeatedly collecting it from citizens and businesses (European Commission, 2016). While the once only principle is often discussed as a service improvement tool, conceptually it is also a rule about state information behavior, because it requires lawful data reuse, auditable access, and clear responsibility for data quality. In parallel, the EU's rights based governance environment embeds constraints on data processing through the General Data Protection Regulation, which requires lawful bases, purpose limitation, and accountability for personal data processing in public administration (European Parliament & Council of the European

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Union, 2016). This legal baseline interacts with service innovation by shaping what "proactive" or "personalized" services can legitimately do and how transparency must be provided.

In Ukraine, value framing also emphasizes a service oriented state, but the conceptual narrative places stronger weight on visible citizen outcomes and rapid adoption as indicators of modernization. The Diia ecosystem embodies this orientation by consolidating services and digital documents into unified channels, which supports standardization of user experience and the perception of state capability through everyday interactions (Ministry of Digital Transformation of Ukraine, n.d.). Conceptually, this is a demand responsive service state logic, where the legitimacy of digitalization is reinforced through immediacy, usability, and high frequency services. At the same time, Ukraine's value framing strongly incorporates transparency and anti corruption expectations through open data and open contracting practices, which treat digitalization as an accountability instrument, not only as a service channel (Open Contracting Partnership, 2016). In comparative terms, the EU emphasizes a formalized value regime shaped by harmonized rights and cross border obligations, whereas Ukraine emphasizes a pragmatic value regime centered on rapid service delivery, administrative continuity, and public visibility. These logics are not contradictory, but they imply different implementation priorities and different pathways to trust.

Governance architecture and institutional responsibility. A defining conceptual feature of EU digital government is multilevel governance, where the EU sets legal and policy directions while member states implement, adapt, and operationalize them within their administrative systems. This produces a strong emphasis on harmonization and interoperability, because cross border functionality depends on consistent institutional behavior across jurisdictions. The Single Digital Gateway Regulation is a clear example of this conceptual architecture, as it combines obligations for information provision, procedural accessibility, and quality requirements for online services relevant to cross border mobility (European Parliament & Council of the European Union, 2018). It reflects a governance logic in which digital public services are part of the Single Market's functioning, not merely national administrative modernization. Another example is the evolution of electronic identification and trust services. The European Digital Identity framework, developed as an amendment to the eIDAS regime, reflects an institutional commitment to scalable trust infrastructure that can support public and private transactions under recognized standards (European Parliament & Council of the European Union, 2024a). In conceptual terms,

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

identity and trust services are governance building blocks that reduce uncertainty, enable lawful automation, and support cross border operability.

Ukraine's governance architecture differs primarily in the degree of central steering and the sequencing of ecosystem development. A dedicated institutional center for digital transformation supports coordinated decision making, common service standards, and rapid scaling across domains, which can reduce fragmentation in contexts where legacy administrative structures and registries are uneven. The conceptual governance challenge, however, is to ensure that central coordination remains compatible with legal accountability, data governance, and institutional checks, especially as digital services become critical infrastructure. Ukraine's Public Administration Reform Strategy for 2022 to 2025 frames digitalization as part of broader administrative capacity building, which is important conceptually because it links service delivery to institutional professionalism, policy coherence, and sustainable reform rather than to short term project outputs (Cabinet of Ministers of Ukraine, 2021). This linkage also clarifies that digital government requires governance capability, including regulatory clarity, budgeting, procurement integrity, and workforce competencies. From a comparative viewpoint, the EU's governance architecture relies on harmonized obligations and shared frameworks across multiple sovereign administrations, whereas Ukraine's relies on concentrated coordination to compress timelines and ensure coherence under constraints. These two architectures converge when Ukraine's reforms increasingly align with EU requirements, since alignment requires both infrastructure compatibility and governance compatibility.

Enabling infrastructures: interoperability, data governance, trust, and risk management. Interoperability is the most structurally decisive conceptual pillar because it converts isolated digital services into a coherent state capacity for integrated delivery. The European Interoperability Framework conceptualizes interoperability as multidimensional, requiring alignment in legal rules, organizational arrangements, shared semantics, and technical standards (European Commission, 2017). This approach is important because it shifts interoperability from a technical integration problem to an institutional design problem. Legal interoperability concerns whether data exchange and service coordination are permitted and regulated. Organizational interoperability concerns whether roles, responsibilities, and service ownership are defined across agencies. Semantic interoperability concerns whether data are defined consistently so that meaning is preserved across systems. Technical interoperability concerns protocols, interfaces, and security mechanisms for exchange. The EIF logic implies that progress

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

in technical integration without progress in legal and organizational alignment yields fragile or superficial interoperability. It also implies that a mature digital state invests in data governance regimes, registry quality, and auditability as much as in user facing portals.

Ukraine's Trembita system reflects a practical interoperability backbone that enables secure interagency exchange while preserving distributed ownership of registries. Conceptually, such a system operationalizes the once only logic by making data reuse feasible and by reducing the administrative need to request repeated information from citizens. Yet interoperability also increases exposure to governance risks, including unauthorized access, inconsistent data quality, and accountability ambiguity when multiple agencies contribute to a single service outcome. Therefore, the conceptual foundation must include cybersecurity and risk governance as baseline conditions. In the EU context, cybersecurity governance is reinforced through common legal baselines such as the NIS2 Directive, which frames cybersecurity as a systemic governance obligation rather than an agency level technical matter (European Parliament & Council of the European Union, 2022). Similarly, the AI Act introduces a risk based governance approach to AI systems, including those used in high impact contexts such as public administration decision processes, which conceptually extends digital government governance from data and identity into algorithmic accountability (European Parliament & Council of the European Union, 2024b). Ukraine's conceptual trajectory increasingly converges with these governance expectations through alignment and integration dynamics, particularly as digital services, data exchange, and identity systems become part of broader European digital space compatibility. The comparative implication is that interoperability and scale require a parallel strengthening of safeguards, including privacy compliance, cybersecurity resilience, and audit mechanisms. Without these, digitalization can increase systemic risk even while improving convenience.

The table 1.3 summarizes the core conceptual pillars and clarifies how each pillar translates into operational implications, making the comparison between the EU and Ukraine analytically explicit.

Conceptual convergence is strongest at the level of principles, while divergence is most visible in sequencing and governance architecture, especially regarding cross border obligations in the EU and centralized ecosystem scaling in Ukraine.

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Table 1.3. Conceptual pillars of digital government and their operational implications (EU and Ukraine)

Conceptual pillar	Operational implication in the EU	Operational implication in Ukraine
User centricity and life event design	Service integration across administrations and cross border usability requirements	Unified citizen facing channels and standardization of service journeys
Administrative burden reduction and once only logic	Data reuse with quality standards, accountability, and cross border consistency	Data exchange to reduce repeated submissions, rapid scaling of high frequency services
Interoperability as governance	Multilayer alignment across legal, organizational, semantic, technical dimensions	Infrastructure backbone for interagency exchange, registry coordination under central steering
Trust infrastructure and digital identity	Harmonized identity and trust services for secure transactions	Consolidated authentication and service access within a unified ecosystem
Rights, privacy, and lawful data governance	GDPR constrained service design and data processing accountability	Increasing institutionalization of data governance alongside service scaling
Cybersecurity and systemic resilience	Common baseline obligations and supervisory expectations	Resilience embedded through continuity oriented digital infrastructure and coordination
Algorithmic accountability and AI risk governance	Risk based oversight of high impact AI use cases	Gradual convergence toward risk governance as AI use expands in administration

Sources: systematized by the authors based on (European Commission, 2016; European Commission, 2017; European Commission, 2020; European Parliament & Council of the European Union, 2016; European Parliament & Council of the European Union, 2022; European Parliament & Council of the European Union, 2018; European Parliament & Council of the European Union, 2024b; Cabinet of Ministers of Ukraine, 2021; Ministry of Digital Transformation of Ukraine, 2025)

The table 1.4 provides a compact matrix that distinguishes between policy level commitments, governance mechanisms, and infrastructure readiness as three dimensions of institutionalization.

The EU model prioritizes harmonization and cross border consistency, while the Ukrainian model prioritizes accelerated delivery supported by central coordination; sustainable convergence depends on strengthening legal, audit, and risk governance in parallel with service expansion.

3. Institutional Change and Implementation Policy. Institutional change is the mechanism that converts digitalization from a sequence of projects into a durable administrative capability. In digital government, service quality and continuity depend on coordinated rules, roles, and infrastructures across agencies, because most high value services require multiple registries, approvals, and decision points. When institutions do not change, digital solutions often remain superficial, creating a “digital front office” while legacy workflows, duplicated data requests, and fragmented accountability persist in the back office.

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Table 1.4. Comparative institutionalization matrix for digital government (EU and Ukraine)

Dimension	EU: dominant pattern	Ukraine: dominant pattern
Policy commitments	Harmonized principles combined with cross border obligations	Service state orientation combined with administrative modernization strategy
Governance mechanisms	Multilevel coordination, standardization, monitoring cycles	Central steering and ecosystem consolidation for speed and coherence
Legal infrastructure	Strong rights baseline and harmonized sectoral obligations	Rapid development of enabling rules alongside service scaling and integration efforts
Core building blocks	Interoperability frameworks, identity and trust services, reusable components	Unified channels and interoperability backbone enabling integrated services
Risk governance	Cybersecurity baseline and AI risk based oversight	Increasing focus on resilience and safeguards as scale and complexity grow
Accountability orientation	Rights based accountability and cross border service quality expectations	Visibility and transparency orientation through digital instruments and open data culture

Sources: systematized by the authors based on (OECD, 2014; European Commission, 2017; European Commission, 2020; European Parliament & Council of the European Union, 2016; 2018; 2022; 2024a; 2024b; Cabinet of Ministers of Ukraine, 2021; Ministry of Digital Transformation of Ukraine, 2025

Contemporary frameworks therefore treat digital government as a governance reform that must align legal mandates, organizational design, data governance, financing, procurement, and workforce capacity (OECD, 2014). In the European context, institutional change is also shaped by cross border expectations, interoperability commitments, and rights based constraints that structure how data may be reused and how identity and trust services must operate (European Commission, 2017; European Parliament & Council of the European Union, 2016). In Ukraine, accelerated service scaling illustrates that institutional change can be compressed when central steering and shared building blocks are strong, but it still requires sustained policy instruments to stabilize coordination, registry quality, and accountability as complexity grows (Cabinet of Ministers of Ukraine, 2021; Ministry of Digital Transformation of Ukraine, 2025).

What "institutional change" means in digital government. Institutional change in this domain has at least five dimensions. First, it is legal change, meaning that statutes, bylaws, and administrative rules must permit digital channels, define lawful data exchange, and clarify liabilities for errors or unauthorized access. Second, it is organizational change, meaning that agencies redefine responsibilities for end to end services, not only for their internal segments of a process. Third, it is informational change, meaning that registries, data models, and metadata standards are treated as strategic public assets, with assigned ownership and quality

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

management. Fourth, it is technological change, but in a specific sense, namely the creation of reusable components, interoperability layers, identity solutions, and monitoring capabilities that can support scale. Fifth, it is cultural and professional change, meaning that civil servants acquire skills and routines for iterative service redesign, evidence based decision making, and risk management. These dimensions are interdependent. For example, interoperability can fail even with advanced technical interfaces if legal permissions are unclear or if agencies cannot agree on data definitions and accountability for outcomes. Similarly, a modern portal can fail to improve public value if service journeys are not redesigned and if performance is not measured beyond the number of digitized procedures.

A useful way to conceptualize institutional change is as a shift from "agency autonomy" toward "networked accountability." In a networked model, agencies remain legally distinct, but they share obligations for common outcomes, such as service completion, timeliness, and data accuracy. This is why governance frameworks emphasize whole of government coordination, interoperability governance, and shared building blocks (OECD, 2014; European Commission, 2017).

Implementation policy as a portfolio of instruments, not a single strategy. Implementation policy refers to the set of instruments that governments use to steer, finance, standardize, and audit digital transformation. It is not limited to a strategy document. A sustainable implementation policy typically combines three types of instruments. The first type is binding instruments, such as regulations on identity, data protection, cybersecurity, and cross border service obligations, which create enforceable minimum standards (European Parliament & Council of the European Union, 2016; European Parliament & Council of the European Union, 2022). The second type is coordination instruments, such as interoperability frameworks, reference architectures, service standards, and governance bodies, which reduce fragmentation and create a common operating model (European Commission, 2017). The third type is capability instruments, such as funding models, procurement rules, workforce development, and change management practices, which determine whether standards can be implemented in daily administrative routines (OECD, 2014).

In the EU, implementation policy has increasingly moved toward measurable steering through targets, monitoring, and coordinated cycles, reflecting a maturity shift from guiding principles to performance oriented governance (European Parliament & Council of the European Union, 2022). In Ukraine, implementation policy emphasizes rapid service delivery

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

through unified channels and strong central coordination, while progressively stabilizing institutional capacity through public administration reform objectives and interoperability infrastructure (Cabinet of Ministers of Ukraine, 2021; Ministry of Digital Transformation of Ukraine, 2025).

Core institutional reforms that enable digitalization at scale. A recurrent pattern across jurisdictions is that scale requires institutional reforms in four enabling domains.

Interoperability governance and registry coordination. Interoperability is an institutional problem before it is a technical problem, because it requires agreement on legal bases, responsibilities, semantics, and service ownership. The European Interoperability Framework formalizes this by defining interoperability across legal, organizational, semantic, and technical layers, implying that governments need governance structures and standards bodies that can manage these layers as a coherent system (European Commission, 2017). Ukraine's emphasis on interoperability infrastructure illustrates the same logic operationally, because secure interagency exchange enables integrated services only when registry quality, access rights, and accountability are defined and enforced (Ministry of Digital Transformation of Ukraine, 2025).

Identity, trust, and lawful digital interaction. Digital public services depend on trustworthy identification and legally recognized transactions. The EU has institutionalized this through the eIDAS framework and its later evolution toward a European Digital Identity framework, which demonstrates how trust services become a public infrastructure layer, not merely a convenience feature (European Parliament & Council of the European Union, 2024a). Implementation policy in this domain must also align with privacy and data protection requirements, because identity and service personalization increase the sensitivity of processing and therefore demand stronger accountability and transparency (European Parliament & Council of the European Union, 2016).

Cybersecurity and systemic resilience. As services become critical infrastructure, continuity and security become policy outcomes rather than purely technical concerns. The NIS2 Directive illustrates a governance approach that treats cybersecurity as a baseline obligation with institutional responsibilities and supervisory expectations (European Parliament & Council of the European Union, 2022). In practice, institutional change in cybersecurity includes governance structures, incident response readiness, monitoring, and a risk management culture embedded in everyday operations.

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Workforce capability and change management. Digital government requires competence in service design, data governance, procurement, risk management, and evaluation. Institutional change therefore includes training, professional standards, and HR incentives that support cross agency collaboration. The OECD approach stresses that digital government strategies require capacity building and governance arrangements that enable implementation, not only high level vision (OECD, 2014).

The table 1.5 clarifies what must change institutionally for digitalization to become an administrative capability rather than a set of standalone projects.

Table 1.5. Institutional Change Domains in Digital Government: Objectives, Mechanisms, and Typical Risks

Domain of institutional change	Primary objective	Typical governance mechanisms	Typical risks if underdeveloped
Legal and regulatory alignment	Lawful digital channels and data exchange	Digital by default rules, data sharing provisions, liability clarity	"Pilot legality," fragmented mandates, uncertainty in accountability
Organizational design and coordination	End to end service ownership	Cross agency steering, service managers, interagency agreements	Fragmentation, inconsistent service standards, slow dispute resolution
Data governance and registry quality	Reliable data reuse and auditability	Data owners, data stewards, metadata, quality controls	Poor data quality, semantic mismatch, low trust in registries
Shared building blocks and architecture	Reusable components and scale	Reference architectures, interoperability layers, shared identity services	Vendor lock in, duplicated solutions, integration fragility
Security, privacy, and risk governance	Trust and continuity of services	Risk management, security operations, privacy governance	Systemic cyber risk, privacy violations, service disruption
Workforce capability and culture	Sustainable implementation capacity	Training, professional standards, incentives	Resistance, skills gaps, "project fatigue," weak evaluation culture

Sources: systematized by the authors based on (European Commission, 2017; OECD, 2014; European Parliament & Council of the European Union, 2016; 2022)

Institutional change is multidimensional, and implementation fails most often when one domain advances rapidly while the others remain stagnant, especially governance and data quality.

Policy instrument design: how to prevent predictable implementation failures. Implementation policy must address predictable failure modes that recur in digital government reforms. One common failure is "portalism," where governments invest heavily in user interfaces but neglect registry modernization and interoperability, resulting in low automation and high

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

manual back office work. Another failure is "fragmented procurement," where agencies buy incompatible systems that cannot interoperate, producing high future integration costs and vendor dependence. A third failure is "risk externalization," where cybersecurity and privacy are treated as afterthoughts, increasing the probability of incidents that undermine trust. A fourth failure is "measurement failure," where success is defined by outputs such as number of services online rather than outcomes such as completion rates, time saved, error reduction, inclusion, and trust. EU governance instruments and cross border obligations implicitly counter these failures by requiring standards, quality criteria, and lawful trust infrastructure, while the Digital Decade approach strengthens the performance steering dimension (European Parliament & Council of the European Union, 2018; European Parliament & Council of the European Union, 2022). In Ukraine, centralized ecosystem scaling mitigates fragmentation, but it increases the importance of formal governance for data access, auditability, and long term sustainability as the ecosystem grows (Cabinet of Ministers of Ukraine, 2021).

The table 1.6 maps typical reform failures to policy instruments that can prevent them, emphasizing that implementation is a governance problem with predictable solutions.

Table 1.6. Implementation Policy Toolkit: Instruments Matched to Common Failure Modes

Common failure mode	Symptom in practice	Policy instrument response	Implementation focus
Portal without transformation	Digital channel exists but manual back office remains	Process redesign standards, interoperability governance	Redesign service journeys and automate decisions where lawful
Fragmented solutions	Multiple incompatible systems across agencies	Reference architecture, shared building blocks, procurement rules	Enforce reuse and interoperability requirements in procurement
Low trust and security incidents	Public reluctance to use services, disruptions	Security baseline, incident governance, privacy by design	Embed risk management and accountability in operations
Data reuse blocked	Repeated requests for the same information	Data governance, registry quality programs, access rules	Define data ownership, metadata standards, and lawful reuse
Weak outcomes measurement	Success measured by number of e services	Performance indicators, monitoring cycles, user feedback	Measure completion, time saved, equity, satisfaction, trust
Sustainability gap	Projects end, systems decay	Multi year financing, lifecycle governance, maintenance obligations	Fund operations, upgrades, and capacity building, not only pilots

Sources: systematized by the authors based on (OECD, 2014; European Commission, 2017; European Parliament & Council of the European Union, 2018&2022)

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Effective implementation policy is preventative: it anticipates typical failures and institutionalizes standards, governance, and incentives that make good outcomes the default.

Institutional roles and accountability architecture. Implementation requires a governance architecture that assigns responsibility for outcomes and controls, not only for technical delivery. A minimal architecture usually includes a central coordination unit that sets standards and monitors implementation, sectoral owners who manage domain registries and service portfolios, and cross cutting functions responsible for security, privacy, procurement integrity, and evaluation. EU practice often relies on multilevel governance, where common frameworks set direction and member states operationalize them, while cross border obligations require consistent service quality (European Commission, 2017; European Parliament & Council of the European Union, 2018). Ukraine's model demonstrates the capacity effects of strong central coordination for standardization and scaling, especially when unified channels and interoperability backbones are deployed (Ministry of Digital Transformation of Ukraine, 2025). In both contexts, accountability is strengthened when service ownership is explicit, when data owners are assigned, and when auditability is built into access and processing.

The table 1.7 outlines core roles and responsibilities that institutionalize coordination and accountability in digital transformation.

Governance roles institutionalize transformation by making coordination and accountability explicit; without them, scale produces fragmentation and unmanaged risk.

4. Monitoring, evaluation, and policy learning as institutional routines. A mature digital government implementation policy institutionalizes monitoring and evaluation as continuous administrative routines, because digital services behave as socio technical systems whose performance depends on law, process design, data quality, security, and user capabilities, not only on software functionality (OECD, 2014). Monitoring, in this context, is the systematic collection of performance signals at a frequency that supports management decisions, while evaluation is a structured assessment that explains why performance looks as it does, attributes effects to interventions where feasible, and formulates recommendations for redesign or policy adjustment. In the European Union, this logic is reinforced by a target and measurement orientation within the Digital Decade governance approach, which frames digital transformation as a measurable policy agenda rather than a set of isolated projects (European Parliament and Council of the European Union, 2022).

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Table 1.7. Minimum Governance Architecture for Digital Government Implementation

Role or body	Core responsibility	Typical deliverables	Key accountability question
Central digital coordination authority	Standards, portfolio steering, monitoring	Service standards, reference architecture, maturity monitoring	Who ensures coherence across government
Service owner (end to end)	Journey redesign and performance	Process maps, automation roadmap, service KPIs	Who is accountable for outcomes, not steps
Registry and data owner	Data quality, lawful access, metadata	Data catalog, quality controls, access policies	Who guarantees correctness and reuse conditions
Security governance function	Cyber risk management and continuity	Risk registers, incident plans, monitoring	Who guarantees resilience and response readiness
Privacy and compliance function	Lawful processing and transparency	DPIA routines, processing registers, guidance	Who ensures rights and lawful data practices
Procurement and vendor management	Interoperable purchasing and lifecycle control	Model contracts, interoperability clauses, SLAs	Who prevents vendor lock in and fragmentation
Evaluation and audit function	Outcomes measurement and accountability	Performance reviews, user feedback loops	Who validates public value and equity impacts

Sources: systematized by the authors based on (OECD, 2014; European Commission. (2017; European Parliament & Council of the European Union, 2016; European Parliament & Council of the European Union, 2022)

Conceptually, monitoring should be organized across multiple levels: service level (user journeys and completion), organizational level (capacity, interoperability, and workflow integrity), and system level (equity, trust, resilience, and compliance). This multilevel structure matters because an apparent improvement in portal usage can coexist with deterioration in data quality or growing cybersecurity exposure, creating misleading "success narratives" if monitoring is narrowly defined. A further requirement is comparability over time and across agencies, which demands standardized indicator definitions, stable measurement protocols, and clear data ownership for each metric. The European Interoperability Framework supports this institutional perspective by emphasizing that interoperable digital public services require organizational and legal alignment in addition to technical exchange, which implies that monitoring must also include governance and coordination indicators, not only technical uptime (European Commission, 2017).

Monitoring systems should therefore combine operational indicators with outcome oriented indicators. Operational indicators include service availability, response time, and processing time, but they must be interpreted alongside quality indicators such as error rates, rework loops, and the share

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

of cases that require manual intervention. Outcome indicators include completion rates, user satisfaction, and time and cost savings for users and government, but these outcomes require careful operationalization to avoid measuring convenience for some groups while invisibilizing barriers for others. Inclusion and accessibility indicators are conceptually central because digital transformation can widen the digital divide if design assumes high digital literacy, stable connectivity, or modern devices, thereby undermining equity and trust (United Nations Department of Economic and Social Affairs, 2024). In addition, trust and legality are not abstract values but measurable conditions of adoption, so monitoring should include complaints, appeals, data protection incidents, and transparency indicators that reflect whether citizens perceive the digital state as legitimate and safe (European Commission, 2020; European Parliament and Council of the European Union, 2016). In the Ukrainian case, systematic monitoring is especially important because rapid scaling of services increases systemic complexity, which raises the need for performance management, registry governance, and risk controls to preserve continuity and public confidence (Cabinet of Ministers of Ukraine, 2021).

Evaluation and policy learning should be institutionalized as a feedback loop that links evidence to decisions, budgets, and redesign cycles. A practical model is to connect continuous monitoring dashboards with periodic evaluations that test hypotheses about bottlenecks, such as whether low completion rates are driven by usability issues, interoperability failures, legal constraints, or insufficient support for vulnerable groups. Policy learning is strengthened when evaluation outputs are translated into change requests with named owners, deadlines, and measurable acceptance criteria, rather than remaining as narrative reports. It is also strengthened when services are treated as products with lifecycle governance, meaning that each service has a roadmap, a backlog of improvements, and a structured review of risks and user feedback. Finally, learning should incorporate risk governance, because cybersecurity and privacy failures can erase adoption gains quickly, making resilience metrics and incident readiness part of regular performance reviews rather than exceptional audits (European Parliament and Council of the European Union, 2022; European Parliament and Council of the European Union, 2016).

Table 1.8 introduces a multilevel monitoring and evaluation architecture that clarifies what should be measured, why it matters, and how frequently it should be reviewed.

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Table 1.8. Multilevel monitoring and evaluation architecture for digital government implementation

Level	Core evaluation question	Illustrative indicators	Typical frequency	Primary owner
Service level (user journey)	Do users complete the service successfully and with low burden	Completion rate, drop off points, time to complete, share of cases requiring manual follow up	Weekly to monthly	Service owner and product team
Process level (back office)	Is the workflow stable, predictable, and auditable	Processing time, rework rate, exception handling rate, automation share	Monthly	Process owner and operations
Data and interoperability level	Is data reuse lawful, correct, and consistent across systems	Data quality score, interoperability failure rate, registry synchronization issues, semantic mismatch incidents	Monthly to quarterly	Registry and data owner
Trust and rights level	Are rights protected and legitimacy sustained	Complaints, appeals, data protection incidents, transparency response time	Quarterly	Privacy and compliance function
Security and resilience level	Can the system resist and recover from incidents	Incident frequency and severity, recovery time, patch compliance, continuity test results	Monthly to quarterly	Security governance function
System level (policy steering)	Is digitalization improving public value and inclusion	Equity of access by group, satisfaction distribution, net burden reduction, strategic target progress	Quarterly to annual	Central coordination authority

Sources: systematized by the authors based on (European Commission, 2017; European Commission, 2020; European Parliament and Council of the European Union, 2016; European Parliament and Council of the European Union, 2022; OECD, 2014)

A multilevel architecture prevents overreliance on single metrics by linking service convenience to governance quality, rights protection, and resilience, which is essential for sustainable scale.

Table 1.9 proposes a compact indicator set that balances operational performance, outcomes, equity, trust, and risk, so that policy learning can be evidence based rather than anecdotal.

A balanced indicator set supports policy learning by making trade offs visible, especially between speed, equity, legality, and resilience.

Conclusion. The public administration digitalization should be interpreted primarily as an institutional transformation, not as a narrow programme of IT modernization. This distinction is substantive because the quality and legitimacy of digital public services are determined by governance capacity, namely the ability to align law, procedures, organizations, data, and accountability mechanisms, rather than by the presence of advanced software alone.

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Table 1.9. Core indicator set for monitoring digital public services and governance quality

Indicator family	What it captures	Example indicators (definition focus)	Decision use
Service performance	Reliability and usability	Availability, median completion time, drop off rate by step	Operational improvements and UX redesign
Administrative burden	Burden reduction for users and businesses	Number of required documents, number of interactions, time saved estimates	Process simplification and once only implementation planning
Outcome quality	Whether the service delivers intended results	Error rate, appeal rate, correction rate, decision timeliness	Quality management and legal process refinement
Inclusion and accessibility	Equity of access and usability	Completion rate by demographic proxy, accessibility conformance, assisted service usage	Targeted support and inclusive design interventions
Trust and legitimacy	Perceived safety and fairness	Satisfaction distribution, complaint rate, transparency response time	Trust building measures and accountability improvements
Data governance and interoperability	Integrity of shared data and coordination	Data quality score, interoperability failure rate, registry mismatch incidents	Registry modernization and coordination governance
Security and resilience	Exposure to systemic risk	Incident rate, mean time to recover, continuity test pass rate	Risk mitigation, investment prioritization, resilience planning

Sources: systematized by the authors based on (Cabinet of Ministers of Ukraine, 2021; European Commission, 2020; European Parliament and Council of the European Union, 2016; European Parliament and Council of the European Union, 2022; United Nations Department of Economic and Social Affairs, 2024; OECD, 2014)

The historical progression from informatization to value based resilient digital government clarifies that each subsequent stage increases interdependence across agencies and raises the cost of fragmentation. In early phases, efficiency gains can be achieved within single institutions, but at higher maturity levels, the decisive factor becomes the state's capacity to deliver end to end services across organizational boundaries, supported by consistent rules for data reuse and coordinated responsibility for outcomes.

From the EU perspective, the experience demonstrates how reform principles become durable when they are institutionalized through coordinated commitments, interoperability frameworks, and measurable steering instruments. In this model, interoperability is treated as a multi layer governance requirement, covering legal permission for data exchange, organizational agreements on roles, shared semantics that preserve meaning across registries, and technical standards that ensure secure exchange. Consequently, the EU pathway illustrates that sustainability depends on the ability to transform principles into routine administrative obligations,

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

monitoring practices, and shared building blocks that reduce duplication and prevent incompatible solutions.

Ukraine's experience complements this logic by showing that accelerated scaling is feasible when unified service channels and interoperability backbones are developed in parallel. A unified interface increases adoption and standardizes service experience, while interoperability infrastructure makes integration operational by enabling secure interagency exchange and reducing repetitive administrative requests. At the same time, accelerated implementation heightens the need for continuous strengthening of legal alignment, safeguards, and institutional accountability, because complexity grows quickly as services multiply and data flows expand.

Across both contexts, performance management and policy learning emerge as core conditions for maturity. Monitoring must be multilevel and outcome oriented, covering service completion and burden reduction, but also equity, trust, and resilience, so that success is not reduced to counts of digital services. Overall, the findings support a governance centered model of digital transformation in which service expansion is continuously balanced with rights protection, cybersecurity readiness, and transparent accountability.

Funding. The authors declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The authors declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Cabinet of Ministers of Ukraine. (2021). *Strategy for public administration reform in Ukraine for 2022–2025*. https://www.kmu.gov.ua/storage/app/sites/1/reforms/pars-2022-2025-eng.pdf
2. European Commission. (2016). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU eGovernment Action Plan 2016–2020. Accelerating the digital transformation of government* (COM(2016) 179 final).

ISBN 978-9916-9389-0-4 (pdf)

EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016DC0179
3. European Commission. (2017). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Interoperability Framework – Implementation Strategy* (COM(2017) 134 final). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52017DC0134
4. European Commission. (2017, October 6). *Ministerial Declaration on eGovernment: The Tallinn Declaration*. https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration
5. European Commission. (2020, December 8). *Berlin Declaration on Digital Society and Value-Based Digital Government*. https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-governmentdigital-strategy.ec.europa.eu
6. European External Action Service. (2025, April 23). *European Union supports Ukraine's digital path to the EU (DT4UA project results)*. https://www.eeas.europa.eu/delegations/ukraine/european-union-supports-ukraine%E2%80%99s-digital-path-eu-dt4ua-project-results_en
7. European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
8. European Parliament and Council of the European Union. (2018). *Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2018/1724/oj/eng
9. European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive)*. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
10. European Parliament and Council of the European Union. (2022). *Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030*. EUR-Lex. https://eur-lex.europa.eu/eli/dec/2022/2481/oj/eng
11. European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
12. European Parliament and Council of the European Union. (2024). *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)*. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
13. EU4Digital. (2025). *EGOV4Ukraine*. Retrieved December 9, 2025, from https://eufordigital.eu/discover-eu/egov4ukraine/
14. Interoperable Europe Portal. (2025). *Governance: Ukraine*. Retrieved December 9, 2025, from https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/governance-ukraine

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

15. Kutkov, O., Zolotov, A., Akimova, L., & Akimov, O. (2025). Digital Transformation of Social Governance: Economic Challenges and Opportunities of Smart Cities. *Economics, Finance and Management Review*, (1(21), 17–28. https://doi.org/10.36690/2674-5208-2025-1-17-28
16. Karpa, M., Akimov, O., & Kitsak, T. (2022). Problems of Stabilization of the System of Public Administration under the Conditions of Decentralizational Changes and Martial Law in Ukraine. *Public Administration and Law Review*, (3), 24–31. https://doi.org/10.36690/2674-5216-2022-3-24
17. Ministry of Digital Transformation of Ukraine. (2025). *Diia (GovTech project description)*. Retrieved December 9, 2025, from https://digitalstate.gov.ua/projects/govtech/diia
18. OECD. (2014). *Recommendation of the Council on Digital Government Strategies* (OECD/LEGAL/0406). OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406
19. OECD Observatory of Public Sector Innovation. (2025). *E-procurement system ProZorro*. Retrieved December 9, 2025, from https://oecd-opsi.org/innovations/eprocurement-system-prozorro
20. Open Contracting Partnership. (2016, July 28). *ProZorro: How a volunteer project led to nation-wide procurement reform in Ukraine*. https://www.open-contracting.org/2016/07/28/prozorro-volunteer-project-led-nation-wide-procurement-reform-ukraine/
21. Open Data Portal of Ukraine. (n.d.). *Open data portal*. Retrieved December 9, 2025, from https://data.gov.ua/en
22. Serhieiev, V., Voronina, Y., Zolotov, A., Akimova, L., Rovynska, K., & Akimov, O. (2025). Innovative competences within public administration landscape: sustainable development, financial efficiency and national security strengthening vectors. *Sapienza: International Journal of Interdisciplinary Studies*, *6*(1), e25017. https://doi.org/10.51798/sijis.v6i1.947
23. State Enterprise Diia. (2025). *Open Data Web Portal*. Retrieved December 9, 2025, from https://se.diia.gov.ua/en/opendata
24. State Enterprise Diia. (2025). *Trembita: System of Electronic Interaction of State Electronic Information Resources*. Retrieved December 9, 2025, from https://se.diia.gov.ua/en/trembita
25. Sydorchuk, O. ., Bashtannyk, V. ., Terkhanov, F. ., Kravtsov, O. ., Akimova, L. ., & Akimov, O. . (2024). Integrating digitization into public administration: Impact on national security and the economy through spatial planning. *Edelweiss Applied Science and Technology*, *8*(5), 747–759. https://doi.org/10.55214/25768484.v8i5.1740
26. 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. https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf

https://doi.org/10.36690/PUBADM ISBN 978-9916-9389-0-4 (pdf)

Public Administration 4.0: Leveraging Digital Tools for Effective Governance

Monograph

Number of copies: 300
First printing: December 12, 2025
DOI: https://doi.org/10.36690/PUBADM
Distributed worldwide by Scientific Center of Innovative Research OÜ office@scnchub.com
Full text available online at https://scnchub.com

https://doi.org/10.36690/PUBADM
ISBN 978-9916-9389-0-4 (pdf)