Innovative
Scientific
Center
Research

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

Introduction 4

Chapter 1. Digital Public Governance: Conceptual Frameworks, International Models and AI Driven Public Services 8

Section 1.1. Digitalization of Public Administration: Conceptual Foundations, Institutional Change, and Implementation Policy
Oleksandr Akimov, Liudmyla Akimova 9

Section 1.2. International Practices of Digital Governance: Lessons, Policy Transfer, and Adaptation to National Context
Volodymyr Zahorskyi, Andriy Lipentsev 32

Section 1.3. Digital Era of Public Administration: Using Artificial Intelligence to Improve the Efficiency of Public Services
Volodymyr Panchenko, Oksana Panchenko 53

Chapter 2. Public Governance of Digital Accounting and Reporting: Risk-Based Supervision, Anti-Fraud Policy, and Economic Security 78

Section 2.1. Risk-Based Digital Supervision and Anti-Fraud Governance: Policy Instruments, Compliance, and Administrative Burden Reduction
Iryna Mihus 79

Section 2.2. Public Administration of the Digitalization of Accounting and Reporting in Ukraine
Vira Shepeliuk 102

Section 2.3. Quality of digital reporting: risks, precautions, and government oversight mechanisms
Zinaida Zhyvko 132

Chapter 3. Public Administration in the Architecture of Security: National, Economic, and Energy Policy Contexts 154

Section 3.1. The Role and Significance of Public Administration in the System of Ensuring National Security of EU Countries Against the Background of a Full-Scale Invasion of Ukraine
Julian Maj, Tomasz Gorski, Paulina Kolisnichenko 155

Section 3.2. Public Administration in Ensuring the Economic Security of the State: Digital Tools and Management Innovations
Yana Koval, Alona Zahorodnia 182

Section 3.3. Public Governance of Energy Policy: Evidence from the Visegrád Group Countries
Dmytro Tkach 206

Conclusion 241
References 246

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 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 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

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.*

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 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 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

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.

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.

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 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 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.

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 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)

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).

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 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.

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.

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, 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).

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

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

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

Section 1.2. International Practices of Digital Governance: Lessons, Policy Transfer, and Adaptation to National Context

Volodymyr Zahorskyi[1], Andriy Lipentsev[2]

[1]Doctor of Economic Sciences, Professor, Honored Worker of Science and Technology of Ukraine, Academician of the Academy of Economic Sciences of Ukraine, Ukrainian National Forestry University, Lviv, Ukraine, ORCID: https://orcid.org/0000-0003-3260-3271

[2]Ph.D. (Economics), Professor, Honored Worker of Education of Ukraine, Head of the Center for Professional Development, Professor of the Department of Public Management and Administration, Deputy Head of the Department, Ukrainian National Forestry University, Lviv, Ukraine, ORCID: https://orcid.org/0000-0001-8960-3059

Citation:
Zahorskyi, V. & Lipentsev, A. (2025). International Practices of Digital Governance: Lessons International Practices of Digital Governance: Lessons. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 32-52). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-32-52

Abstract. *Digital governance reforms are frequently evaluated through visible artefacts, such as portals, apps, and platforms, yet sustained public value depends on institutional mechanisms that secure lawful data use, interoperability, accountability, and inclusion. The goal of this study is to structure international learning in digital governance through three interlinked lenses, namely lessons, policy transfer, and adaptation to national context. Methodologically, the study applies qualitative policy synthesis and comparative institutional reasoning to trace how international practices are translated into domestic reform design. Within this approach, lessons are formulated as conditional propositions that connect outcomes to causal mechanisms and to enabling conditions, and these propositions are assessed through triangulated evidence rather than single-source success narratives. Policy transfer is treated as a process of institutional translation shaped by actors, channels, and incentives, which explains why reform elements often travel as modular components rather than as complete models. Adaptation is examined through dependency and fit assessment, focusing on whether the receiving context can operationalize the prerequisites that make transferred mechanisms work in practice. The analysis indicates that lessons become transferable only when outcomes, mechanisms, enabling conditions, and evidence standards are made explicit, because this reduces artefact imitation and improves the precision of reform design. It also shows that policy transfer most commonly moves components such as interoperability frameworks, service standards, and digital identity, but implementation success depends on institutionalizing hidden dependencies, including clear legal bases, enforceable authority, data stewardship, procurement discipline, and the sequencing of safeguards and capacity building before scaling. Overall, international practice is most useful when knowledge travels as enforceable routines and institutional capabilities and when performance management prioritizes completion, administrative burden reduction, equity, trust, and resilience over digitization counts.*

Keywords: *digital governance; international practices; lesson drawing; policy transfer; adaptation; institutional design; interoperability; data governance; digital identity; public value; trust; resilience.*

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

1. Lessons in digital governance. In this study, a “lesson” is conceptualized as a transferable, evidence based proposition that links a public outcome to a causal mechanism and to the enabling conditions that make the mechanism operational. This definition is necessary because digital governance reforms are frequently communicated through visible artefacts, such as portals, apps, dashboards, or branded platforms, while durable performance is usually produced by less visible institutional arrangements, including lawful data reuse, cross agency accountability, registry stewardship, procurement discipline, and service lifecycle governance. A lesson is therefore not a technology and not a narrative about “success”, it is a conditional claim that can be tested against data and revised when evidence contradicts the initial hypothesis. Lesson drawing is rigorous only when it is problem driven. It begins with a clearly stated administrative failure and a measurable baseline, then searches for external experience that plausibly addresses that specific failure, rather than selecting a reference case because it is famous or highly ranked. The baseline matters because it determines what “improvement” means and prevents the common error of equating adoption with public value.

A lesson becomes analytically valid when three elements are explicitly specified. The first element is the outcome, including its distribution across groups and regions, because reforms can raise average performance while increasing inequality of access. The second element is the mechanism, meaning the operational pathway that produced the outcome, for example end to end process redesign plus lawful data reuse, or service standards plus enforceable service ownership and assessment routines. The third element is the enabling conditions, meaning the legal, organizational, informational, financial, and risk governance prerequisites that activate the mechanism. If any of these elements is missing, the lesson tends to collapse into artefact imitation. Artefact imitation is predictable in digital reforms because interfaces are easier to replicate than governance authority, registry quality, or interagency coordination. As a result, governments may import a portal and still preserve a manual back office, or they may adopt standards and still have no institution capable of enforcing compliance.

A robust lesson drawing workflow follows a logical sequence. First, the analyst defines the domestic problem in measurable terms, such as repetitive document submission, low service completion, high error rates, long processing times, low trust, or exclusion of low capacity users. Second, the analyst selects reference cases by functional similarity, not by reputational status, and collects evidence beyond promotional narratives. Third, the analyst reconstructs causality, separating the access layer from the transformation layer, and identifying which rule changes, incentives, and governance routines were necessary to make the mechanism work. Fourth, the analyst maps enabling conditions and then performs a fit assessment in the receiving context, asking which prerequisites exist, which are missing, and which substitutes are feasible within legal and administrative constraints. Fifth, the analyst formulates the lesson as a conditional proposition with indicators and decision thresholds, so that implementation is evaluated through outcomes and not through output counts. Finally, the analyst designs a monitoring and learning loop, because digital governance reforms behave as socio technical systems, and they require iterative adjustment as demand grows and risks evolve.

The Table 1.10 specifies how to express lessons as testable propositions, making implicit assumptions explicit and strengthening analytical transferability.

Table 1.10. Structure of a testable lesson in digital governance

Component	What must be specified	Typical operational form	Why it matters
Outcome	What improves, for whom, and with what equity profile	Completion rate, time to completion, error rate, burden reduction, accessibility metrics	Prevents success being reduced to adoption or website visits
Mechanism	The causal pathway that produces the outcome	End to end redesign, lawful data reuse, enforced standards, shared building blocks	Avoids artefact copying and clarifies active ingredients
Enabling conditions	The institutional prerequisites that activate the mechanism	Legal bases, authority, data stewardship, procurement rules, risk governance	Makes feasibility explicit and supports sequencing
Evidence standard	What evidence justifies the claim	Administrative data, audits, user research, distributional analysis	Protects against narrative bias and selection effects
Evaluation rule	When the lesson is considered successful	Thresholds, trends, and equity constraints	Enables governance decisions, scale, pause, redesign
Adaptation note	What must change in the receiving context	Substitutes, phased implementation, safeguards	Converts learning into implementable design

Sources: (OECD, 2014; OECD, 2020; Rose, R.,1991; United Nations Department of Economic and Social Affairs, 2024)

Lessons are more likely to “travel” when they are formulated as outcome plus mechanism plus enabling conditions, with explicit evidence standards and evaluation rules.

A further deepening of lesson drawing requires differentiating the kinds of evidence that can support a lesson. Digital governance claims often rely on anecdotes or rankings, yet robust lessons depend on triangulation.

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

Administrative data can show completion, processing time, and error rates, but it may not explain why users drop out. User research can explain friction, trust concerns, and accessibility barriers, but it may not capture system wide impacts. Audit and compliance evidence can reveal whether rules are followed and whether data sharing is lawful and accountable. Distributional analysis can reveal whether improvements are concentrated among digitally skilled groups. A strong lesson therefore combines quantitative indicators with qualitative evidence, and it treats "success" as a multi-dimensional condition involving public value, rights protection, and resilience.

The Table 1.11 proposes an evidence ladder for lesson credibility, emphasizing triangulation rather than a single "best" method.

Table 1.11. Evidence ladder for validating lessons in digital governance

Evidence type	What it can credibly support	Typical indicators or artefacts	Key limitation
Administrative performance data	Whether outcomes changed over time	Completion, processing time, error rates, cost proxies	Weak explanation of causality without process insight
Process and workflow evidence	Whether mechanisms actually changed	Journey maps, automation share, exception handling rates	Can miss user experience and distributional effects
User research and accessibility audits	Why users succeed or fail	Usability findings, accessibility compliance, trust concerns	May not generalize without sampling and baselines
Compliance, privacy, and security evidence	Whether safeguards and legality are real	DPIA routines, incident logs, audit findings, access logs	Often underreported or inconsistent across agencies
Distributional and inclusion analysis	Who benefits and who is excluded	Completion by group, assisted channel use, regional disparities	Depends on data availability and ethical measurement design
Comparative benchmarking	Whether progress aligns with peers	Maturity indicators, cross country comparisons	Risks rewarding visibility and encouraging cosmetic reforms

Sources: (OECD, 2014; OECD, 2020; United Nations Department of Economic and Social Affairs, 2024)

Lesson validity increases when outcome claims are supported by multiple complementary evidence types that jointly address performance, causality, safeguards, and inclusion.

Another deep requirement is mechanism precision. Many reforms declare a goal, such as "once only" or "user centricity," but the lesson is not the slogan. The lesson is the institutional mechanism that makes the slogan operational. For example, "once only" becomes real only when lawful data reuse is combined with registry governance, semantic standards, and

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

enforceable cross agency interoperability. Similarly, user centricity becomes operational only when service ownership is end to end, when teams can redesign processes rather than merely publish information online, and when performance metrics reward completion and burden reduction. Mechanism precision is also essential for sequencing. A government that scales the front office first may generate demand that the back office cannot absorb, increasing delays and dissatisfaction. Conversely, investing in back office interoperability without service redesign can produce infrastructure that is technically impressive but weakly used.

The Table 1.12 maps frequent lesson mechanisms to the institutional dependencies that must be checked before transfer.

Table 1.12. Common lesson mechanisms in digital governance and their dependency profile

Mechanism (lesson level)	What it changes in practice	Primary dependencies	Typical false lesson
Lawful data reuse and once only operation	Eliminates repeated submissions, enables automation	Legal basis, registry stewardship, semantics, auditability	“APIs alone create once only”
End to end service ownership	Improves completion and reduces handoffs	Mandated owner, escalation rights, cross agency agreements	“A portal creates integrated services”
Service standards with assessment	Raises quality and consistency	Enforcement authority, measurement, procurement alignment	“Publishing standards is sufficient”
Shared building blocks and reference architecture	Reduces duplication, increases reuse	Architectural governance, lifecycle funding, procurement clauses	“Buying a platform equals reuse”
Monitoring and learning loop	Sustains improvement over time	Stable indicators, feedback routines, decision authority	“Reporting dashboards produce learning”
Inclusion by design with assisted channels	Reduces exclusion and increases legitimacy	Accessibility governance, support services, outreach	“Digital only is more efficient for all”

Sources: (OECD, 2014; OECD, 2020; United Nations Department of Economic and Social Affairs, 2024)

Mechanisms are the core of transferable learning, and dependency mapping prevents the common error of importing surfaces while omitting institutional prerequisites.

Because enabling conditions are often the true constraints, lesson drawing should include a structured fit assessment before any adoption decision is made. Fit assessment is not a generic checklist, it is a constraint analysis linked to the specific mechanism. If the mechanism is lawful data reuse, the key questions concern legal permissions, data ownership, auditability, and registry quality. If the mechanism is service standard enforcement, the key questions concern authority, incentives, and procurement alignment. If the mechanism is trust infrastructure, the key questions concern privacy governance, security operations, incident response, and inclusion. A fit assessment also enables a realistic minimum viable sequence, specifying what must be built first to activate the mechanism, and what can be added later without undermining legality or equity.

The Table 1.13 provides a fit assessment matrix that aligns enabling conditions with the kind of mechanism being transferred.

Table 1.13. Fit assessment matrix for lesson feasibility in the receiving context

Enabling condition domain	Fit question	Minimum viable requirement	Common gap pattern
Legal interoperability	Is data exchange lawful and accountable	Clear legal basis, purpose limits, liability clarity	Informal exchange substitutes for lawful design
Institutional authority	Who can enforce cross agency rules	Mandate, escalation rights, compliance monitoring	Coordination without enforcement power
Registry and data stewardship	Can data be reused reliably	Data owner roles, quality controls, metadata	Poor data quality prevents automation
Procurement and lifecycle funding	Can reuse be enforced through contracts	Interoperability clauses, portability, O and M funding	One-off projects, fragmented procurement
Safeguards and resilience	Can trust be maintained at scale	Privacy governance, security baselines, incident routines	Safeguards postponed until after scaling
Inclusion capacity	Can low capacity users complete services	Accessibility compliance, assisted channels, support	Digital divide widens, legitimacy declines

Sources: (OECD, 2014; United Nations Department of Economic and Social Affairs, 2024)

Fit assessment turns lesson drawing into implementable design by making constraints explicit and by supporting phased sequencing based on mechanism activation.

Finally, a deep lesson drawing approach must clarify how lessons become operational decisions. A lesson is not complete until it is translated into a decision rule, such as when to scale, when to pause, and what redesign is required. This requires outcome thresholds and equity constraints, not merely target statements. For example, a service may be scaled only if completion exceeds a threshold for the general population and does not fall below an acceptable threshold for vulnerable users, and if error rates and complaint rates remain within defined bounds. These decision rules protect against output inflation, meaning the tendency to declare success by counting digitized services while ignoring the burden and exclusion that users experience.

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

The Table 1.14 offers templates that translate lessons into operational statements and decision rules that support accountability and learning.

Table 1.14. Templates for operationalizing lessons into governance decisions

Template element	Example formulation	Implementation use
Lesson statement	If outcome X is targeted, mechanism M is expected to improve X, provided conditions C are met	Forces explicit causality and prerequisites
Indicator set	Completion, burden reduction, error rates, accessibility compliance, complaint rate	Prevents single-metric success narratives
Decision thresholds	Scale if completion rises and equity gap narrows, pause if error rate rises	Creates actionable governance control
Learning trigger	Redesign if drop-off concentrates in one step or one group	Links evidence to iterative improvement
Risk trigger	Halt automation expansion after significant incident until controls are verified	Protects trust and legitimacy

Sources: (OECD, 2014; OECD, 2020; United Nations Department of Economic and Social Affairs, 2024)

When lessons are linked to indicators and thresholds, they become governable, and reform becomes a managed learning process rather than a one-time launch event.

The "lessons" perspective demonstrates that effective digital governance learning requires more than identifying attractive technological solutions or highly visible reforms. A lesson is analytically meaningful only when it specifies the targeted public outcome, the causal mechanism that generated change, and the enabling legal, institutional, data, procurement, and safeguard conditions that make the mechanism workable in practice (OECD, 2014; OECD, 2020). This logic reduces artefact bias by separating interfaces from back-office transformation and by clarifying which institutional capacities must be built before scaling. It also strengthens legitimacy by integrating inclusion, trust, and resilience into lesson formulation and evidence standards, ensuring that performance improvements are assessed not only in aggregate but also across groups and regions (United Nations Department of Economic and Social Affairs, 2024). Finally, by translating lessons into explicit indicators and decision rules, lesson drawing becomes a governed learning process that supports iterative improvement rather than one-time launches (Rose, 1991).

2. Policy transfer in digital governance. Policy transfer in digital governance refers to the process through which knowledge about policies, institutions, instruments, and administrative arrangements from one jurisdiction is used to design, justify, or implement reforms in another. In the classic formulation, the core analytical questions are who transfers, what is transferred, why transfer occurs, through which channels it travels, and which constraints shape feasibility and outcomes (Dolowitz & Marsh, 2000). Digital governance is a particularly intensive transfer field because reform objects are modular and easily packaged as standards, maturity models, reference architectures, playbooks, and procurement templates. However, the portability of these objects is deceptive, because their effectiveness depends on institutional prerequisites that often remain implicit. Consequently, transfer should not be treated as a technical import or a procurement decision. It is a governance process that redistributes authority, redefines accountability for service outcomes, and restructures data flows across agencies (OECD, 2014; OECD, 2020). The central risk is therefore not "wrong technology," but the adoption of artefacts without the mechanisms and enforcement capacity that produced success in the reference context.

A crucial distinguishing feature of digital governance transfer is that what travels is rarely a complete model. More commonly, jurisdictions transfer partial elements such as interoperability frameworks, service standards, digital identity components, data governance templates, cybersecurity baselines, and delivery routines. These elements are often adopted by different actors at different times, which can fragment reform logic if coordination is weak. For example, a central unit may transfer a service standard, while sectoral agencies procure incompatible systems that undermine reuse, or donors may support parallel platforms that satisfy reporting requirements but complicate long term integration. Transfer channels also shape outcomes. Peer learning may enable deeper understanding and gradual adaptation, whereas benchmarking environments tend to privilege visible deliverables, potentially encouraging interface first digitization. Vendor and consultant channels can accelerate deployment by packaging solutions, but they also increase lock in and institutional dependency risks if contracts do not protect interoperability, portability, and lifecycle accountability (Peck & Theodore, 2010). In addition, the motive for transfer matters. Problem solving motives tend to generate stronger fit assessment and realistic sequencing, whereas legitimacy motives can encourage symbolic adoption that "looks modern" while leaving back office processes unchanged (Dolowitz & Marsh, 2000).

Another feature is the speed at which transfer occurs. Digital reforms often diffuse under crisis conditions or political cycles, creating pressure to deliver quick wins. Speed can be beneficial when it breaks inertia, yet it also increases the probability of "fast policy" failure, meaning that safeguards, auditability, and capacity building lag behind scaling (Peck & Theodore, 2010). This is especially consequential because digital governance reforms expand data sharing, automation, and reliance on common infrastructures. If privacy governance, cybersecurity readiness, and continuity routines are underdeveloped, a single incident can erode trust and suppress adoption, thereby converting technical progress into political and institutional regression (OECD, 2014). For that reason, a governance centered view treats transfer as a staged translation process: clarify the mechanism, map dependencies, design enforceable roles, pilot with measurable outcomes, then scale with monitoring and corrective authority.

The Table 1.15 distinguishes what typically transfers in digital governance and highlights the hidden dependencies that determine whether transferred components can function as intended.

Table 1.15. Transfer objects in digital governance and their institutional dependencies

Transfer object	Typical purpose in reforms	High dependency conditions	Failure mode when dependencies are missing
Interoperability framework or layer	Enable cross agency data exchange and once only reuse	Legal basis for sharing, registry stewardship, semantic alignment, security operations	"API without reuse," exchange exists but services still request documents
Service standard and assessment routine	Improve end to end service quality and usability	Enforceable authority, service ownership, cross agency dispute resolution	Standard becomes guidance only, uneven compliance, fragmented experiences
Digital identity and trust services	Enable secure authentication, consent, and lawful transactions	Privacy governance, liability rules, incident response, inclusion mechanisms	Exclusion of vulnerable users, trust erosion after incidents
Reference architecture and shared building blocks	Reduce duplication and enforce reuse	Procurement rules, architectural governance, lifecycle funding	Fragmented systems, rising integration costs, vendor lock in
Delivery playbooks and agile routines	Improve implementation discipline and learning cycles	Product teams, skills, procurement flexibility, performance measurement	Pilots succeed but cannot scale, reform fatigue
Data governance templates	Improve data quality and accountability	Data ownership, metadata standards, auditability, incentives	Inconsistent registries, low trust in data, policy disputes persist

Sources: (OECD, 2014; OECD, 2020; Peck, J., & Theodore, N., 2010)

In digital governance, transfer success depends less on the imported artefact and more on whether legal, organizational, data, and security dependencies are institutionalized.

Transfer channels should be analyzed not only as communication pathways but as incentive structures. Benchmarking and reputational

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

competition can create incentives for rapid launches and "countable outputs," such as the number of services digitized, which may crowd out deeper back office reform. Donor programmes can reduce fiscal constraints and provide expertise, but they may also introduce compliance logics and parallel delivery units that are difficult to integrate into permanent administrative systems. Vendor diffusion translates private product roadmaps into public governance choices, especially when procurement is treated as a technical transaction rather than as a policy instrument. The policy transfer lens is therefore valuable because it makes visible how power, incentives, and accountability are reshaped through the seemingly neutral adoption of frameworks and platforms (Dolowitz & Marsh, 2000). In other words, transfer is not merely about copying ideas. It is about institutionalizing new rules and routines in a way that survives political turnover, changes in leadership, and shocks to infrastructure.

The table 1.16 systematizes the main channels of transfer and the characteristic governance problems that accompany each channel.

Table 1.16. Transfer channels, incentive patterns, and governance risks in digital reforms

Transfer channel	What it typically prioritizes	Incentive effect	Main governance risk	Practical countermeasure
Peer learning and communities of practice	Methods, lessons, implementation know how	Encourages incremental capability building	Selective learning, overgeneralization	Require evidence dossiers and fit assessment
Benchmarking and rankings	Visible outputs and maturity claims	Rewards speed and symbolic compliance	Portal first reform, weak back office change	Add outcome and equity metrics to dashboards
Donor and programme assistance	Templates, funding, project delivery	Accelerates adoption under conditions	Parallel systems, low ownership	Co-design, integration into budgets and HR
Vendor and consultancy diffusion	Packaged platforms and standard solutions	Lowers design effort and timeline	Lock in, fragmentation, weak auditability	Interoperability clauses, portability, audits
Regional integration frameworks	Harmonization and cross border alignment	Aligns standards and legal expectations	Overstandardization without capacity	Sequenced adoption linked to capability growth

Sources: (Dolowitz, D. P. & Marsh, D., 2000); Peck, J. & Theodore, N., 2010; OECD, 2014)

Transfer channels shape what gets implemented first, and therefore they must be managed as governance environments rather than treated as neutral information flows.

A deeper interpretation of policy transfer requires distinguishing degrees of transfer. In digital governance, inspiration is common, where countries borrow principles such as user centricity or once only without replicating institutional form. Emulation involves adopting a similar institutional arrangement, such as a central delivery unit or a service standard, but tailoring enforcement mechanisms. Hybridization is typical in practice, combining components from multiple sources into a new configuration, which increases design flexibility but also increases coherence risks if dependencies are not mapped. Direct copying is rare and often fragile, because it presumes that legal, administrative, and data environments are sufficiently similar. Degree matters because it determines the level of governance work required. The more ambitious the degree, the more explicit the dependency management, authority design, and monitoring must be.

The Table 1.17 defines degrees of transfer and specifies what must be in place for each degree to be viable.

Table 1.17. Degrees of policy transfer in digital governance and required governance capacity

Degree of transfer	What is adopted	Typical benefit	Viability condition	Typical failure pattern
Inspiration	Principles and narratives	Low risk learning, agenda setting	Clear problem definition and outcome metrics	Slogans without implementation instruments
Emulation	Similar instruments and routines	Faster design and standardization	Enforceable authority and incentives	Guidance without compliance, uneven results
Hybridization	Components from multiple models	Flexibility, local fit	Strong architecture governance and integration capability	Fragmentation, incompatible components
Direct copying	Institutional form plus tools	Shortest design time	High similarity of legal and administrative conditions	Misfit, legitimacy problems, fragile operations

Sources: (Dolowitz, D. P. & Marsh, D., 2000; OECD, 2020)

Higher degrees of transfer increase the burden of governance design, and weak authority is the most common constraint on ambitious transfer.

Policy transfer also has a predictable risk structure that can be managed through design. Common risks include artefact transfer without mechanism transfer, fragmented procurement, parallel systems created by programme logic, and performance measurement that rewards outputs rather than outcomes. In addition, as governments scale automation and data reuse, new risks emerge around accountability for automated decisions, auditability, and the distribution of errors across social groups. These risks are not reasons to avoid transfer. They are reasons to treat transfer as a governed lifecycle with explicit controls. Controls include reference architectures with enforceable procurement clauses, service ownership arrangements with escalation rights, legal interoperability instruments, data stewardship and quality assurance, and monitoring systems that track completion, burden reduction, equity, trust, and resilience.

The Table 1.18 links common transfer risks to governance controls that can be embedded in reform design from the beginning.

Table 1.18. Risk control matrix for policy transfer in digital governance

Risk pattern	Observable symptom	Structural cause	Governance control
Artefact without mechanism	Portal grows, burden does not fall	Back office unchanged, weak data reuse	End to end redesign and reuse enforcement
Standards without authority	Service quality varies across agencies	No enforcement, weak incentives	Mandates, audits, escalation rights
Fragmented procurement	Incompatible systems multiply	Contracts ignore interoperability and reuse	Reference architecture, interoperability clauses
Parallel platforms	Multiple overlapping solutions	Programme logic not integrated into state systems	Integration plan, unified governance
Fast policy failure	Incidents or instability after scaling	Safeguards and capacity lag behind rollout	Staged scaling, security baselines, continuity tests
Output inflation	Success claimed via counts	KPIs not tied to public value	Outcome and equity indicators, independent review

Sources: (OECD, 2014; Peck, J., & Theodore, N., 2010; Pritchett, L., Woolcock, M., & Andrews, M., 2013)

Transfer becomes safer when risks are anticipated as structural patterns and when controls are institutionalized as routine requirements, not as post hoc corrections.

Policy transfer in digital governance is best understood as a staged institutional translation process rather than a simple adoption of foreign technologies. The transferable content of digital reforms is typically modular, yet each module depends on hidden legal, organizational, data, and security prerequisites that must be built or substituted in the receiving context. Transfer channels are consequential because they shape incentives, frequently privileging visible outputs over governance capacity and back office change. Degrees of transfer range from inspiration to direct copying, and higher degrees increase dependency and authority requirements. The evidence across frameworks implies that transfer succeeds when mechanisms are preserved, authority is enforceable, procurement is governed by interoperability and lifecycle rules, and safeguards co-develop with scaling. A governance centered approach therefore treats policy transfer as an instrument for building state capability, measured through outcomes, equity, trust, and resilience, rather than through digitization counts alone.

3. Adaptation to national context. Adaptation is the decisive stage in cross national digital governance learning because it translates a transferred practice into an operable institutional arrangement under a specific legal order, administrative structure, and capability profile. In this study, adaptation is defined as deliberate redesign that preserves the causal mechanism of an imported practice while reshaping its institutional form to fit domestic constraints and normative commitments. The practical implication is that adaptation is not a "soft" activity of contextual wording; it is a hard design task that reallocates authority, formalizes accountability for outcomes, and changes the rules of data production, sharing, and use. Digital reforms typically fail at this stage when the receiving system imports surface elements, such as an interface, a platform label, or a template, while leaving intact the institutional conditions that caused the original problem, such as fragmented mandates, registry inconsistency, or procurement incentives that reward duplication (OECD, 2014; OECD, 2020). A second failure pathway occurs when scaling precedes safeguards and capacity building, creating fragile systems that can rapidly lose legitimacy after incidents, service instability, or exclusion of low capacity users (United Nations Department of Economic and Social Affairs, 2024).

A useful way to structure adaptation is to treat any imported practice as a bundle of interdependent components: a legal component, an institutional governance component, a data and interoperability component, an operational delivery component, and a safeguards component. Each component must be explicitly re specified for the receiving context, because the "same" practice behaves differently when administrative law defines discretion differently, when institutional coordination is stronger or weaker, or when registries differ in quality and semantic coherence. This is why capability diagnostics are central. The receiving system must identify which prerequisites are already present, which are missing, and which can be substituted through staged design. GovTech maturity logic supports this stance by emphasizing that enabling conditions and core system maturity constrain what can be implemented credibly at each stage (World Bank, 2022). If a country lacks stable registry governance, it can still adopt a once only principle rhetorically, but it cannot operationalize it reliably without first investing in stewardship, metadata, and quality controls.

A deeper adaptation design starts with identifying the intended reform mechanism and then choosing the minimum viable institutional package required to activate it. For example, if the target mechanism is administrative burden reduction through lawful data reuse, the critical adaptation tasks are establishing legal permissions and liabilities for reuse, clarifying registry ownership, and institutionalizing auditability and access logging. If the target mechanism is service quality improvement through service standards, the critical tasks are end to end service ownership, escalation rights, compliance assessment routines, and procurement alignment so that service teams can redesign workflows, not only digitize existing forms. If the target mechanism is trust infrastructure, the critical tasks are privacy governance, cybersecurity operations, incident response readiness, and inclusion measures such as assisted digital channels. In all cases, the adaptation task is to ensure that the receiving context has an enforceable chain of responsibility for outcomes and harms, including errors introduced by automation.

The Table 1.19 decomposes adaptation into design domains and specifies concrete outputs that convert an imported practice into an enforceable national arrangement.

Table 1.19. Adaptation domains, design decisions, and minimum viable outputs

Adaptation domain	Core design decision	Minimum viable outputs in the receiving context	Common failure pattern
Legal interoperability	Define lawful bases for exchange, reuse, and accountability	Clear permissions, purpose limits, liability allocation, auditability rules	Informal exchange substitutes for lawful design
Institutional authority	Determine who can set and enforce cross agency rules	Mandate, escalation rights, compliance monitoring function	Coordination without enforcement power
Service ownership	Assign end to end responsibility for outcomes	Named service owner, cross agency workflow authority	Diffuse responsibility, unresolved bottlenecks
Data and registry governance	Make data reuse reliable and interpretable	Data owner roles, quality controls, metadata, semantic standards	APIs exist, but data is inconsistent and unusable
Architecture and reuse	Enforce reuse of shared components	Reference architecture, approved building blocks, integration standards	Fragmented systems, costly integration
Procurement and lifecycle funding	Align incentives with interoperability and maintenance	Interoperability clauses, portability requirements, O and M funding model	One off projects, vendor lock in
Safeguards and resilience	Institutionalize rights protection and continuity	Privacy governance, security baselines, incident routines, continuity tests	Safeguards postponed until after scaling
Inclusion and assisted access	Ensure low capacity users can complete services	Accessibility compliance, assisted channels, outreach and support	Digital divide widens, legitimacy declines

Sources: (OECD, 2014; OECD, 2020; United Nations Department of Economic and Social Affairs, 2024; World Bank, 2022)

Adaptation becomes implementable when each domain yields enforceable outputs, rather than remaining at the level of principles or strategy statements.

https://doi.org/10.36690/PUBADM

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

Adaptation also requires sequencing because institutional prerequisites cannot be built simultaneously at full scale. A strong sequencing principle is mechanism first, scale second. Mechanism first means building the smallest set of legal, data, and governance conditions that allow an imported practice to function predictably, with measurable outcomes and controllable risk. Scale second means expanding coverage only after monitoring demonstrates stable performance and after safeguards are verified under real operating conditions. This principle directly counters isomorphic mimicry, where systems adopt formal structures that resemble high performing states but do not build implementation capability and therefore produce persistent failure (Pritchett, Woolcock, & Andrews, 2013). In digital governance, isomorphic mimicry often appears as portal first approaches, where demand is scaled through a unified interface while the back office remains fragmented, or as standards without enforcement authority, where compliance depends on voluntary cooperation.

The Table 1.20 provides sequencing pathways that align adaptation decisions with the dominant reform objective and its risk profile.

Table 1.20. Sequencing pathways for adaptation, aligned with reform objectives

Dominant objective	Mechanism to activate	First sequence priorities	Second sequence priorities	Typical risk if reversed
Burden reduction	Lawful data reuse and automation	Legal basis, registry stewardship, auditability, interoperability governance	Service redesign, reuse of building blocks, expansion to new domains	Portal scales demand while burden remains
Service quality and completion	End to end ownership plus standards	Service ownership, assessment routine, workflow authority, measurement	Shared components, procurement alignment, broader rollout	Standards become guidance with uneven compliance
Trust and legitimacy	Safeguards plus inclusion	Privacy governance, cybersecurity operations, incident response, assisted channels	Gradual automation, data reuse expansion, wider integration	Incident or exclusion collapses adoption
Fiscal efficiency	Reuse and lifecycle governance	Reference architecture, procurement clauses, shared platforms, O and M funding	Process redesign, workforce capability, consolidation	Short term savings create long term lock in costs
Cross border alignment	Harmonized rules and interoperability	Legal alignment, semantics, cross agency agreements, trust services	Service integration, scaling, continuous monitoring	Harmonization without capacity yields paper compliance

Sources: (OECD, 2014; OECD, 2020; Pritchett, Woolcock, & Andrews, 2013; United Nations Department of Economic and Social Affairs, 2024)

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

Sequencing should be chosen by the target mechanism and the main risk exposure, not by what is most visible or easiest to launch.

A further requirement for deep adaptation is capability realism. Digital governance reforms rely on delivery capacity, product management routines, and operational security functions that behave differently from traditional project management. The receiving context therefore needs a capability map that distinguishes project delivery from service operations, and technical capacity from institutional authority. Without this distinction, reforms often fund build phases while underfunding run phases, producing fragile services that degrade after launch. Capability realism also includes human resource constraints, because many administrations cannot quickly hire or retain specialized talent, which means that adaptation should include institutional mechanisms for capability building, such as shared service teams, training pipelines, and procurement models that prevent the externalization of core state functions.

The table 1.21 proposes a capability maturity matrix used to decide whether an imported practice should be scaled, piloted, or redesigned.

Table 1.21. Capability maturity matrix for adaptation feasibility

Capability area	Low maturity signal	Minimum viable maturity for scaling	Practical adaptation response
Cross agency authority	Coordination bodies lack enforcement rights	Mandate with escalation and compliance monitoring	Start with narrower scope and formalize authority
Registry governance	No clear data owners, weak quality controls	Stewardship roles, metadata, quality monitoring	Prioritize registry modernization before automation
Service delivery routines	Project mode dominates, weak product ownership	Product teams, service owner, lifecycle KPIs	Pilot with stable teams and explicit ownership
Procurement discipline	Contracts ignore interoperability and reuse	Interoperability clauses and portability requirements	Use reference architecture and reusable components catalogue
Security operations	Reactive incident handling	Baselines, monitoring, incident response drills	Stage scaling, require security readiness gates
Inclusion capability	Accessibility not institutionalized	Accessibility governance and assisted channels	Build assisted channels and support before digital only shifts

Sources: (OECD, 2020; World Bank, 2022; United Nations Department of Economic and Social Affairs, 2024)

Capability maturity defines the ceiling of credible transfer; adaptation reduces risk by aligning ambition with maturity and by sequencing capability building.

Adaptation must also address procurement as a policy instrument, because procurement decisions lock in architectures, data models, and vendor dependencies for years. Treating procurement as a technical step rather than a governance lever is a common cause of fragmentation. Adaptation should therefore translate interoperability and reuse principles into enforceable contractual clauses, such as requirements for open interfaces, data portability, audit access, and lifecycle responsibilities. It should also define architectural governance so that agencies cannot procure incompatible solutions that undermine whole of government outcomes. Importantly, procurement governance must be paired with funding models that sustain operations, because shared building blocks create value only when they are maintained, secured, and improved continuously.

The table 1.22 identifies procurement clauses and governance controls that operationalize adaptation goals, especially interoperability, portability, and lifecycle accountability.

Table 1.22. Procurement clauses and governance controls for adapted digital reforms

Governance objective	Contractual requirement	Oversight control	Failure prevented
Interoperability	Standard APIs, agreed data schemas, secure exchange protocols	Architecture review and compliance testing	Incompatible systems and manual integration
Portability and exit	Data export, escrow or handover provisions, documentation duties	Vendor exit plan and periodic portability checks	Vendor lock in and loss of institutional memory
Auditability	Access logs, audit trails, independent testing rights	Regular audits and incident review board	Unaccountable data use and weak incident learning
Lifecycle accountability	Clear O and M responsibilities, patching and update obligations	Service level monitoring and penalties	Degradation after launch, security debt
Reuse of building blocks	Mandatory use of approved components where applicable	Reuse catalogue and exemption process	Duplication and fragmentation across agencies

Sources: (OECD, 2014; OECD, 2020; World Bank, 2022)

Adaptation is stabilized when procurement translates principles into enforceable requirements and when oversight makes compliance routine.

Inclusion is another adaptation domain that is often underestimated because many international models implicitly assume high digital literacy and stable connectivity. In practice, national contexts differ in infrastructure, skills distribution, disability prevalence, language diversity, and trust in institutions. Adaptation should therefore institutionalize accessibility governance and assisted digital channels as core parts of service design, not as exceptional accommodations. Assisted channels should be designed as integrated complements to digital services, ensuring that non digital access does not become a slower, lower quality pathway that reproduces inequality. Inclusion design also requires measurement choices that respect ethics and privacy, using appropriate proxies and voluntary data where possible, while still enabling distributional monitoring.

The table 1.23 outlines an inclusion oriented service access model that can be adapted to differing national contexts while maintaining consistent accountability for outcomes.

Table 1.23. Inclusion oriented access model for adapted digital public services

Access pathway	Target users	Institutional requirement	Key performance indicator
Self service digital	Digitally capable users	Usable design, plain language, accessibility compliance	Completion rate and drop off by step
Assisted digital	Users with partial capacity	Support staff, guidance scripts, integrated identity support	Assisted completion rate and time to completion
In person support	Users with low capacity or special needs	Service points, trusted intermediaries, safeguards	Equity of access and satisfaction distribution
Alternative formats	Users with disabilities or language barriers	Accessibility governance, translation policy, standards	Accessibility conformance and complaint rate

Sources: (United Nations Department of Economic and Social Affairs, 2024; OECD, 2020)

Inclusion becomes an operational attribute of adaptation when assisted channels are designed, funded, and measured as part of the same service system.

Finally, adaptation requires a risk governance layer because imported practices can change the state's risk exposure by expanding data reuse, automation, and reliance on common infrastructures. A national context may have different threat levels, different legal expectations of transparency, or different administrative review procedures. Adaptation should therefore include a risk register that identifies risk owners, triggers, and mitigation controls. This approach shifts safeguards from being reactive responses to being design constraints that shape what is scaled and when.

The table 1.24 provides a risk register template tailored to adaptation of imported digital governance practices.

Table 1.24. Risk register for adapting imported digital governance practices

Risk category	Typical trigger	Impact pathway	Mitigation control	Named owner
Legal noncompliance	Ambiguous basis for reuse or automation	Litigation, loss of legitimacy, reversals	Legal review gates, auditability, liability clarity	Legal and compliance lead
Data quality failure	Registry inconsistency or missing fields	Wrong decisions, rework, appeals	Stewardship, quality metrics, semantic standards	Registry owner
Security incident	Weak monitoring or patching	Trust collapse, service outages	Security baselines, incident drills, continuity testing	Security governance
Exclusion and inequality	Low accessibility or weak assisted channels	Reduced uptake, legitimacy loss	Accessibility governance, assisted channels, outreach	Service owner
Fragmentation and lock in	Procurement without interoperability clauses	Rising integration cost, dependence	Reference architecture, portability and exit clauses	Architecture and procurement lead
Output inflation	Metrics reward counts	Misallocation of funding, weak outcomes	Outcome and equity KPIs, independent review	Central coordinating authority

Sources: (OECD, 2014; OECD, 2020; United Nations Department of Economic and Social Affairs, 2024)

Risk governance makes adaptation sustainable by linking triggers to controls and assigning ownership for mitigation and learning.

Adaptation to national context determines whether international practices become functional capacity or symbolic imitation. Deep adaptation requires decomposing imported practices into legal, institutional, data, operational, procurement, safeguards, and inclusion components, then re specifying each component as enforceable outputs. Sequencing is essential because mechanisms must be activated before scaling, especially where lawful data reuse, registry governance, and enforcement authority are prerequisites for public value outcomes. Capability realism prevents reforms from exceeding the maturity of cross agency coordination, security operations, and service delivery routines, thereby reducing the probability of isomorphic mimicry and implementation fatigue. Procurement must be treated as a governance lever that locks in interoperability, portability, auditability, and lifecycle accountability. Inclusion and assisted digital channels must be institutionalized as core service attributes so that digitalization does not widen inequality and undermine legitimacy. Finally, risk governance provides the control structure that aligns scaling with safeguards and learning, ensuring that adaptation strengthens trust and resilience alongside efficiency.

Conclusion. International practices of digital governance become practically useful when they are handled as lessons, transferred through accountable mechanisms, and adapted through capability realistic design. Lessons are most robust when expressed as outcome plus mechanism plus enabling conditions, with evidence and indicators that prevent cosmetic imitation. Policy transfer is most effective when it moves beyond artefacts and labels and instead transfers governance routines, enforcement authority, and lifecycle capabilities. Adaptation is the decisive step because institutional fit determines whether imported mechanisms can operate lawfully, reliably, and inclusively at scale. The analysis also implies a consistent evaluation stance: digital transformation should be judged by outcomes such as completion, burden reduction, equity, trust, and resilience, rather than by counts of digitized services. Finally, the study supports a governance centered approach in which interoperability, data stewardship, procurement discipline, and safeguards are treated as core institutional capacities that must co develop with service expansion.

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

Conflict of interest. The author 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 author 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 author 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. OECD. (2014). *Recommendation of the Council on Digital Government Strategies* (OECD/LEGAL/0406).
2. OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*.
3. Rose, R. (1991). What is lesson-drawing? *Journal of Public Policy, 11*(1), 3–30.
4. 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).*
5. Dolowitz, D. P., & Marsh, D. (2000). Learning from abroad: The role of policy transfer in contemporary policy-making. *Governance, 13*(1), 5–24.
6. OECD. (2014). *Recommendation of the Council on Digital Government Strategies* (OECD/LEGAL/0406).

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

7. OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*.
8. Peck, J., & Theodore, N. (2010). Mobilizing policy: Models, methods, and mutations. *Geoforum, 41*(2), 169–174.
9. Pritchett, L., Woolcock, M., & Andrews, M. (2013). Looking like a state: Techniques of persistent failure in state capability for implementation. *Journal of Development Studies, 49*(1), 1–18.
10. OECD. (2014). *Recommendation of the Council on Digital Government Strategies* (OECD/LEGAL/0406).
11. OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*.
12. Pritchett, L., Woolcock, M., & Andrews, M. (2013). Looking like a state: Techniques of persistent failure in state capability for implementation. *Journal of Development Studies, 49*(1), 1–18.
13. 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).*
14. World Bank. (2022). *GovTech maturity index: 2022 update.*
15. Zagorsky, V., Rahimov, F., Horbova, N., Zhuk, O., Pershko, L., & Mihus, I. (2023). Socio-economic aspect of territorial organization of power. *Economic Affairs, 68*(3), 1555–1564. https://doi.org/10.46852/0424-2513.3.2023.22

Section 1.3. Digital Era of Public Administration: Using Artificial Intelligence to Improve the Efficiency of Public Services

Volodymyr Panchenko[1], **Oksana Panchenko**[2]

[1]*Doctor of Science (Economics), Doctor of Science (Public Administration), Professor, Professor of the Department of Aviation Management, Ukrainian State Flight Academy, Kropyvnytskyi, Ukraine, ORCID: https://orcid.org/0000-0003-0958-7752*

[2]*Ph.D. in Economics, Associate Professor, Associate Professor of the Department of Management and Entrepreneurship, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, Ukraine, ORCID: https://orcid.org/0000-0002-6608-4783*

Citation:
Panchenko, V. & Panchenko, O. (2025). Digital Era of Public Administration: Using Artificial Intelligence to Improve the Efficiency of Public Services. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 53–77). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-53-77

***Abstract**. This study analyses how artificial intelligence reshapes public administration by transforming the design, delivery, and oversight of public services. The emphasises that AI is not only a technological innovation but also an institutional and organisational change that influences trust in government, access to services, and the legitimacy of administrative decisions. The objective is to conceptualise the digital era of public administration through the lens of AI use in core areas such as social protection, taxation, citizen data management, and anticorruption policy, while identifying conditions under which AI enhances rather than undermines public value. Methodologically, the study relies on comparative analysis of international practices, combining a review of academic literature, examination of policy documents and strategies, and case studies from countries that actively implement AI in government, including Ukraine, EU member states, the United States, and Estonia. This approach makes it possible to contrast different governance models and to trace how technological, legal, and ethical factors interact in real administrative contexts. The main results demonstrate that AI can significantly increase the efficiency and targeting of public services, automate routine processes, and support predictive analytics for more proactive policy design, yet at the same time generates new risks of bias, opacity, data insecurity, and digital exclusion. Special attention is given to the role of the state as designer of regulatory frameworks, builder of digital infrastructure, and guarantor of citizens' rights in algorithmic decision making. The conclusions argue that AI in public administration should be treated as part of a broader digital ecosystem that integrates legal safeguards, organisational capacity, and citizen centric design. Directions for further research include the development of quantitative indicators of AI effectiveness in the public sector, deeper analysis of ethical and human rights implications of algorithmic governance, and evaluation of long term institutional effects of AI on accountability, transparency, and democratic participation.*

***Keywords:** artificial intelligence; public administration; digital transformation; public services; algorithmic governance; automation; social protection; tax administration; data security; ethics; transparency; Ukraine*

ISBN 978-9916-9389-0-4 (pdf)
© Scientific Center of Innovative Research, 2025

1. Conceptualisation of Artificial Intelligence in Public Administration. In the era of digital transformations, states face the need to modernise their administrative systems. One of the most powerful instruments for optimising such systems is artificial intelligence (AI) technologies. AI has the potential to change approaches to management in the public sector, making public services more accessible, efficient and transparent.

The digitalisation of public administration makes it possible to reduce bureaucratic barriers, accelerate decision-making processes and facilitate citizens' access to essential services. Taking into account global trends, it is important to examine how the introduction of AI can change the face of the public sector and improve the quality and accessibility of services for citizens.

Interest in the potential of artificial intelligence in philosophical research has remained stable throughout the entire history of its development. Scholars continue to actively discuss the problem of AI systems today, covering political, economic and legal doctrines, social and cognitive sciences, automated control systems, neurocybernetics and other disciplines. Among the scholars who have considered artificial intelligence as an important science and a tool for transforming various aspects of civilisation, including education and scientific inquiry, it is possible to single out A. Turing, who noted the absence of emotional perception in machines and proposed the first test of intelligence for an AI system (Turing, 1950). A. Newell, H. Simon and C. Shaw developed the first artificial intelligence program, the Logic Theorist (Newell et al., 1959). J. McCarthy, a professor who at the Dartmouth College conference presented his own concept of AI and symbolically launched a new scientific field, also created the LISP programming language in 1963 (McCarthy et al., 2006). Three years later, J. Weizenbaum developed the first chatbot, ELIZA, which imitated a dialogue with a psychotherapist (Weizenbaum, 1966). J. Hinton in 2006 together with colleagues proposed new approaches to constructing deep neural networks and resolving the vanishing gradient problem during training (Hinton et al., 2006). F. Fukuyama in his research stressed that AI is an important component of the information society (Fukuyama, 2014). A. Pohorelenko drew attention to the development of AI in the sphere of international relations, as well as other domestic and foreign scholars who actively study different aspects of artificial intelligence development (Pohorelenko, 2018).

2. Core Technologies of Artificial Intelligence and Deep Learning Applications. Artificial intelligence is a branch of computer science that deals with the development and implementation of algorithms and systems capable of performing tasks that usually require human intellectual activity, in particular perception, analysis, learning and decision-making. Artificial intelligence (AI) is a method of making a computer or software "think" like the human brain. This is achieved by studying the patterns of the human brain and analysing cognitive processes. The result of this research is the development of intelligent software and systems (GigaCloud, 2025).

AI technologies are rapidly gaining popularity, and the market based on deep learning is showing significant growth. In 2022 its global value amounted to 12.67 billion USD. It is forecast that the market will grow from 17.60 billion USD in 2023 to 188.58 billion USD by 2030, which indicates impressive growth rates of 40.3 percent per year over the entire forecast period (Stfalcon, 2025).

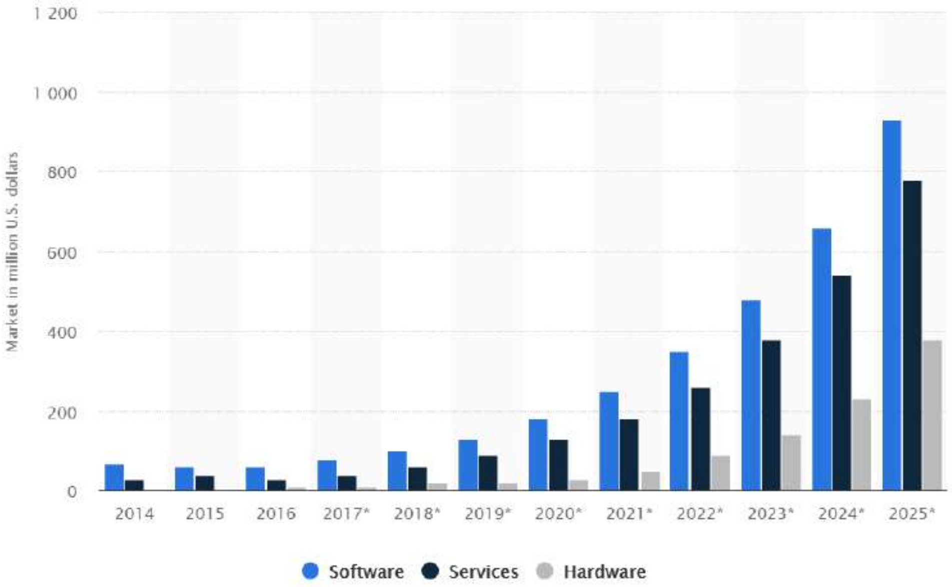

Figure 1.1. The value of AI applications in the world

Source: developed by the authors

AI covers a wide range of technologies, including machine learning (ML), deep learning (DL), natural language processing (NLP), as well as computer vision and decision-making algorithms.

The main purpose of using AI in public administration is to automate routine processes, increase the accuracy of decision-making and ensure more efficient use of public resources. It is important that AI not only increases the efficiency of public authorities but also contributes to improving the quality of public service delivery for citizens.

3. Machine Learning, Decision-Making Algorithms and Public Service Delivery. Machine learning (ML) is a subfield of AI that focuses on creating algorithms capable of learning from data without the need for explicit programming. Machine learning includes several types of approaches:

- supervised learning;
- unsupervised learning;
- reinforcement learning (GigaCloud, 2025).

Supervised learning occurs when algorithms receive training data in which each sample has a label or correct answer. The algorithm learns to find relationships between input data and corresponding outputs.

In unsupervised learning, the algorithm works with unstructured or unlabelled data. This approach helps to find hidden patterns or classifications in the data. For example, it can be applied in the analysis of public requests or for detecting anomalies in the processing of financial transactions. Reinforcement learning means that the algorithm interacts with an environment and receives a reward for performing correct actions, which allows it to adapt its strategies based on experience. This type of learning is used to optimise administrative processes in real time (GigaCloud, 2025).

Deep learning is a more complex form of machine learning that uses artificial neural networks to process large volumes of data. This method enables the performance of complex tasks such as image recognition, natural language processing and automated decision-making.

Deep learning plays an important role in the development of many AI applications and services, significantly enhancing the intellectual capabilities and automation of existing AI-based products. This direction is a component of machine learning that allows computers to perform both analytical and physical tasks without human intervention. In essence, deep learning is an advanced aspect of machine learning that provides computers with the ability to imitate human reactions and make data-based decisions. It is an important technology for such innovations as autonomous vehicles, voice assistants and speech recognition on various devices, from smartphones to smartwatches and televisions. Deep learning is the main driving force behind these revolutionary technological achievements (Stfalcon, 2025).

In the process of deep learning, computers are trained on large volumes of input data such as images, text or sound, gradually achieving a high level of accuracy, often surpassing human capabilities in various tasks. Deep learning models use neural networks with many layers that imitate the structure of the human brain and require powerful computational resources to work effectively with large data sets.

AI applications have great potential to increase the efficiency and effectiveness of administrative service delivery, as well as to support government decision-making by modelling different policy options in the performance of public administration functions (Veale & Brass, 2019). Researchers note that AI technologies can improve policy design by providing civil servants with additional data-based information, automating routine tasks and processes, improving the quality of information that citizens receive, making services more personalised and allowing for a deeper understanding of citizens' attitudes and needs, for example through the analysis of social media data (Zuiderwijk et al., 2021; Gaozhao et al., 2023).

In public administration, deep learning can be used for:

- analysis of images and video, for example to monitor public spaces in order to ensure security;
- natural language processing, for example through the use of chatbots or voice assistants to automate citizen interaction with public authorities.

A management decision is an instrument of influence on the object of management and its individual subsystems, an important link in the formation and implementation of management relations within the structure (Vahanova et al., 2022, pp. 94–98).

Decision-making algorithms are an important tool for optimising processes in public administration, particularly in setting priorities for the provision of public services. They make it possible to allocate limited resources efficiently and contribute to more accurate forecasting of future needs, which is especially important under conditions of a constrained budget. These algorithms can be applied in areas such as health services and social support, as well as in forecasting demand for various services.

Decision-making algorithms can be used to optimise the allocation of medical resources such as doctors, equipment and medicines. In the case of limited budgetary funds, it is important to determine which services and resources should receive priority. For example, an algorithm can take into account factors such as the urgency of treatment, the individual needs of patients and the effectiveness of resource use. In the event of epidemics or large-scale disasters, algorithms can help quickly identify which regions or hospitals need medical resources the most, giving priority to those with the greatest need. Algorithms can analyse patient data, including medical history, disease severity and other indicators, in order to determine which patients require immediate assistance or more complex treatment. They can also optimise the use of hospital beds, medicines and equipment so as to avoid both excessive and insufficient use, which makes it possible to ensure more even access to treatment.

In Ukraine the sphere of social services has acquired particular importance, since during the full-scale war challenges for the social sector have increased significantly. During 2022–2023 Ukraine's position in the global Social Progress Index deteriorated markedly: in 2021 Ukraine ranked 48th out of 168 countries, in 2022 it ranked 52nd out of 169, and in 2023 it ranked 59th out of 170 countries. Therefore, the social sphere requires change, improvement of approaches and better accessibility of social services for all social groups. At the same time, challenges in the social sphere are only increasing, as the full-scale invasion has exacerbated existing problems and revealed all the systemic shortcomings that had accumulated over the years (International Renaissance Foundation, 2025).

Therefore, AI in the sphere of social support, in particular decision-making algorithms, can also be extremely useful for managing the provision of financial assistance, housing subsidies, support for the unemployed and other social services.

They can analyse various data, such as income, family status and health status, to identify the most vulnerable categories of the population who need financial assistance or other social support. Algorithms can help optimise assistance procedures by determining who is entitled to social benefits, what amount of support is necessary and in what order these amounts should be paid (International Renaissance Foundation, 2025). They make it possible to predict increases or decreases in demand for social services based on demographic changes or economic conditions, which helps to plan the social support budget more effectively.

Algorithms can also be used to forecast infrastructure development needs. For example, in the transport sector they can predict where the highest demand for transport services will arise, allowing optimisation of routes and timetables. Under conditions of a limited budget this enables public authorities to use available resources more efficiently.

Overall, decision-making algorithms provide public authorities with powerful tools for effective management of limited resources, forecasting citizens' needs and optimising the provision of public services. They allow not only to improve the accuracy of decisions but also to ensure more even and fair access to essential services for citizens.

4. Artificial Intelligence in Ukrainian Public Institutions: Opportunities and Constraints. The use of artificial intelligence in public institutions in Ukraine is gaining popularity in the context of the digital transformation of public administration, especially with the use of Diia. The introduction of AI in the public sector has great potential to increase administrative efficiency, improve the quality of services provided to citizens and reduce bureaucratic barriers. However, in Ukraine this process is only beginning and has certain specific features determined by technological, social and economic factors.

One of the main aspects of AI use in Ukraine is its introduction in public authorities to automate decision-making processes and the performance of routine tasks (Table 1.25).

Table 1.25. AI in public administration of Ukraine

Areas of implementation	Description
Automation of administrative processes	This includes the use of AI for automatic processing of applications, documents, and requests from citizens and businesses. For example, automatic analysis of large amounts of data helps in the automatic collection of statistical reports or in the processing of large amounts of information within tax or customs authorities.
Improvement of public services	The use of AI allows for the automation of the work of registration, notary, and other government agencies. This helps speed up processes, reduce errors, and improve access to services.

Source: developed by the authors

AI has enormous potential for processing and analysing large datasets accumulated in public authorities.

The public sector seeks to maximise public value, rather than commercial value, when applying artificial intelligence technologies. This defines the difference in staff motivation, organisational goals and strategies, and creates specific barriers that limit the implementation of AI in public institutions. These barriers require careful analysis in order to understand why the process of AI adoption in the public sector is slower compared to the private sector (Zuiderwijk et al., 2021).

For Ukraine, it is important to develop analytical systems capable of supporting data driven decision making. Such applications include the analysis of economic and social indicators, as well as the monitoring and evaluation of public programs. The use of AI enables government institutions to make forecasts and assessments based on real data from various spheres such as the economy, health care, education and the environment. This helps in planning public programs and in providing targeted assistance to the most vulnerable categories of the population. With the help of AI it is possible to assess the effectiveness of different programs and initiatives, providing civil servants with objective data on their outcomes.

One of the greatest challenges for public institutions in Ukraine is corruption and a low level of transparency. The requirements for transparency and clarity in public administration are significantly stricter than in the private sector, both regarding the functioning of AI systems themselves and the transparency of public resource expenditure. This creates specific requirements for the implementation of AI in administrative services and the activities of public authorities that differ from those in private companies. Therefore, although some problems associated with the introduction of innovations, including AI technologies, may be similar in both sectors, the context of public administration is unique (Gaozhao et al., 2023).

AI can become a powerful tool in combating these problems through:

- analysis of financial transactions and reporting;
- detection of corruption schemes.

AI systems can automatically check financial reports and monitor public procurement, helping to identify anomalies, abuses or violations of legislation. AI can analyse large volumes of data on financial transactions, contracts and other documents to detect potential corruption schemes, which helps law enforcement agencies respond more quickly to crimes.

The main challenges faced by the judicial system during the war include instability in court operations, lack of access to combat zones, destruction of environmental infrastructure and limited data for judicial proceedings. However, even under these conditions, citizens can protect their rights by applying to pre trial instances in government controlled territories and by filing claims to international courts (Palamarchuk, 2024, p. 466).

In Ukraine AI is also beginning to be used to improve the functioning of the judicial system and to ensure justice. Algorithms are used to automate some stages of judicial proceedings, such as preliminary case analysis, case sorting or even forecasting decisions based on previous practice. AI can be applied to predict trends in the criminal sphere, for example to identify offences that may be committed under certain conditions or circumstances.

AI can also be used in infrastructure management, particularly in the energy sector. AI algorithms can help optimise the allocation of energy resources, forecast energy consumption and reduce energy supply costs. The use of AI makes it possible to manage transport systems, monitor traffic flows and efficiently manage water supply, waste management and other critical infrastructure components.

It should be noted that the use of AI in public institutions in Ukraine has certain difficulties and challenges (Table 1.26).

Table 1.26. Challenges of using AI in public institutions

Challenges	Description
Limited Digital Infrastructure	For the effective implementation of AI in Ukraine, it is necessary to significantly improve the digital infrastructure and ensure a high level of Internet access in all regions.
Data Protection and Security	Problems with the protection of personal data, as well as cybersecurity issues, remain relevant when implementing new technologies.
Ethical Issues	It is important to address ethical issues related to the use of AI, such as making decisions that can affect the lives of citizens without proper human participation.

Source: developed by the authors

The use of artificial intelligence in Ukraine is gradually expanding, and at present most such initiatives are implemented in leading organisations in the fields of industry, information and communication technologies, and financial technologies. At the same time, a significant share of AI technologies in Ukraine is based on foreign developments or is used within licensed solutions that do not belong to Ukrainian companies. In many cases, development is carried out on the territory of Ukraine, but the intellectual property rights belong to foreign companies, which limits the economic benefits for the national economy (Shevchenko & Baranovskyi, 2023, p. 66).

According to LinkedIn, as of 2023 Ukraine has more than 2,000 companies and institutions that specialise in software development in the field of AI, in particular in large cities such as Kyiv, Kharkiv, Lviv and Odesa. This figure continues to grow, which indicates significant potential for the development of the AI industry in Ukraine. In addition, according to the Clutch platform, Ukrainian IT companies occupy leading positions among AI developers in Eastern Europe (Shevchenko & Baranovskyi, 2023, p. 66).

For the further development of AI use in Ukraine it is necessary to:

- develop human resources capable of working with advanced technologies;
- implement state programs to support innovation in the IT sphere;
- improve legal regulation of AI use, in particular in the context of data protection and ethics.

The development of AI in public institutions in Ukraine is an important step towards digital transformation and increased efficiency of public administration.

In Ukraine the number of AI start ups is also growing rapidly. According to IT Ukraine, in 2022 Ukrainian AI start ups attracted more than 50 million US dollars of investment, which is almost twice as much as in the previous year. This indicates a growing interest of investors in Ukrainian developments and technologies in the field of AI. Among the most well known Ukrainian companies working with AI are start ups such as Grammarly, a tool for automatic text correction, Reface, a platform for face swapping in video, Ring Ukraine (SQUAD) and others. In addition, Ukraine is currently one of the leaders in AI development in the areas of image recognition, natural language processing and data forecasting (Shevchenko & Baranovskyi, 2023, p. 66).

One of the key advantages of implementing AI technologies in public administration is the significant automation of administrative processes. The use of AI allows public authorities not only to increase the efficiency of their internal processes, but also to focus efforts on more complex and strategic tasks. This concerns such areas as document registration, processing of citizens' requests, monitoring of services provided and analytics (Pohorelenko, 2018).

One of the main directions of AI use is the automation of registration processes. In many countries, including Ukraine, the registration of property rights, business registration, registration of citizens or vehicles is a complex and labour intensive process that requires significant resources and time.

AI can automate a number of such tasks, including:

- verification of documents in order to automatically check the accuracy of documents submitted for registration and detect possible forgeries or inaccuracies in the data;
- automatic distribution of applications in order to sort applications according to their priority or importance and to ensure rapid and accurate forwarding to the relevant authorities;
- collection and processing of documents, where through optical character recognition technologies and machine learning it is possible to automatically extract data from submitted documents and enter them into relevant databases for further processing.

The introduction of AI in the processing of citizens' requests makes it possible to significantly accelerate interaction between citizens and public institutions. On the basis of big data analysis and natural language processing algorithms, public authorities can automatically respond to citizens' requests, which significantly reduces response time and lowers the workload on staff (IBM, 2025).

For example, chatbots and virtual assistants. An AI system can automatically respond to frequently asked questions or help citizens receive advice on services provided by public institutions. Chatbots can operate around the clock, which ensures the availability of services at any time of day.

AI algorithms can classify the type of request and automatically direct it to the relevant department or service. They can also provide answers to standard requests through embedded knowledge bases (IBM, 2025).

Another important aspect is the monitoring and analysis of the quality of administrative services. AI can ensure effective data collection and analysis, which allows public authorities to quickly assess their performance and identify problems in a timely manner. AI can automatically collect citizens' feedback on the quality of services provided, analyse this feedback to detect problems and propose possible solutions. The use of algorithms for analysing and evaluating the effectiveness of administrative processes makes it possible to identify weaknesses in the management system and optimise workflows.

Despite all the advantages of automation through AI, there are certain challenges that public authorities may face when introducing these technologies. These include technical problems, data protection and staff training.

In Ukraine and other developing countries there may be an insufficient technical infrastructure for the effective implementation of complex AI systems. Since the processing of personal data is an important component of the automation of administrative processes, it is essential to ensure a high level of protection for such data. For the effective use of AI in the public sector, it is necessary to have staff with appropriate knowledge and skills to work with these technologies.

Artificial intelligence has considerable potential to improve the quality of public services, in particular through the personalisation of citizen service. Personalisation means adapting public services to the individual needs of each person, which allows not only to increase the efficiency of service delivery, but also to improve citizens' satisfaction with interaction with public authorities.

The use of machine learning algorithms can be applied to predict citizens' needs. AI can help identify which services may be most useful for pensioners, taking into account their specific characteristics.

Machine learning algorithms can analyse data about persons with disabilities and, on this basis, automatically propose or provide specialised services such as building accessibility, medical care or assistance in applying for benefits (GigaCloud, 2025).

In addition to pensioners and persons with disabilities, the personalisation of services can also extend to other social groups, each of which has its own specific needs and requirements for public services.

This may concern young people and students, as well as families with children. Through the analysis of citizens' behaviour on the internet, their applications and requests, AI can help public authorities offer young people accurate recommendations on opportunities for education, career and social support. For families with children, AI algorithms can predict their need for benefits for child services, health care, as well as for assistance in applying for housing subsidies and other social services.

The adaptation of social services is another important direction of personalisation. By analysing citizens' behaviour and needs, public authorities can create specialised programmes to support vulnerable categories of citizens such as the unemployed, low income households or large families (Ranerup & Henriksen, 2022).

AI can analyse citizens' socio economic status and propose benefits or assistance of the type that best corresponds to their needs. AI algorithms can identify the most vulnerable categories of citizens and direct them to a support programme that is most appropriate to their situation, for example support for the unemployed, assistance for the elderly or for persons with disabilities.

The personalisation of services requires the continuous collection and analysis of data about citizens. AI can help optimise this process through the integration of different databases and the automatic analysis of the data collected. Important tools include the analysis of data from social networks and other open sources. Using social media analytics and other open data, AI can assess current public moods and needs, which allows public authorities to respond promptly to requests and provide relevant services.

The continuous improvement of algorithms is essential, since they constantly update their models on the basis of new data, which allows public authorities to continually improve service quality and make services more personalised (McCarthy et al., 1955).

Most AI projects largely depend on internal and external cooperation between academic institutions, private companies and public agencies. The networks within which public administration operates and the way public bodies use the expertise of these networks are crucial for launching and successfully implementing many innovations. This requires organisations to be able to cooperate effectively with different stakeholders. However, such cooperation is complicated by several factors, including confidentiality and security in data exchange, a lack of common understanding regarding which data are required and available, the absence of harmonised policies between organisations and insufficient engagement from public authorities. In addition, data security issues threaten the sovereignty of the information space, creating risks for data protection and the possibility of external interference in sensitive information (Cordella & Hesse, 2015).

Since the personalisation of services requires the collection and processing of large volumes of personal data, it is necessary to guarantee their security and confidentiality. For the effective implementation of AI technologies, a developed technical infrastructure and access to large volumes of data are required, which may be a problem in countries with less developed digital infrastructure. It is also important to consider the ethical aspects of service personalisation, in order to avoid discrimination against certain population groups or misuse of personal information. However, under proper use AI can significantly improve the quality of public services, making them more personalised, efficient and accessible for every citizen (Zuiderwijk et al., 2021).

One of the main problems faced by public administration bodies is corruption, which significantly reduces the efficiency of the state and undermines citizens' trust in government. Artificial intelligence has significant potential to combat this problem through its ability to automate and make many administrative processes more transparent.

The automation of decision making processes with the help of AI makes it possible to exclude the human factor, which is a key source of corruption risks in many administrative processes. In traditional management systems people can make subjective decisions, which may lead to bias, abuse or even bribery. With the help of AI it is possible to establish clear decision making algorithms based on objective facts, data and predefined criteria (Veale & Brass, 2019).

For example, the automation of budget allocation processes can significantly reduce opportunities for corrupt actions, since an algorithm cannot be bribed or influenced by personal interests. Such a system operates on the basis of clearly defined rules and parameters, which reduces the probability of unlawful manipulation.

One of the most promising directions for using AI to combat corruption is the integration of blockchain technologies. Blockchain makes it possible to create immutable and transparent ledgers for processing financial transactions and public contracts. The use of AI to monitor and analyse blockchain data allows the rapid detection of anomalies that may indicate potential corruption schemes (Table 1.27).

Table 1.27. Capabilities of blockchain technologies

Capabilities	Description
Ensuring Transparency	All transactions and operations with financing can be recorded in the blockchain, which makes them available for verification at any time and by any participant in the system. Such transparency significantly reduces the possibilities for corruption, since all changes in the data will be recorded and cannot be changed without tracking.
Preventing Fraud	The use of immutable registers based on blockchain technology provides a high level of protection against falsification and manipulation of state documents and financial transactions.
Process Automation	Blockchain allows you to automate the secure exchange of data between various state bodies, as well as, if necessary, between state and private structures, which significantly increases the efficiency of interaction and prevents corrupt influences.

Source: developed by the authors

Artificial intelligence can be used to monitor various administrative processes and detect potentially corrupt schemes by analysing large volumes of data. For example, with the help of AI algorithms it is possible to examine transactions of public institutions, financial flows, contractual agreements and other administrative documents in order to identify anomalous or suspicious patterns (Stfalcon, 2025).

Machine learning algorithms can be trained on historical data to detect atypical situations that may indicate possible abuses, such as inflated prices, non-competitive tenders or unauthorised changes to contracts. Since AI can process huge amounts of data in real time, it is able to react quickly to violations, which makes it possible to prevent corrupt actions before they lead to serious consequences.

One of the most corruption-prone areas is public procurement. Through the use of AI it is possible to automate and improve tender procedures, which significantly reduces opportunities for manipulation. AI algorithms can be used to analyse tender proposals. This means that AI is able to automatically examine all submitted bids, identifying possible shortcomings, manipulations or improper practices, such as overpricing of goods or services (GigaCloud, 2025).

In addition to analysing tender proposals, AI can perform a forecasting function with respect to tender outcomes. By analysing historical data on winning bids and the distribution of contracts, AI can predict probable results and assist in detecting cases where tenders were conducted with violations.

AI can also help increase the transparency of interaction between public authorities and citizens. For example, by analysing citizens' complaints and requests submitted through different channels (electronic applications, social networks, surveys), AI can detect potential violations or reports addressed to public officials that may indicate corrupt schemes, bribery or other misconduct.

The combined use of AI and blockchain technologies can bring anti-corruption efforts to a new level by increasing efficiency, transparency and trust in public authorities while simultaneously reducing opportunities for abuse (PwC, 2025).

5. International Experience of AI-Enabled Public Administration and Lessons for Ukraine. To understand the importance of AI in public administration, it is useful to consider the experience of using AI in the public sector of different countries.

Estonia is one of the world leaders in the introduction of digital technologies into public administration, and its experience has become a benchmark for many other countries. An important component of Estonia's digital transformation is the e-Estonia project, which provides for the integration of all public services into a single digital platform. This enables citizens to receive online services in various areas such as health care, social benefits, business registration and taxation (AI Leap, 2025).

The use of artificial intelligence in this context makes it possible to significantly increase the efficiency of public services. One of the key elements is the X-Road system, which ensures the integration of all government information systems into a single platform. This allows the processing of large volumes of data, reduces costs and improves the efficiency of service delivery. AI is also used to forecast citizens' needs, which enables the state to respond promptly to changing circumstances and plan resources for service provision. In addition, the system contributes to the fight against corruption, since automation of a significant share of processes reduces the human factor, which is a major source of corruption risks.

Singapore is one of the most advanced examples of using AI to manage the urban environment and improve the quality of life of citizens. Within the Smart Nation initiative, the government of Singapore actively implements AI technologies in various areas of public administration, in particular for monitoring road traffic, forecasting needs in urban planning and managing energy resources (Smart Nation, 2025).

AI makes it possible to collect and analyse data on urban infrastructure, which improves the efficiency of resource use, reduces energy costs and improves the environmental situation (Smart Nation, 2025). For example, the traffic management system uses AI algorithms to determine optimal routes based on data about the current state of the roads and traffic forecasts, which helps reduce congestion and improve travel times for citizens. The accumulated data also makes it possible to plan infrastructure development more effectively and to build new facilities where they are most needed.

According to a 2021 study by McKinsey & Company, more than 60% of US federal agencies already use AI technologies or plan to implement them in the coming years. This includes such areas as document automation, forecasting citizens' needs and optimisation of management processes.

According to information provided on USA.gov, over 50% of US public bodies actively use various forms of AI-based automation to simplify and accelerate the processing of citizens' applications, to monitor and manage administrative processes, and to collect and analyse data in real time (Carahsoft, 2025).

One of the important areas is tax administration, where AI helps detect tax fraud and abuses. AI algorithms analyse large volumes of financial data, identifying anomalies and potential cases of fraud.

Public institutions are responsible for using data to make important decisions that affect everything from citizens' everyday lives to issues of national security. Thanks to artificial intelligence (AI), machine learning (ML) and high-performance computing (HPC), the public sector can manage data efficiently and securely while maintaining regulatory compliance (Carahsoft, 2025).

In addition, AI is used to automate interaction with citizens through voice assistants and chatbots, which makes it possible to provide round-the-clock support without involving staff. For example, national support services in the United States use chatbots to provide advice on a range of issues, from taxation to social security. These systems help reduce the workload on public servants and make services more accessible and responsive for citizens.

The United States also uses systems that apply AI to collect and analyse data from different sources in order to identify patterns and predict citizens' needs (Carahsoft, 2025). For instance, by analysing social media data, the government can obtain additional information about public sentiments and needs, which helps improve planning of social services and responses to current challenges.

Artificial intelligence is being actively implemented in many countries around the world. In addition to Estonia, Singapore and the United States, many other states also use AI in various areas of public administration, the economy and the social sector.

China is actively introducing AI technologies into public administration and investing in AI development with the aim of increasing the efficiency of public services and ensuring national security. According to the Ministry of Science and Technology of China, in 2020 the country spent more than 10.5 billion US dollars on AI research and development. China plans to become a world leader in AI technologies by 2030, in particular through initiatives such as "Made in China 2025", which envisages the large-scale introduction of AI in government processes and in the health care, transport and urban management sectors. In 2021 China also increased spending on projects related to the automation of management processes by 18% compared to the previous year, and more than 60% of large state-owned enterprises have already integrated AI to optimise their internal operations.

The government is actively investing in AI technologies and has ambitious plans for AI use in various fields:

- Urban management and infrastructure: China uses AI to monitor urban traffic, improve logistics and optimise energy resources.
- Intelligent security systems: China extensively applies facial recognition technologies to ensure public safety, which are actively used by the police and other public bodies.
- Medicine and health care: AI is used to analyse medical images, diagnose diseases and predict their development.

India is actively developing the use of AI technologies in public administration, focusing on improving the efficiency of public services and digitalising government processes. According to the Indian government, in 2020 the country invested more than 1.1 billion US dollars in AI development. India aims to become one of the leaders in this sphere, and within the national AI for All strategy the government plans to invest a further 10 billion US dollars by 2025 to integrate AI into various fields, including agriculture, health care, education and security. AI-based programmes in India support the monitoring of social benefits, the improvement of the health care system and the forecasting and management of infrastructure projects. According to the National Informatics Centre of India, more than 30% of government initiatives use AI technologies to improve the delivery of public services (Press Information Bureau, 2025).

India actively uses AI to develop the health care sector, urban management and to improve access to education and social services. AI technologies are used for disease diagnosis and to improve access to medical services in remote regions. In public administration AI is used to automate administrative processes such as citizen registration, the provision of social benefits and tax administration. India also applies AI to create adaptive learning platforms that make it possible to provide personalised educational services.

Canada is actively implementing AI in public and economic structures, especially in the health care and financial sectors. AI is used to improve access to medical services and to enhance diagnostic and treatment procedures. In Canada AI is used to detect financial fraud and improve the efficiency of financial services. AI helps public institutions analyse large data sets, which allows a better forecasting of social needs and more effective resource planning.

In 2021 the Canadian government announced investments of 125 million Canadian dollars to develop AI and its application in the public sector within the "AI Strategy for Canada". This includes the creation of innovative solutions for automating administrative processes such as processing applications for social benefits, monitoring citizens' health and managing urban infrastructure. In addition, the Canadian Intellectual Property Office actively uses AI algorithms for patent analysis and to facilitate access to cutting-edge technologies. As a result, the Canadian government has managed to reduce administrative process costs by 15% and improve service efficiency for citizens by 20% over the past five years (Canadian Management Centre, 2025).

In the United Kingdom, the Gov.uk Verify system is one of the most successful examples of using AI to automate administrative processes. This system was developed to ensure secure online interaction between citizens and public institutions. It enables citizens who wish to use different public services to verify their identity online, guaranteeing a high level of security and confidentiality (Gov.uk, 2025).

The Gov.uk Verify system uses AI to perform several functions:

- verification of personal data;
- automation of the registration process;
- enhancement of security.

The system applies AI algorithms to verify citizens' personal data such as passports, driving licences and utility bills in order to confirm the user's identity. Citizens can automatically create a digital profile that provides access to various public services without the need to visit authorities in person. The use of AI technologies such as biometrics and machine learning makes it possible to detect false or forged documents, which significantly reduces the risk of fraud.

Gov.uk Verify uses AI for the provision of online services, the verification of citizens' personal data and security assurance during interaction with public institutions.

AI is also being integrated into medical technologies, particularly for the recognition of medical images and monitoring of patients' conditions. AI is used to collect and analyse data on citizens, which enables public authorities to forecast population needs more accurately.

Japan is one of the countries that actively applies AI technologies in the management of social services and industry. In Japan, where the share of elderly people is increasing, robotic technologies and AI are used for elder care and the optimisation of social services. Japan uses AI to automate production processes, making them more efficient. AI technologies are employed for disease prediction and for improving treatment processes.

Finland is actively implementing AI in various areas of public administration and business. The country uses AI to automate the processing of citizens' requests, improve social services and support urban management. AI is used to develop personalised educational platforms that allow students to receive education tailored to their needs and abilities. AI is also extensively applied to detect financial fraud and to improve the processing of large data volumes in the banking sector.

Israel is another leader in the introduction of AI technologies, especially in the fields of security and defence. Israel uses AI to analyse intelligence data, monitor and prevent threats in real time. AI is actively used for diagnostics, disease prediction and the provision of health services on the basis of big data.

The international experience of AI-enabled public administration demonstrates that successful implementation of artificial intelligence in the public sector is based on a combination of long term digital strategies, stable investments and clear institutional responsibilities. Estonia, Singapore, the United States, China, India, Canada, the United Kingdom, Japan, Finland and Israel illustrate different models of integrating AI into urban management, social policy, health care, taxation, identity management and security. These cases show how AI can enhance the efficiency, transparency and responsiveness of public services while simultaneously creating new demands for data governance, ethical standards and cyber security. For Ukraine, a systematic comparison of these approaches is important for identifying realistic priorities, avoiding fragmented pilot projects and aligning national strategies with global trends in digital governance.

Table 1.28. International experience of AI-enabled public administration and lessons for Ukraine

Country	Main domains of AI use in public administration	Key instruments and initiatives	Observed or expected effects	Possible lessons for Ukraine
Estonia	Integrated digital government, online public services, anti corruption	e-Estonia platform, X-Road data exchange layer, AI modules for forecasting citizens' needs	Seamless access to health, social, business and tax services; reduced costs; faster decisions; lower corruption risks due to process automation	Build a single secure interoperability platform for state registers; prioritise end to end digital services; embed AI into existing digital infrastructure rather than isolated projects
Singapore	Smart city management, transport, energy, urban planning	Smart Nation initiative, AI based traffic management and resource optimisation systems	More efficient use of infrastructure and energy, reduced congestion, better environmental outcomes, data driven urban planning	Use AI for city level pilots in transport, utilities and urban planning; combine technical systems with clear performance indicators and environmental goals
United States	Document automation, tax administration, social security, real time analytics, citizen interaction	AI and ML systems in federal agencies, AI supported fraud detection in taxation, chatbots and voice assistants in national support services, high performance computing for data management	Faster processing of applications, improved fraud detection, better forecasting of social needs, round the clock digital support for citizens	Introduce AI for back office process automation and fraud detection in tax and social spheres; develop ethical and legal frameworks for algorithmic decision making in the public sector
China	Urban management, logistics, security, health care, large scale automation of government processes	National AI programmes, "Made in China 2025", city level AI platforms, facial recognition in public safety, AI in medical imaging and diagnosis	Strong integration of AI into security and urban management, rapid scaling of AI projects, significant budgetary support and coordination	Treat AI as part of long term industrial and security policy; plan flagship projects with stable funding while balancing innovation with rights protection and data safeguards
India	Social benefits, health care, education, agriculture, infrastructure projects	National strategy AI for All, AI based monitoring of social payments, adaptive learning platforms, AI tools in tax and administrative services	Better targeting of social programmes, improved access to medical and educational services in remote areas, more accurate planning of infrastructure	Use AI to improve targeting of social support and regional development; combine AI projects with programmes that remedy regional digital divides and capacity gaps
Canada	Health care, financial regulation, social services, urban infrastructure	AI Strategy for Canada, AI supported diagnostics, fraud detection in	Reduced administrative costs, higher efficiency of public services, better anticipation of	Link AI projects with national innovation and intellectual property policies; invest in analytical capacity in

Country	Main domains of AI use in public administration	Key instruments and initiatives	Observed or expected effects	Possible lessons for Ukraine
		financial services, AI in patent analysis at the Canadian Intellectual Property Office	social needs, improved access to innovations	ministries and agencies so that AI outputs are critically interpreted
United Kingdom	Digital identity, secure access to online public services, anti fraud measures	Gov.uk Verify digital identity system using AI, biometrics and ML for verification and fraud detection	Secure remote access to public services, reduced need for in person visits, better protection against identity fraud	Develop a national digital identity framework with AI enhanced verification; ensure high standards of privacy, cybersecurity and public trust
Japan	Social services for the elderly, industrial automation, health care	AI and robotics in elder care, AI based disease prediction and treatment optimisation, AI in manufacturing processes	Support for ageing population, higher productivity in industry, more timely medical interventions	Use AI for demographic challenges such as ageing and regional depopulation; integrate AI with robotics and telemedicine where human resources are scarce
Finland	Social services, urban management, education, banking and financial supervision	AI for processing citizens' requests, personalised educational platforms, AI supported fraud detection and big data processing in the banking sector	More responsive social services, personalised learning, enhanced financial integrity and more efficient data handling	Apply AI to front line services and education; promote open data and interoperability to encourage innovation by public and private actors
Israel	Security and defence, intelligence analysis, health care	AI based systems for real time threat monitoring, analysis of intelligence data, AI in diagnostics and predictive medicine	Strengthened national security, faster identification of threats, advanced medical services based on big data	Develop AI capacities in critical security and resilience domains while ensuring democratic oversight; use security driven AI advances to support civilian health and emergency management systems

Source: developed by the authors

The comparative analysis of international experience shows that AI is not a single technology but a complex layer of tools embedded in wider strategies of digital governance, security, social policy and innovation. Countries that achieve visible results rely on robust data infrastructures, integrated digital platforms and clear institutional mandates for AI deployment. At the same time, they invest in human capital, cyber security and ethical regulation in order to prevent abuses and maintain public trust. For Ukraine, the key implication is that AI in public administration should be developed as part of a coherent national digital state strategy with pilots in clearly defined sectors such as social protection, taxation, urban

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

management and health care. Only the combination of technical solutions, organisational reforms and a strong legal and ethical framework can ensure that AI becomes a driver of more effective, transparent and inclusive public governance.

Conclusions. The monograph provides a detailed examination of the role of artificial intelligence in contemporary public administration, with particular emphasis on enhancing the efficiency of public service delivery in Ukraine. Artificial intelligence technologies open significant opportunities for improving public governance, optimising administrative processes, raising the quality of services for citizens, and ensuring greater transparency in the activities of public authorities.

The use of AI to automate routine tasks allows a substantial reduction in the administrative burden on civil servants, freeing their resources for the resolution of more complex and strategic issues. Technologies such as machine learning and deep learning are able to improve decision making, since the processing of large volumes of data makes it possible to identify trends, forecast citizens' needs, and ensure more precise resource management. Examples of the application of these technologies in other countries show that they can form the basis for the modernisation of state structures, the enhancement of managerial effectiveness, and the achievement of sustainable development.

One of the most important aspects of AI use is the personalisation of services for citizens. Through machine learning algorithms it becomes possible to forecast more accurately the needs of different social groups, such as pensioners, people with disabilities, and large families, and to provide them with tailored services. This significantly improves citizens' quality of life and makes public services more accessible and user friendly. Personalisation also helps to reduce bureaucratic barriers and to ensure a more rapid response to changes in social conditions.

The implementation of AI in public administration contributes to greater transparency, which is crucial in the fight against corruption. The automation of decision making processes, together with the use of instruments such as blockchain, can considerably reduce the role of the human factor in decisions and lower the scope for abuse. This provides greater openness in interaction between public institutions and citizens, particularly in the areas of public procurement, the provision of social assistance, and the management of budgetary funds.

The use of AI also supports the response to various challenges facing public administration, such as limited budgetary resources and complex social problems. Owing to its capacity for forecasting and modelling different scenarios, AI enables public authorities to plan resources more effectively and to optimise expenditures. This is especially important in conditions of economic instability and the need for rational allocation of public funds.

Taking into account the experience of countries such as Estonia, Singapore, the United States and others, it is possible to observe the positive impact of AI on management processes and the quality of public services. Ukraine has all the prerequisites for integrating these technologies into public administration, since basic digital infrastructures already exist and there is experience in using individual elements of AI in such areas as tax administration and the provision of social services. However, successful large scale implementation of AI requires the resolution of several key tasks, including infrastructure modernisation, training and capacity building for personnel, enhancement of cybersecurity, and the development of a legal framework that regulates the ethical and legal aspects of AI use in public administration.

It is also important to highlight the need to strengthen cooperation between public authorities, the private sector, and academic institutions in order to create innovative solutions and to ensure the sustainable development of AI technologies. Raising the level of digital literacy among citizens and expanding access to advanced technologies are essential steps towards building trust in digital tools in governance.

In conclusion, the continued development of AI has the potential to become a key instrument for the modernisation of public administration in Ukraine, ensuring more effective delivery of public services, higher transparency, stronger anti corruption measures, and improved interaction between citizens and the state. A successful integration of AI requires not only technological support but also strategic, legal, and social foundations. This will enable Ukraine to improve substantially the quality of life of its citizens, support economic development, and ensure the sustainable evolution of public administration in the digital era.

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. Vahanova, L. V., Yurychyna, I. A., & Karpanasiuk, O. S. (2022). Upravlinske rishennia yak forma realizatsii orhanizatsiinoi funktsii derzhavnoho upravlinnia [Managerial decision as a form of implementing the organisational function of public administration]. *Visnyk Khmelnytskoho natsionalnoho universytetu*, (1), 94–98.
2. Pohorelenko, A. (2018). Shtuchnyi intelekt: sutnist, analiz zastosuvannia, perspektyvy rozvytku [Artificial intelligence: Essence, application analysis, development prospects]. *Ekonomichni nauky*, (32), 22–27.
3. Palamarchuk, A. I. (2024). Sudovyi zakhyst prava na dostup do informatsii pro stan navkolyshnoho seredovyshcha v umovakh voiennoho stanu [Judicial protection of the right to access information on the state of the environment under martial law]. In *Suchasni vyklyky ta aktualni problemy sudovoi systemy v Ukraini* [Contemporary challenges and pressing problems of the judicial system in Ukraine] (p. 466). Chernivtsi, Ukraine. Retrieved March 2, 2025, from: https://web.ccu.gov.ua/library/suchasni-vyklyky-ta-aktualni-problemy-sudovoyi-reformy-v-ukrayini-2024
4. Shevchenko, A. I., & Baranovskyi, S. V. (2023). *Stratehiia rozvytku shtuchnoho intelektu v Ukraini. Rozdil 4. Stan rozvytku sfery shtuchnoho intelektu v Ukraini* [Strategy for the development of artificial intelligence in Ukraine. Section 4. State of development of the artificial intelligence sphere in Ukraine] (p. 66). Kyiv, Ukraine. Retrieved March 10, 2025, from: https://jai.in.ua/archive/2023/ai_mono.pdf
5. Mizhnarodnyi fond «Vidrodzhennia». (2025). *Doslidzhennia nadannia sotsialnykh posluh: Problemy ta stan sfery sotsialnykh posluh v Ukraini* [Study of the provision of social services: Problems and state of the social services sector in Ukraine]. Retrieved March 19, 2025, from: https://parlament.org.ua/news/problemy-ta-stan-sfery-soczialnyh-poslug-v-ukrayini-lzi-provela-prezentacziyu-doslidzhennya/
6. Zastosuvannia hlybokoho navchannia v shtuchnomu intelekti [Applications of deep learning in artificial intelligence]. (2025). *Stfalcon Blog*. Retrieved March 21, 2025, from https://stfalcon.com/uk/blog/post/5-fascinating-applications-of-deep-learning
7. Shcho take shtuchnyi intelekt: Istoriia, vydy ta skladovi [What is artificial intelligence: History, types and components]. (2025). *GigaCloud*. Retrieved March 19, 2025, from: https://gigacloud.ua/articles/shho-take-shtuchnyj-intelekt-istoriya-vydy-ta-skladovi/
8. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433–460. https://doi.org/10.1093/mind/LIX.236.433
9. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence (1955). *AI Magazine*, 27(4), 12–14.
10. Fukuyama, F. (2014). *Political order and political decay: From the industrial revolution to the globalization of democracy*. Farrar, Straus and Giroux.
11. Newell, A., Shaw, C., & Simon, H. (1959). Report on a general problem-solving program. In *Proceedings of the International Conference on Information Processing* (pp. 256–264).

12. Cordella, A., & Hesse, J. (2015). E-government in the making: An actor-network perspective. *Transforming Government: People, Process and Policy*, 9(1), 104–125. https://doi.org/10.1108/TG-02-2014-0006
13. Hinton, G., Osindero, S., & Teh, Y. (2006). A fast learning algorithm for deep belief nets. *Neural Computation*, 18(7), 1527–1554. https://doi.org/10.1162/neco.2006.18.7.1527
14. Gaozhao, D., Wright, J. E., & Gainey, M. K. (2023). Bureaucrat or artificial intelligence: People's preferences and perceptions of government service. *Public Management Review*, 1–28. https://doi.org/10.1080/14719037.2022.2160488
15. Ranerup, A., & Henriksen, H. Z. (2022). Digital discretion: Unpacking human and technological agency in automated decision making in Sweden's social services. *Social Science Computer Review*, 40(2), 445–461. https://doi.org/10.1177/0894439320980434
16. Veale, M., & Brass, I. (2019). Administration by algorithm? Public management meets public sector machine learning. In *Algorithmic regulation* (pp. 1–30). https://doi.org/10.31235/osf.io/mwhnb
17. Weizenbaum, J. (1966). ELIZA – A computer program for the study of natural language communication between man and machine. *Communications of the ACM*, 9(1), 36–45. https://doi.org/10.1145/365153.365168
18. Zuiderwijk, A., Chen, Y.-C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38, Article 101577. https://doi.org/10.1016/j.giq.2021.101577
19. e-Estonia. (2025). *AI Leap programme to bring AI tools to all schools*. Retrieved March 17, 2025, from: https://e-estonia.com/estonia-announces-a-groundbreaking-national-initiative-ai-leap-programme-to-bring-ai-tools-to-all-schools/
20. Carahsoft. (2025). *AI solutions for government: AI in the public sector*. Retrieved March 20, 2025, from: https://www.carahsoft.com
21. Canadian Management Centre. (2024). *Discover 2024 AI trends*. Retrieved March 22, 2025, from: https://cmcoutperform.com/
22. Government Digital Service. (2025). *Introducing GOV.UK Verify*. Retrieved March 22, 2025, from: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
23. Press Information Bureau. (2024). *India's AI revolution*. Retrieved March 27, 2025, from: https://pib.gov.in/PressReleasePage.aspx?PRID=2108810
24. Smart Nation and Digital Government Office. (2025). *Smart Nation Singapore initiative*. Retrieved March 22, 2025, from: https://www.smartnation.gov.sg/
25. PwC. (2025). *Strategy in the age of AI*. Retrieved March 12, 2025, from: https://www.pwc.com/us/en/services/ai.html
26. IBM. (2025). *What is NLP (natural language processing)?* Retrieved March 22, 2025, from: https://www.ibm.com/think/topics/natural-language-processing

Chapter 2
Public Governance of Digital Accounting and Reporting: Risk-Based Supervision, Anti-Fraud Policy, and Economic Security

https://doi.org/10.36690/PUBADM

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

Section 2.1. Risk-Based Digital Supervision and Anti-Fraud Governance: Policy Instruments, Compliance, and Administrative Burden Reduction

Iryna Mihus[1]

[1] *Doctor of Science (Economics), Professor, Visiting Professor of the Pontifical Catholic University of Paraná (Curitiba, Brazil), Director of the Scientific Center of Innovative Research (Estonia), Professor of the Department of Financial and Economic Security Management, "KROK" University (Kyiv, Ukraine), ORCID: https://orcid.org/0000-0001-6939-9097*

Citation:
Mihus, I. (2025). Risk-Based Digital Supervision and Anti-Fraud Governance: Policy Instruments, Compliance, and Administrative Burden Reduction. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 79-101). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-79-101

The publication was funded by a scholarship provided in accordance with the Program for the Reception of Ukrainian Scientists of the Araucaria Foundation (agreement 042/2024) and the Pontifical Catholic University of Paraná (PUCPR), Brazil, as a participant in the project "Possibilities of using blockchain technologies in corporate governance."

Abstract. *Risk based digital supervision is often evaluated through visible digital artefacts, yet durable public value depends on institutional mechanisms that enable lawful data use, interoperability, accountability, and inclusion, supported by safeguards that preserve legitimacy. The goal of this study is to conceptualize risk based digital supervision and anti-fraud governance by linking the evolution of supervision, mechanism-based fraud typologies and indicators, and instrument level evaluation focused on administrative burden reduction, detection, deterrence, and fairness. The study applies qualitative policy synthesis and institutional reasoning to systematize the shift from inspection led compliance to harm-oriented supervision, to define decision grade indicator frameworks grounded in fraud mechanisms, and to develop an evaluation logic that connects instruments to outcomes and governance requirements. The analysis shows that modern supervision evolves toward risk segmentation and analytics enabled triage, which can improve timeliness and consistency but also introduces governance obligations related to explainability, auditability, model risk, and due process. It further demonstrates that anti-fraud functions as the operational core of the risk approach because it translates abstract risk into observable patterns, measurable indicators, and coordinated responses that rely on lawful data reuse, reliable identifiers, and inter agency routines. In addition, the results indicate that reform effectiveness depends on a coherent instrument mix combining prevention, compliance support, targeted detection, and proportionate enforcement, reinforced by trace governance and performance management that prioritizes outcomes rather than digitization counts. Risk based digital supervision is best understood as institutional capacity building that aligns law, data governance, analytics, and accountability into an integrated decision cycle, enabling harm reduction with proportional burden and defensible legitimacy.*

Keywords: *risk-based supervision; digital supervision; anti-fraud governance; supervisory analytics; interoperability; lawful data sharing; digital traces; model governance; compliance risk management; administrative burden reduction; fairness and legitimacy.*

https://doi.org/10.36690/PUBADM

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

1. Evolution of supervision: from inspections to risk-based supervision and supervisory analytics. Supervision was long organised around inspection-led compliance, where regulators verified conformity with prescriptive rules through periodic checks, documentary reviews, and on-site visits. This approach offered legal clarity and a straightforward accountability narrative because effort could be reported through inspection counts, sanctions, and findings. At the same time, as markets and administrative systems became more complex, inspection-led models increasingly struggled to align supervisory effort with actual harm. Three structural limitations became prominent: weak targeting precision, high compliance costs for low-risk actors, and a reactive posture in which problems are often identified after harm has occurred (OECD, 2014).

Risk-based supervision emerged as an institutional response to these limitations by reframing supervision as harm reduction under capacity constraints. Instead of treating all entities as equally likely to create harm, the risk-based approach segments the supervised population, prioritises resources according to probability and impact, and applies proportional interventions. OECD best practice principles emphasise targeting, proportionality, consistency, and the need to embed these principles into governance arrangements rather than treating them as optional techniques (OECD, 2014; OECD, 2018).

The Table 2.1 contrasts the governance logic of inspection-led and risk-based supervision, clarifying how accountability shifts from activity reporting to outcome justification.

Table 2.1. Evolution of supervision models across core governance dimensions

Dimension	Inspection-led compliance	Risk-based supervision	Analytics-enabled risk-based supervision
Primary aim	Verify rule compliance	Reduce harm through prioritisation	Reduce harm with earlier detection and consistent triage
Unit of action	Inspection event	Risk segment and supervisory plan	Risk signals integrated into case management
Information base	Documents, site evidence	Risk assessment, history, sector signals	Integrated datasets, digital traces, anomaly patterns
Cadence	Periodic, scheduled	Targeted, adaptive	Increasingly continuous for high-risk areas
Accountability	Counts of inspections and sanctions	Outcomes plus proportionality rationale	Outcomes plus model governance and auditability
Main limitation	High burden, weak targeting	Data gaps, inconsistent criteria	Model risk, data quality, cyber and privacy exposure

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2014; Organisation for Economic Co-operation and Development, 2018)

https://doi.org/10.36690/PUBADM

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

The evolution is institutional: supervision moves from episodic verification toward prioritised harm reduction, and analytics adds new accountability obligations.

The shift shown in Table 2.1 has two immediate implications for design. First, risk-based supervision requires explicit decision rules that justify selectivity. Selective scrutiny can improve effectiveness, yet it also increases the need for transparency, consistency, and appealability because regulated actors may perceive targeting as arbitrary unless the criteria are explainable and applied consistently (OECD, 2014; OECD, 2018). Second, risk-based supervision pushes regulators to define harm categories and to connect supervisory actions to those harms, otherwise risk classification becomes an administrative ritual rather than an operational tool.

The table 2.2 operationalises segmentation by linking risk tiers to supervisory stance and proportional instruments, making “risk-based” concrete in supervisory planning.

Table 2.2. Risk segmentation and proportional supervisory stance

Risk tier	Supervisory objective	Typical instruments	Expected burden profile	Governance safeguard
Low	Maintain compliance at low cost	Guidance, self-reporting, light-touch checks	Low and predictable	Clear criteria and periodic validation
Medium	Correct emerging weaknesses	Targeted reviews, thematic checks, remediation plans	Moderate and time-bound	Consistency and documented escalation rules
High	Prevent material harm	Intensive supervision, on-site inspections, enforcement	Higher but justified by risk	Explainability, due process, audit trails
Critical or systemic	Contain contagion and protect trust	Continuous monitoring, special measures, coordinated actions	High, tightly governed	Senior oversight and legality controls

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2014; Organisation for Economic Co-operation and Development, 2018).

Segmentation is defensible when it links risk to proportional instruments and explicitly manages legitimacy through procedural safeguards.

Segmentation alone does not ensure effectiveness, because a risk-based regime also needs a supervisory cycle that translates risk assessments into operational decisions, including planning, intervention, and learning. In inspection-led systems, the cycle often ends with a completed inspection and an enforcement outcome. In risk-based systems, the cycle should end with evidence about whether harm reduced and whether risk models and instruments need recalibration. This is where supervisory analytics becomes structurally important, not as a reporting upgrade but as a capability that strengthens risk identification, improves triage consistency, and reduces delays in detecting patterns across entities and time.

The Table 2.3 specifies the risk-based supervisory cycle and pinpoints where analytics changes decisions, ensuring that data is tied to action rather than to passive dashboards.

Table 2.3. Risk-based supervisory cycle and analytics touchpoints

Cycle stage	Core decision	Typical supervisory action	Analytics contribution	Governance requirement
Risk identification	What harms matter	Define taxonomy and signals	Signal catalogue, data mapping	Legal basis and documentation
Risk assessment	Who is higher risk and why	Classification and segmentation	Scoring, clustering, network signals	Explainability and validation
Planning	Where to allocate capacity	Proportional plans	Prioritisation and scenario selection	Transparent criteria and consistency checks
Intervention	What action is proportionate	Guidance, targeted inspection, sanctions	Case triage and evidence assembly	Human review and due process
Evaluation	Did harm reduce	KPI review and redesign	Trend analysis and drift detection	Audit trails and learning loop

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2014; Organisation for Economic Co-operation and Development, 2018)

Analytics improves supervision only when integrated into each stage with explicit governance controls and feedback routines.

Supervisory analytics is commonly referred to as SupTech, meaning technology used by supervisors to improve data collection, analysis, and supervisory processes. Early user experience documented by the Bank for International Settlements highlights that SupTech can enhance effectiveness and efficiency, while also raising operational, legal, and resource challenges (Broeders & Prenio, 2018). The World Bank discussion note on market conduct supervision similarly emphasises that SupTech adoption is constrained by data quality, institutional capacity, and the need to preserve professional judgement even when analytic tools expand screening and filtering capacity (World Bank, 2018). Toronto Centre guidance frames SupTech as a lever for more proactive supervision supported by better data and improved workflows (Toronto Centre, 2018).

The Table 2.4 clarifies the data foundations of analytics-enabled supervision by distinguishing administrative, behavioural, and trace data, and by linking each to supervisory uses and control requirements.

Table 2.4. Supervisory data foundations: sources, uses, and control requirements

Data source family	What it contains	Supervisory use	Primary quality risk	Minimal control
Regulatory reporting	Filings, statements, returns	Baselines, compliance monitoring	Inconsistent definitions	Standardisation and validation rules
Operational and incident data	Outages, breaches, operational events	Early warning and resilience oversight	Underreporting	Reporting obligations and audits
Complaints and consumer signals	Complaints, inquiries, dispute data	Market conduct risk detection	Noise and selection bias	Sampling, classification, triangulation
Digital traces	Access logs, workflow events, submissions	Process mining, anomaly detection	Incomplete logging	Logging standards and completeness checks
Market and third-party data	Prices, networks, open sources	Contextual risk signals	Provenance uncertainty	Source governance and careful use rules

Sources: systematized by the author based on (Broeders, D., & Prenio, J., 2018; World Bank, 2018; Toronto Centre, 2018)

Data richness increases supervisory power, but without governance and quality controls it also increases error, unfairness, and legitimacy risks.

Because analytics can influence targeting and enforcement, it introduces model risk and governance risk. Model risk includes poor calibration, drift, and false signals, while governance risk includes opaque criteria, unequal treatment, and inadequate mechanisms for contestation. In supervisory contexts, the governance standard must therefore be higher than in purely internal management analytics, because decisions affect rights, market access, reputations, and resource allocation. The Financial Stability Board highlights that SupTech and RegTech can improve efficiency and risk monitoring, while also requiring careful governance to manage operational and data risks (Financial Stability Board, 2020).

The Table 2.5 systematises analytics method families used in SupTech and clarifies their prerequisites and governance risks, supporting responsible method selection.

Table 2.5. Supervisory analytics methods: uses, prerequisites, and governance risks

Method family	Typical use	Data prerequisite	Primary governance risk	Minimal control
Descriptive analytics	Dashboards and monitoring	Standardised reporting	Misleading indicators	Data quality and metadata governance
Anomaly detection	Early warning and triage	Time series baselines	False positives and overreach	Human review and thresholds
Network analytics	Collusion and relationship risk	Reliable identifiers	Privacy and inference risk	Purpose limits and auditability
Text and NLP analytics	Pattern detection in text	Large text corpora	Opacity and bias	Sampling checks and interpretability
Process mining	Bottlenecks and exceptions	Event logs and traces	Incomplete traces	Logging standards and validation
Predictive scoring	Prioritising cases	Credible labels or proxies	Drift and bias	Validation and recalibration

Sources: systematized by the author based on (Broeders, D., & Prenio, J., 2018; World Bank, 2018; Financial Stability Board, 2020)

Method choice should be driven by supervisory purpose and governance capacity, not by technical novelty.

To translate Tables 2.4 and 2.5 into operational reality, supervisory authorities typically need a model governance framework. This framework should define purposes, decision rights, validation duties, monitoring for drift, and processes for explaining outputs to decision-makers and, where relevant, to regulated entities. The aim is not to eliminate judgement but to discipline it through documented, reproducible reasoning.

The Table 2.6 provides a model governance checklist tailored to supervision, where decisions must be defensible, auditable, and contestable.

Model governance is a prerequisite for scaling supervisory analytics because it protects legality, consistency, and trust.

Implementation is often constrained less by software acquisition and more by organisational design. Supervisors typically need to re-balance skills and workflows, introducing data stewardship and analytics roles while ensuring that supervisory staff can interpret and challenge analytic outputs. They also need to integrate analytics into case management so that insights become decisions and actions rather than parallel reporting streams. The BIS review of early SupTech users underscores the practical challenges of data, resourcing, and legal issues, indicating that capacity building and governance design must be planned alongside technical development (Broeders & Prenio, 2018).

https://doi.org/10.36690/PUBADM

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

Table 2.6. Model governance checklist for analytics-enabled supervision

Governance element	Requirement	Supervisory rationale	Observable evidence
Purpose and scope	Clear objective and limits	Prevents function creep	Model card and decision rules
Validation and calibration	Performance testing	Reduces systematic error	Validation reports and benchmarks
Explainability	Interpretable drivers	Supports legitimacy and appeals	Explanation outputs and guidance
Fairness review	Disparate impact checks where feasible	Protects equal treatment	Fairness audits and mitigation notes
Drift monitoring	Detect changes over time	Maintains reliability	Drift triggers and recalibration logs
Human oversight	Defined approval rights	Prevents automated enforcement	Review logs and escalation protocols
Auditability	Reproducibility and access logs	Ensures accountability	Version control and audit trails

Sources: systematized by the author based on (Financial Stability Board, 2020; Broeders, D., & Prenio, J., 2018; Toronto Centre, 2018)

The Table 2.7 proposes a phased implementation roadmap that aligns capability building with governance gates, reducing the risk of scaling fragile systems.

Table 2.7. Phased roadmap for adopting analytics-enabled risk-based supervision

Phase	Primary goal	Core deliverables	Governance gate for moving forward
Foundation	Make data usable and lawful	Data standards, validation, access controls	Data quality and legality sign-off
Targeting	Improve planning and triage	Risk taxonomy, segmentation, case management linkage	Transparent criteria and escalation rules
Analytics expansion	Add advanced methods safely	Anomaly detection, process mining, scoring	Validation, explainability, oversight routines
Continuous monitoring	Increase timeliness for high risk areas	Near real-time feeds, automated alerts	Resilience testing and incident readiness
Outcome governance	Link supervision to harm reduction	KPI framework, learning loops, redesign cycles	Independent review of outcomes and fairness

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2018; Broeders, D., & Prenio, J., 2018; World Bank, 2018)

Roadmaps work when each phase has measurable capability outputs and a governance gate that protects legitimacy.

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

The Table 2.8 identifies common failure modes in the transition to risk-based and analytics-enabled supervision and proposes mitigations aligned with OECD principles and SupTech experience.

Table 2.8. Common failure modes and mitigations in supervision modernisation

Failure mode	Why it happens	Observable symptom	Mitigation aligned with good practice
Digitised inspections without risk logic	Tools added, logic unchanged	Same plans, faster paperwork	Build taxonomy, segmentation, proportionality rules
Risk scores without governance	Models deployed without controls	Unexplained targeting, disputes	Validation, explainability, audit trails
Data integration without stewardship	Data pooled, quality unmanaged	Conflicting numbers, weak trust	Data owners, metadata, quality metrics
Dashboards without workflow change	Insights not embedded	Reports increase, actions do not	Case management integration and escalation
Scaling before safeguards	Speed prioritised	Incidents, trust decline	Security baselines, staged scaling, readiness gates
Narrow KPIs	Count-based incentives	Output inflation, gaming	Outcome KPIs tied to harm, burden, fairness

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2014; Organisation for Economic Co-operation and Development, 2018; Financial Stability Board, 2020; Broeders, D., & Prenio, J., 2018)

Most failures are governance failures, not software failures, and mitigations therefore emphasise decision rules, stewardship, and safeguards.

The evolution from inspection-led compliance to risk-based supervision reflects a shift from activity verification toward harm reduction under limited supervisory capacity. Supervisory analytics strengthens this shift by improving timeliness, consistency, and targeting, but it simultaneously raises governance requirements related to data quality, model risk, explainability, auditability, and fairness. Consequently, modernisation is best understood as institutional redesign in which segmentation, analytics, and enforcement are integrated into a supervised decision cycle with explicit safeguards and learning loops. In practice, supervision becomes genuinely "digital" when analytic insights change planning and interventions, and when legitimacy is protected through transparent criteria, due process, and robust model governance.

2. Anti-fraud as the core of the risk approach: typologies, indicators, data, and inter-agency coordination. Anti-fraud governance functions as the practical "engine" of risk-based supervision because it translates abstract risk concepts into observable patterns, measurable signals,

https://doi.org/10.36690/PUBADM

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

and enforceable responses. While traditional inspection models often concentrated on detecting non-compliance after the fact, risk-based approaches treat fraud and abuse as dynamic behaviours that adapt to controls, exploit weak interfaces between institutions, and concentrate where oversight is fragmented. In this logic, anti-fraud is not a narrow compliance add-on. It is the discipline that connects supervision strategy, data governance, and enforcement proportionality, ensuring that scarce supervisory resources focus on the highest harm profiles while avoiding unwarranted burdens for lower-risk actors. International guidance increasingly frames effective supervision as tailoring intensity, frequency, and tools to assessed risk, and explicitly recognises that a risk-based approach should reduce unnecessary compliance burden for low-risk segments while improving overall system effectiveness (FATF, 2021). For public governance, the anti-fraud core is also a public value claim: citizens accept data-driven oversight when it is lawful, accountable, and demonstrably fair, and when it produces tangible reductions in waste, abuse, and administrative burden.

Fraud typologies as "mechanisms," not only categories. Fraud typologies are most useful when defined by mechanism. Mechanism-based typologies identify how value is extracted, which controls are bypassed, and which data traces are left behind. This approach supports risk-based supervision because it enables supervisors to connect "what happened" to "how it happened" and to "what should change" in institutional routines. It also helps avoid a common trap of digital reforms: counting detected cases without improving the underlying control environment, data quality, and inter-agency coordination that determine whether detection is systematic or accidental. Updated fraud risk management guidance emphasises governance, periodic fraud risk assessment, preventive and detective controls, investigations, and continuous monitoring as an integrated programme rather than isolated tools (COSO & ACFE, 2023). In public sectors, the same logic applies across domains such as procurement, tax, social benefits, licensing, grants, and regulated industries.

Mechanism-based typologies enable a more disciplined chain of reasoning:

– define harm and mechanism,
– identify observable indicators,
– map indicators to data sources,
– select proportionate supervisory actions.

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

Table 2.9. Mechanism-Based Typology of Fraud Relevant to Risk-Based Supervision

Typology (mechanism)	Typical scheme pattern	Common control weakness exploited	"Digital trace" candidates
Identity and eligibility fraud	False identity, synthetic identity, duplicate beneficiaries	Weak identity assurance, siloed registries	Duplicate identifiers, device reuse, repeated contact details
Procurement collusion and bid rigging	Bid rotation, cover bids, subcontracting to "losing" bidders	Limited market intelligence, weak red-flag monitoring	Repeated winner networks, abnormal price dispersion, bidder relationships
Invoice and payment fraud	Fake invoices, split invoices, duplicate payments	Weak three-way matching, weak segregation of duties	Duplicate invoice numbers, unusual vendor bank changes, timing anomalies
Grants and subsidy misuse	Misreporting, front companies, non-delivery	Limited verification capacity, weak ex-post audits	Beneficial owner overlaps, delivery proof gaps, anomaly in outcomes reporting
Regulatory evasion and reporting manipulation	Misclassification, underreporting, structured avoidance	Low data reuse, limited cross-checks	Discrepancies across filings, outliers vs peers, "too consistent" reporting
Corruption-enabled fraud	Bribery to bypass controls, conflict of interest	Weak transparency, weak conflict-of-interest controls	Award concentration, decision-maker links, unusual exceptions granted

Sources: systematized by the author based on (COSO & ACFE, 2023; World Bank, 2019)

This chain is essential because the same surface event, for example a single-bid procurement, may reflect legitimate market conditions or coordinated collusion. Without mechanism thinking, supervision either becomes overly punitive and burdensome or overly permissive and ineffective. Evidence from data analytics applications in integrity and fraud risk management also suggests that analytics can complement qualitative judgement by improving prioritisation, reducing both false positives and false negatives, and supporting earlier interventions, but it cannot replace governance discipline and professional scepticism (OECD, 2019).

Risk indicators: from red flags to decision-grade signals. In risk-based supervision, indicators must be designed for decisions, not for dashboards. A useful indicator is one that changes supervisory action in a predictable way and is defensible under legal and ethical scrutiny. In practice, indicator systems combine structural risk indicators, transactional anomalies, behavioural signals, and network patterns. Procurement illustrates the point well because some warning signs are visible in single bids, while others only emerge across multiple tenders, suppliers, and time periods. The World Bank's procurement guidance highlights warning signs such as unexplained inflated prices, identical unit prices across different bidders, unusual last-minute discounts, and patterns such as losing bidders becoming subcontractors or apparent bid rotation (World Bank, 2019). These are not proofs of wrongdoing; they are triage signals that trigger proportionate follow-up.

Table 2.10. Indicator Families for Anti-Fraud Triage in Risk-Based Supervision

Indicator family	Examples of operational indicators	Typical data inputs	Supervisory use
Structural and concentration	Winner concentration, repeated single-bid awards, unusual market share shifts	Contract registers, supplier registry	Prioritise sectors and buyers for review
Price and cost anomalies	Price above benchmark, identical pricing across bids, split-contract patterns	Bid data, cost estimates, catalogues	Flag tenders for forensic sampling
Process deviations	Excessive exceptions, late modifications, rushed timelines	Workflow logs, approvals, audit trails	Check control compliance and accountability
Network and relationship patterns	Shared owners, repeated subcontract chains, bidder clusters	Beneficial ownership, corporate registry, subcontract data	Detect collusion risk and hidden dependencies
Behavioural and integrity signals	Unusual access patterns, repeated overrides, conflicts of interest	System logs, HR declarations, access management	Trigger targeted controls and investigations

Sources: systematized by the author based on (OECD, 2019; World Bank, 2019)

Between "red flag" and "sanction" there must be a clearly defined escalation ladder. This ladder protects fairness and reduces burden by ensuring that low-confidence signals lead to low-intrusion actions, while high-confidence patterns justify deeper investigation. In addition, indicator systems must be continuously recalibrated because fraud adapts to controls and because digital reforms change baseline behaviour. A robust approach therefore specifies indicator thresholds, evidence standards, and review responsibilities, and it documents why particular indicators are used, what biases they may introduce, and how affected parties can contest outcomes. This is consistent with the broader integrity literature that stresses institutional clarity in roles, assurance, and co-ordination, including how audit and oversight functions relate to fraud and corruption prevention (OECD, 2020).

Data and inter-agency coordination: making "hidden dependencies" governable. Anti-fraud risk approaches fail most often not because analytics are weak, but because the underlying data ecosystem is fragmented. Fraud schemes commonly exploit seams: different eligibility rules across programmes, inconsistent identifiers, gaps between registries, or weak feedback loops between detection and policy correction. Therefore, the core institutional question is not only “who detects,” but also “who owns which data,” “who may share which attributes under which legal basis,” and “who is accountable for data quality and correction.” OECD work on analytics for integrity underlines that investing in data-driven risk assessment requires attention to data governance, data quality controls, skills, and institutional readiness, and that early “quick wins” can build legitimacy while longer-term governance capability is constructed (OECD, 2019). In parallel, supervisory guidance emphasises domestic co-operation between relevant authorities as part of effective risk-based supervision, particularly where risks and responsibilities cross organisational boundaries (FATF, 2021).

Table 2.11. Minimum Viable Data Architecture for Anti-Fraud Governance

Data layer	Purpose in anti-fraud	Typical stewardship logic	Key governance controls
Identity and entity resolution	Link persons and organisations across systems	Central identity authority or federated trusted sources	Identity assurance, deduplication, lawful access controls
Transaction and decision logs	Reconstruct decisions and detect anomalies	Owning agency, standardised audit logging	Immutable logs, access monitoring, retention rules
Registries and reference data	Provide ground truth for validation	Registry owners with shared standards	Data quality KPIs, change control, interoperability standards
Network and ownership data	Reveal hidden links and collusion risk	Corporate registry plus beneficial ownership sources	Verification routines, update frequency, uncertainty flags
Outcomes and feedback data	Measure deterrence and burden reduction	Supervisory authority with evaluation mandate	Evaluation protocols, bias review, publication rules

Sources: systematized by the author based on (FATF, 2021; OECD, 2019; OECD, 2020)

Inter-agency coordination should be treated as a design problem with explicit operating rules. Coordination fails when it relies on informal relationships rather than enforceable routines. Effective models specify decision rights, data-sharing protocols, joint prioritisation, and escalation pathways. They also establish how cases move from detection to investigation to prosecution or administrative remedy, and how lessons feed back into policy and control redesign. Importantly, the legitimacy of inter-agency coordination depends on transparency about why data are shared, what safeguards exist, and how errors are corrected. This is where

https://doi.org/10.36690/PUBADM

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

performance management intersects with rights protection: a system that increases detection but produces many wrongful flags erodes trust and may increase administrative burden rather than reduce it.

Table 2.12. Inter-Agency Coordination Models for Anti-Fraud and Risk-Based Supervision

Model	How it works	Strengths	Typical risks	Fit conditions
Hub-and-spoke analytics unit	Central unit builds models, agencies act	Scale, consistent methods, shared learning	Over-centralisation, weak domain feedback	Clear mandate, strong data governance, shared priorities
Joint task forces (case-based)	Multi-agency teams for priority schemes	Fast response, high deterrence in hotspots	Not scalable, depends on personalities	High-impact schemes, strong investigative authority
Federated coordination council	Agencies align indicators and actions	Respects autonomy, improves consistency	Slow decisions, weakest-link problem	Mature agencies, stable governance rules
Platform-based data sharing	Shared services for identity, registries, data exchange	Low duplication, “once-only” reuse capability	Governance complexity, uneven capacity	Standardised interoperability, legal clarity, stewardship roles

Sources: systematized by the author based on (FATF, 2021; OECD, 2020)

From analytics to accountable action: capability building and safeguards. Analytics is valuable when it produces accountable actions. This requires a maturity model that connects techniques to governance safeguards. Rule-based systems are explainable but can be brittle. Advanced models can improve prioritisation but must be governed to prevent opaque decision-making, unfair targeting, or mission creep. Updated fraud risk management guidance explicitly recognises the role of data analytics within a broader fraud risk management programme that includes governance policies, risk assessment, controls, investigations, and monitoring (COSO & ACFE, 2023). OECD analysis similarly warns that analytics must be embedded in institutional and data governance, skills, and culture, and that benefits include non-financial public value that may not appear as immediate budget savings (OECD, 2019).

A practical implementation sequence is therefore: define typologies as mechanisms, build indicator families tied to decisions, establish data governance and inter-agency routines, then scale analytics with safeguards and evaluation.

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

Table 2.13. Anti-Fraud Analytics Maturity and Required Accountability Safeguards

Maturity level	Typical technique	Supervisory benefit	Minimum safeguards
Level 1: Rules and thresholds	Deterministic red flags	Fast triage, low cost	Documented rationale, periodic review
Level 2: Anomaly detection	Outlier and peer comparisons	Better prioritisation	Data quality controls, bias checks
Level 3: Risk scoring models	Supervised prediction	Earlier interventions	Explainability, audit trails, appeal routes
Level 4: Network analytics	Graph-based detection	Collusion and hidden links	Governance for link uncertainty, proportional escalation
Level 5: Continuous learning	Model monitoring and retraining	Adaptive deterrence	Model governance, independent validation, transparency reporting

Sources: systematized by the author based on (COSO & ACFE, 2023; OECD, 2019)

This sequence also reduces administrative burden by ensuring that controls are targeted and that verification is automated only where legal bases and data quality make automation reliable. Where those conditions do not hold, the risk-based approach should explicitly prefer lighter-touch actions and capacity building rather than premature automation.

Anti-fraud is the operational core of risk-based supervision because it links institutional mechanisms, measurable indicators, data governance, and coordinated action. Sustainable results come from mechanism-based typologies, decision-grade indicators, lawful data reuse, and enforceable inter-agency routines, not from isolated digital tools. Analytics strengthens this system when paired with clear escalation rules, transparency, and safeguards that protect fairness and reduce unnecessary burden. In this framing, anti-fraud governance becomes a capability-building agenda: it upgrades how the state learns about risk, targets oversight, and demonstrates public value through deterrence, integrity, and trusted administration.

3. Instruments and effect evaluation: compliance, data-sharing, digital traces, and supervisory KPIs. Risk-based digital supervision becomes operational only when its instrument set is explicit and when each instrument is linked to a measurable theory of change. In inspection-led regimes, instruments are dominated by routine checks and sanctions, and effectiveness is often inferred from activity volume. In risk-based regimes, instruments must be differentiated by risk tier and by behavioural intent, because the supervisory objective is not inspection maximisation but harm reduction with proportional burden. OECD guidance on enforcement and inspections stresses risk focus, proportionality, and responsive approaches in which actions are modulated by regulated entities' behaviour and risk profiles (OECD, 2014; OECD, 2018).

The table 2.14 structures the instrument portfolio as a coherent mix of preventive, detective, and corrective tools, clarifying how each tool contributes to burden reduction, detection, deterrence, and fairness.

Table 2.14. Instrument portfolio for risk-based digital supervision and anti-fraud governance

Instrument category	Primary function	Typical tools	Main effect pathway	Key fairness condition
Preventive instruments	Reduce opportunities for abuse	Clear rules, standardised procedures, digital-by-default workflows with assisted channels	Lowers error and discretion, improves compliance clarity	Accessibility and equal treatment in service access
Compliance support	Increase voluntary compliance	Guidance, nudges, targeted education, simplified reporting, pre-filling	Reduces unintentional non-compliance and rework	Non-discriminatory support for SMEs and low-capacity actors
Detective instruments	Improve risk identification	Risk scoring, anomaly detection, network analytics, thematic reviews	Increases signal detection and targeting quality	Explainable criteria and human review
Corrective instruments	Restore compliance and prevent recurrence	Remediation plans, targeted audits, corrective orders	Reduces repeat risk by fixing control failures	Proportionality and due process
Punitive instruments	Deter high-harm behaviour	Fines, licence actions, exclusions, referrals	Raises perceived and actual cost of misconduct	Consistency, appealability, transparency

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2014; Organisation for Economic Co-operation and Development, 2018)

Effective supervision relies on an instrument mix that matches risk profiles and behavioural drivers, rather than a single dominant tool.

Table 2.14 highlights a key design implication: burden reduction is not achieved by digitising sanctions, but by shifting more supervision effort into prevention and compliance support for low and medium risk segments, while reserving intensive enforcement for demonstrably high-harm cases. This logic aligns with risk-based inspection principles that aim to minimise unnecessary costs for both regulators and regulated entities while improving effectiveness where risks concentrate (OECD, 2014).

Compliance as a supervised system, not a paperwork outcome. In risk-based governance, compliance should be treated as a managed system with segmented strategies, not as a binary state verified through sporadic inspections. This framing is well developed in compliance risk management approaches used in tax administrations, where administrations identify compliance risks, assess their drivers, select tailored treatments, and monitor outcomes through an iterative risk management cycle (OECD, 2004/2012; OECD, 2021). The critical transferable lesson is methodological: supervisors should separate deliberate non-compliance from capability constraints, because the instrument response differs. For capability-driven non-compliance, simplification, assistance, and pre-filled data may reduce errors and burden while improving compliance. For deliberate fraud, deterrence and targeted investigation are required.

The Table 2.15 translates compliance risk management into supervisory practice by mapping risk drivers to treatments and expected effects.

Table 2.15. Compliance risk management logic: drivers, treatments, and expected effects

Compliance risk driver	Observable symptom	Preferred treatment type	Expected effect on burden	Expected effect on deterrence
Capability and literacy constraints	Frequent errors, incomplete filings	Assistance, simplification, pre-filling	Decreases for low-risk actors	Indirect, via fewer opportunities for abuse
Process complexity and discretion	Exceptions, inconsistent decisions	Standardisation, workflow controls, guidance	Decreases by reducing rework	Moderate, by narrowing manipulation space
Opportunity and weak controls	Duplicate payments, weak verification	Automated cross-checks, audit trails	Decreases if reuse is lawful and reliable	Increases by raising detection probability
Intentional evasion and concealment	Outliers, repeated anomalies	Targeted audits, sanctions, referrals	Increases only for targeted high-risk cases	High, if sanctions are credible and consistent
Collusion and networks	Repeated clustered behaviour	Network analytics, joint investigations	Neutral for general population	High, if disruption is visible

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2004/2012; European Commission, 2023)

Treating compliance as risk management makes supervision more proportional, because it targets high-harm behaviours while supporting low-risk actors through lower-friction pathways.

Between Table 2.15 and implementation, a practical constraint must be addressed: treatment choice depends on data maturity and legal permissions. Pre-filling and automated cross-checks require lawful data reuse and interoperable identifiers. Without them, supervisors risk substituting rigid documentation requirements for genuine burden reduction. This is why compliance modernisation and data-sharing governance are inseparable in digital supervision.

Data-sharing as legal, institutional, and technical interoperability. Data-sharing is often described as a technical integration task, yet risk-based supervision requires legal interoperability and institutional accountability for what is shared, why it is shared, and how it is safeguarded. SupTech literature emphasises that supervisory effectiveness depends on data availability and quality, and that strategies should include clear targets and assessment of data use, not only tool acquisition (Broeders & Prenio, 2018; World Bank, 2018). At the system level, data-sharing improves both effectiveness and proportionality: it enables targeted verification for high-risk cases while reducing repeated requests for low-risk actors by reusing already-held data under lawful conditions.

The Table 2.16 distinguishes common data-sharing patterns and specifies governance controls that preserve legality and trust.

Table 2.16. Data-sharing patterns and governance controls in risk-based supervision

Data-sharing pattern	What it enables	Typical risk	Minimum governance control	Supervisory value
Point-to-point exchange	Case-based verification	Inconsistent rules, weak auditability	Standard agreements, access logging	Faster targeted checks
Federated query model	Data stays with owner, queries are executed	Uneven service quality	Query governance, response standards	Lower duplication with better stewardship
Shared data hubs	Consolidated analytics datasets	Privacy and concentration risk	Purpose limits, role-based access, audits	Stronger pattern detection
Trusted registries and reference data	Reliable entity resolution	Data quality drift	Stewardship roles, quality KPIs	Fewer false positives and rework
Supervisory portals for reporting	Standardised submissions and validation	Burden shifting to reporting	Validation automation, reuse of existing data	Improved timeliness and consistency

Sources: systematized by the author based on (Broeders, D., & Prenio, J., 2018; World Bank, 2018; Financial Stability Board, 2020)

Data-sharing improves both detection and burden reduction only when legal permissions, accountability, and auditability are designed alongside technical integration.

Table 2.16 implies an evaluation discipline: supervisors should measure not only whether data-sharing exists, but whether it reduces redundant requests, improves targeting quality, and maintains lawful safeguards. If these effects are not demonstrable, data-sharing risks becoming a costly infrastructure project with ambiguous public value. This logic aligns with

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

the broader SupTech and RegTech assessment that benefits are realised when tools improve oversight capabilities and compliance outcomes, and when associated operational risks are managed (FSB, 2020).

Digital traces as supervision evidence, not merely IT logs. Digital traces are the event records produced by digital service delivery and administrative workflows, including submission timestamps, identity verification events, exception handling, approvals, and access logs. They are valuable because they enable reconstruction of processes and detection of patterns that are invisible in static documents. However, traces become supervisory evidence only if logging standards, retention rules, and integrity controls are defined. Otherwise, traces are incomplete, inconsistent, or contestable, which undermines enforcement and increases disputes. OECD work on analytics for integrity emphasises that institutions need governance, standards, and readiness to use data analytics effectively for fraud and corruption risk assessment (OECD, 2019).

The Table 2.17 classifies trace types and links them to anti-fraud and supervision use-cases, while clarifying their evidentiary requirements.

Table 2.17. Digital traces in supervision: types, uses, and evidentiary requirements

Trace type	Typical content	Supervisory use	Evidentiary requirement	Main risk if weak
Transaction traces	Payments, transfers, invoice metadata	Detect anomalies, duplicate payments	Integrity controls, reconciliation	False signals and disputes
Workflow traces	Steps, exceptions, approvals	Process mining, exception auditing	Complete event logging, timestamps	Manipulation hidden in gaps
Identity and access traces	Authentication events, role changes	Detect account compromise and misuse	Strong access controls, audit trails	Privacy breach or weak attribution
Decision traces	Rule applications, overrides, reasons	Explainability and appeal review	Reason codes, version control	Uncontestable decisions
Communication traces	Notices, responses, messages	Verify timing and due process	Retention rules, provenance	Procedural fairness questioned

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2019; World Bank, 2018)

Traces support both detection and fairness when they are complete, governed, and linked to explainable supervisory decisions.

Table 2.17 also clarifies why trace governance is a fairness issue. If risk scoring triggers interventions, regulated entities need contestable explanations and reliable audit trails, otherwise selective supervision becomes illegitimate even when it is technically effective. In contexts where

AI or advanced analytics are used, principles of transparency, robustness, security, and accountability are commonly emphasised as conditions for trustworthy systems (OECD, 2019).

KPI design: evaluating burden reduction, detection, deterrence, and fairness. KPI systems frequently fail because they measure what is easy rather than what is consequential. A digitisation-count KPI, for example number of e-services or number of checks automated, can grow while administrative burden, fraud loss, or perceived fairness do not improve. Risk-based supervision therefore requires a KPI framework that treats burden reduction, detection, deterrence, and fairness as co-equal dimensions. OECD enforcement principles support outcome-oriented thinking by emphasising risk reduction, proportionality, and consistent enforcement (OECD, 2014; OECD, 2018). SupTech assessments also stress that tools should strengthen oversight and analytical capability, not merely increase data collection (Broeders & Prenio, 2018; FSB, 2020).

The Table 2.18 defines KPI families, suggests operational measures, and notes common interpretation pitfalls.

Table 2.18. KPI framework for risk-based digital supervision and anti-fraud governance

KPI family	What success means	Example measures	Interpretation pitfall	Control against gaming
Burden reduction	Less friction for compliant actors	Steps per process, time to comply, resubmission rate	Averaging hides SME burden	Segment reporting by size and risk tier
Detection quality	Higher precision and timeliness	Hit rate, time to flag, case cycle time	Narrow targeting inflates hit rate	Combine with coverage and fairness checks
Deterrence	Behaviour changes sustainably	Repeat non-compliance, recurrence, voluntary corrections	Confounded by economic shifts	Use trends, matched comparisons where feasible
Fairness and legitimacy	Equal treatment and contestability	Appeal outcomes, consistency indices, disparate impact indicators	Fairness ignored as "soft"	Publish criteria, audit models, provide redress

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2014; Broeders, D., & Prenio, J., 2018; Financial Stability Board, 2020; Recommendation of the Council on Artificial Intelligence, 2019)

KPI credibility depends on segmentation, safeguards against gaming, and explicit fairness measurement alongside efficiency.

Between Table 2.18 and practical evaluation, an important methodological step is to connect each KPI to a plausible mechanism and to a feasible evaluation design. For example, if the intervention is data reuse to reduce repetitive submissions, then burden reduction should be measured through process steps and time-to-complete, and detection quality should be measured through verification accuracy and reduced error correction. If the intervention is network analytics to identify collusion, deterrence should be measured through reduced recurrence and network disruption indicators, while fairness should be monitored through explainability and appeal success rates. This approach aligns with integrity analytics guidance that emphasises institutional readiness, governance, and appropriate technique selection for the objective at hand (OECD, 2019).

The Table 2.19 proposes evaluation designs that match typical instrument types and risk levels.

Table 2.19. Evaluation designs matched to supervision instruments

Instrument type	Suitable evaluation design	What it can show	Data requirement	Main limitation
Compliance support and simplification	Before-after with segmentation	Burden reduction and error reduction	Process measures, user journeys	External factors may confound
Targeted audits and enforcement	Quasi-experimental comparisons	Deterrence and recurrence effects	Case histories, sanctions, recurrence	Selection bias if not adjusted
Data-sharing and cross-checks	Process and accuracy audits	Verification gains and rework reduction	Data quality and reconciliation	Benefits depend on legal and data maturity
Analytics-enabled triage	Precision and drift monitoring	Detection quality and stability	Labels, baselines, monitoring logs	Label scarcity and drift
Inter-agency coordination	Network and workflow evaluation	Case speed, handoff quality	Referral logs, cycle times	Attribution across agencies is complex

Sources: systematized by the author based on (Organisation for Economic Co-operation and Development, 2019; World Bank, 2018; Financial Stability Board, 2020)

Evaluation should be instrument-specific, because burden, deterrence, and fairness respond to different mechanisms and require different evidence.

A risk-based digital supervision regime is effective when its instruments, data-sharing arrangements, and trace governance form a coherent operational system aligned with measurable public value. Compliance is strengthened most sustainably when supervisors segment risks, combine support and deterrence proportionately, and use lawful data reuse to reduce friction for low-risk actors. Digital traces and SupTech tools improve detection and triage only when embedded in workflow and governed through auditability, explainability, and safeguards. Finally, evaluation must prioritise outcome KPIs for burden reduction, detection quality, deterrence, and fairness, because activity counts alone do not demonstrate harm reduction or legitimacy in modern supervision.

Conclusion. Across international practice, the shift from inspection-led compliance to risk-based digital supervision reflects a reorientation toward harm reduction under capacity constraints, supported by supervisory analytics and governed data use. Anti-fraud becomes the core of the risk approach because fraud is adaptive, networked, and high-impact, requiring typology-based indicators, lawful data-sharing, and structured inter-agency coordination. Digital traces and SupTech tools expand detection and targeting capacity, yet they also increase requirements for model governance, auditability, cybersecurity readiness, and fairness safeguards. Instrument design is most robust when it combines prevention, compliance support, and proportionate enforcement while explicitly protecting rights and inclusion. Evaluation is credible when it prioritises outcome KPIs aligned with burden reduction, detection, deterrence, and fairness, and when those KPIs are used for decision-making, not only for reporting. Overall, effective risk-based digital supervision is best understood as institutional capacity building that aligns law, data governance, analytics, and accountability into a coherent operational system.

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

Conflict of interest. The author 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 author 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 author 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. Broeders, D., & Prenio, J. (2018). *Innovative technology in financial supervision (SupTech): The experience of early users* (FSI Insights on policy implementation No. 9). Bank for International Settlements. https://www.bis.org/fsi/publ/insights9.pdf
2. Committee of Sponsoring Organizations of the Treadway Commission. (2023). *Fraud risk management guide* (2nd ed.). COSO. https://www.aicpa-cima.com/resources/landing/coso-fraud-risk-management-guide
3. Committee of Sponsoring Organizations of the Treadway Commission, & Association of Certified Fraud Examiners. (2023). *Fraud risk management guide* (2nd ed.): Executive summary. COSO & ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/fraud-risk-management-guide-executive-summary.ashx

4. Dolowitz, D. P., & Marsh, D. (2000). Learning from abroad: The role of policy transfer in contemporary policy-making. *Governance, 13*(1), 5-24. https://doi.org/10.1111/0952-1895.00121
5. European Commission, Directorate-General for Taxation and Customs Union. (2023). *Compliance risk management in the digital era* (CRM Guide). https://taxation-customs.ec.europa.eu/system/files/2024-01/2023_CRM_Guide.pdf
6. Financial Action Task Force. (2012). *International standards on combating money laundering and the financing of terrorism and proliferation: The FATF Recommendations* (Updated October 2025). FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.pdf
7. Financial Action Task Force. (2021). *Guidance on risk-based supervision*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Risk-Based-Supervision.pdf.coredownload.pdf
8. Financial Stability Board. (2020). *The use of supervisory and regulatory technology by authorities and regulated institutions: Market developments and financial stability implications*. https://www.fsb.org/uploads/P091020.pdf
9. International Monetary Fund. (2025). *AI projects in financial supervisory authorities* (IMF Working Paper No. WP/25/199). https://doi.org/10.5089/9798229025263.001
10. Organisation for Economic Co-operation and Development. (2014). *Regulatory enforcement and inspections: OECD best practice principles for regulatory policy*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/11/regulatory-enforcement-and-inspections_9f73c9ea/fc8bbb87-en.pdf
11. Organisation for Economic Co-operation and Development. (2014). *Recommendation of the Council on digital government strategies* (OECD-LEGAL-0406). OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406
12. Organisation for Economic Co-operation and Development. (2018). *OECD regulatory enforcement and inspections toolkit*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/10/oecd-regulatory-enforcement-and-inspections-toolkit_83d60f55/9789264303959-en.pdf
13. Organisation for Economic Co-operation and Development. (2019). *Analytics for integrity: Data-driven approaches for enhancing corruption and fraud risk assessments*. OECD Publishing. https://doi.org/10.1787/b354a27e-en
14. Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on artificial intelligence* (OECD/LEGAL/0449). OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
15. Organisation for Economic Co-operation and Development. (2020). *OECD public integrity handbook*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/05/oecd-public-integrity-handbook_598692a5/ac8ed8e8-en.pdf

16. Organisation for Economic Co-operation and Development. (2021). *Managing and improving tax compliance*. OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/09/managing-and-improving-tax-compliance_4d5f9c4c/12f8f563-en.pdf
17. Organisation for Economic Co-operation and Development. (2025). *OECD regulatory policy outlook 2025*. OECD Publishing. https://doi.org/10.1787/56b60e39-en
18. Organisation for Economic Co-operation and Development. (2025). *Tax administration 2025: Comparative information on OECD and other advanced and emerging economies*. OECD Publishing. https://doi.org/10.1787/cc015ce8-en
19. 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/
20. Peck, J., & Theodore, N. (2010). Mobilizing policy: Models, methods, and mutations. *Geoforum, 41*(2), 169-174. https://doi.org/10.1016/j.geoforum.2010.01.002
21. Toronto Centre. (2018). *SupTech: Leveraging technology for better supervision*. https://stage.torontocentre.org/media/acfupload/SupTech_Leveraging_Technology_for_Better_Supervision_Updated_Link_copy_1.pdf
22. United Nations Department of Economic and Social Affairs. (2024). *United Nations e-government survey 2024: Accelerating digital transformation for sustainable development*. UN DESA. https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf
23. United Nations Department of Economic and Social Affairs. (2024). *Addendum on AI and digital government: An addendum to the 2024 UN e-government survey*. UN DESA. https://desapublications.un.org/sites/default/files/publications/2024-10/Addendum%20on%20AI%20and%20Digital%20Government%20%20E-Government%20Survey%202024.pdf
24. World Bank. (2018). *From spreadsheets to SupTech: Technology solutions for market conduct supervision* (Discussion note, June 2018). https://documents1.worldbank.org/curated/en/612021529953613035/pdf/127577-REVISED-Suptech-Technology-Solutions-for-Market-Conduct-Supervision.pdf
25. World Bank Group. (2019). *Warning signs of fraud and corruption in procurement*. https://documents1.worldbank.org/curated/en/223241573576857116/pdf/Warning-Signs-of-Fraud-and-Corruption-in-Procurement.pdf

https://doi.org/10.36690/PUBADM

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

Section 2.2. Public Administration of the Digitalization of Accounting and Reporting in Ukraine

Vira Shepeliuk[1]

[1]Ph.D. in Economics, Associate Professor, Associate Professor of the Department of Marketing, Accounting, Taxation and Public Administration, Kryvyi Rih National University, Kryvyi Rih, Ukraine, ORCID: https://orcid.org/0000-0001-6270-5936

Citation:
Shepeliuk, V. (2025). Public Administration of the Digitalization of Accounting and Reporting in Ukraine. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 102-131). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-102-131

Abstract. *The study examines how public administration shapes the digitalization of accounting and reporting in Ukraine under the dual pressure of global digital transformation and martial law. The introduction outlines digitalization as both a technological and institutional shift that reconfigures the interaction between the state, business and citizens through platforms such as Diia, ERP and BAS systems, and digital reporting. The objective is to conceptualize digital accounting in Ukraine as a public governance tool, to assess its impact on the quality of financial information and economic resilience, and to identify conditions for integrating national practices into the European digital space. Methodologically, the study applies a systems approach that combines theoretical generalization of four conceptual views of the digital economy, comparative analysis of EU, US and Chinese digital strategies, and an empirical assessment of Ukraine's digital transformation in 2020–2025 based on official statistics and international reports. The main results show that digital tools such as BAS ERP, Diia, electronic document management, fintech solutions and Inline XBRL form a new architecture of accounting that improves timeliness, transparency and accessibility of data, while simultaneously generating risks related to cybersecurity, human capital and regulatory instability. The role of the accountant shifts from a record keeper to a system integrator who operates at the intersection of finance, information technology and law, and whose competencies become a critical factor for the effectiveness of public digital policies. The conclusions emphasize that accounting digitalization in Ukraine has a dual effect, creating opportunities for deeper integration into global financial markets and for enhancing economic security, but also exposing structural weaknesses in education and regulation. Directions for further research include the development of governance models that align digital infrastructure, regulatory standards and professional training, as well as quantitative assessment of how specific digital tools affect accounting quality and trust in public reporting at micro and macro levels.*

Keywords: *digital accounting; ERP systems; BAS ERP; Diia ecosystem; Inline XBRL; accounting quality; public administration; digital transformation; economic security; fintech; cybersecurity; Ukraine.*

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

1. Digitalisation of Accounting in the Context of the Global Economy and Martial Law in Ukraine. The contemporary stage of economic development is characterised by the global digitalisation of business processes, which necessitates the transformation of traditional approaches to accounting and taxation. The use of information and communication technologies, cloud services and enterprise resource planning systems, in particular ERP solutions such as BAS, is gradually becoming the standard mode of operation for enterprises, as it enables timeliness, transparency and automation of accounting and analytical processes. At the same time, the implementation of such technologies is accompanied by heightened risks related to information security, data quality and regulatory compliance.

Under martial law in Ukraine, these challenges acquire particular urgency. Enterprises face not only financial instability and resource constraints, but also the need to ensure the continuity of accounting processes in the context of cyber threats, disruptions in energy supply and telecommunications infrastructure. The demand for cloud technologies and online reporting is growing, since they provide mobility and data accessibility, yet they simultaneously impose new requirements for cyber resilience and risk management.

There is therefore an objective need to study the specific features of the digitalisation of enterprises' accounting and analytical activities, to determine its impact on management effectiveness and to develop proposals for strengthening information security under conditions of crisis-driven change and global challenges.

The digitalisation of the economy is a key driver of contemporary economic development that integrates information technologies into all spheres of social life. The digital economy is commonly understood as the aggregate of economic relations that function on the basis of information and communication technologies, digital platforms and data as a strategic resource. According to Borblik (2022), it encompasses infrastructure, digital skills, the legal framework, business readiness and the degree of integration into global markets (Borblik, 2022). The OECD (2024) emphasises that the digitalisation of the economy is not only the automation of processes, but also a strategic instrument for enhancing competitiveness, innovativeness and resilience to crises (OECD, 2024).

Contemporary scholars generally distinguish four main approaches to conceptualising the digital economy, namely systems, process, functional and spatio-temporal approaches. Each of these attracts both supporters and critics, which shapes a broad academic debate.

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

Proponents of the systems approach view digitalisation as a complex of interrelated elements that include technologies, institutions, human capital and the legal environment. For example, Vasyltsiv (2022), in the article "Factors of the Development of Ukraine's Digital Economy", identifies six components, including strategy, expertise, readiness and inclusion, which jointly form the digital economy index of Ukraine. Borblik, in the work "Digitalization of the Ukrainian Economy" (2022), also uses a systems perspective, comparing international rankings of digital infrastructure readiness, the level of digital literacy of the population and the legal environment in Ukraine with those in other countries. Dyachenko (2022), however, criticises the systems approach in strategic documents, arguing that it is overly general and detached from real economic relations. Moreover, in Ukraine indicators of "readiness" and "infrastructure" may be relatively high, while in practice there are significant disparities across regions or levels of IT competence. The systems approach sometimes fails to capture these internal asymmetries (Vasyltsiv, 2022).

The process approach focuses on the fact that digitalisation is not a one-off phenomenon, but a gradual transformation of organisational and business processes, management practices and employee roles. In particular, the article "A processual approach to skill changes in digital automation: The case of the platform economy in the service sector" (Xing and Sharif, 2025) examines how automation and digitalisation change competencies in the service sphere and platform-based businesses, that is, how skills evolve over time and at different stages of digitalisation. At the same time, scholars raise the question of whether the process approach offers clear assessment methods and indicators of progress, or merely descriptive accounts of change. Without quantitative metrics it is difficult to compare or measure results. Many organisations remain "stuck" at a certain stage where digitalisation is partial and not embedded in the culture of change. The process approach may overlook stagnation or regress if resources or motivation decline. Consequently, there is a need to expand workers' digital skills in order to improve the assessment and optimisation of business processes.

The functional approach isolates specific digital functions or tools as key elements, such as electronic services, online payments, automated analytical systems and cloud technologies. For instance, in the study "Analysis of digital technologies in Ukraine: problems and prospects" Yurchyshyn, Stepanets and Skorobogatova (2024) note that process automation, market forecasting and asset monitoring are functional capabilities already being implemented in business and that they generate tangible effects. The work "European Integration and Globalisation of Ukraine's Digital Transformation" (Shashyna, 2024) also stresses that access to digital functions of public services, regulatory platforms and business tools is crucial for integration with the European Union. Thus, the functional approach appears highly practical; however, there is a risk that a narrow focus on tools and functions diverts attention from broader structural or institutional transformations. Several authors, including Dyachenko (2022), indicate that Ukrainian strategy documents often describe functions without sufficient attention to production and social relations, changes in labour relations, legal issues or the institutional framework.

The spatio-temporal approach considers digitalisation not only as a technological or business change, but as a set of transformations that depend on space (regions, urban versus rural areas, high-risk zones) and time (periods of crisis, war, pandemics). For example, Verbivska (2023), in the work "Digitalization of the Ukrainian economy during a …", analyses how digital services in rural regions face specific challenges of access and digital literacy, and demonstrates that their development lags behind that of urban centres. Shcherban et al. (2025), in the study "Assessment of the Digital Transformation of Ukraine's Economy", also focus on regional disparities in access to digital infrastructure, business readiness and cybersecurity. At the same time, there are scholarly debates regarding the extent to which spatial conditions, such as region or the urban–rural divide, are decisive, or whether such differences are primarily a matter of resource distribution rather than geography as such. Researchers also note that the temporal dimension, particularly crisis phenomena such as war or a pandemic, frequently reshapes digitalisation priorities by shifting attention to accessibility, security and resilience. Strategic plans, however, often fail to take these temporal aspects sufficiently into account.

Below, Table 2.20 presents the advantages and disadvantages of each approach to interpreting the concept of the digital economy.

Thus, none of the approaches, whether systems, process, functional or spatio temporal, provides a comprehensive understanding of digitalisation when taken in isolation. An effective theory and practice of the digital economy should combine elements of each approach: systemic thinking for strategy and institutions, a process perspective for changes over time, a functional focus for practical applications and a spatio temporal lens for taking context into account.

Table 2.20. Advantages and disadvantages of different approaches to interpreting the concept of the digital economy

Approach	Authors / examples	Advantages	Disadvantages	Impact on development
Systemic	Vasyltsiv (2022); Borblik (2022)	Comprehensive, strategic	Excessive abstraction, weak practicality (Dyachenko, 2022)	Forms a holistic vision of the digital economy
Process	Xing & Sharif (2025)	Shows dynamics and adaptability	Lack of clear metrics	Explains the continuity of change, the role of human resources
Functional	Yurchyshyn et al. (2024); Shashyna (2024)	Practical orientation, quick effect	Ignores institutional context	Gives businesses specific tools
Spatiotemporal	Verbivska (2023); Shcherban et al. (2025)	Consider context and crises	Difficult to measure	Explains the digital divide and crisis dynamics

Sources: systematized by the author

Strategies and theories that rely predominantly on the systems approach often note that without an adequate legal environment, norms and standards, the digital economy can remain at the level of functional solutions without delivering meaningful effects for institutions or society. Empirical studies on Ukraine show that spatial and temporal variability, including regional disparities and the war, significantly modifies the effectiveness of digital approaches. A theoretical model must therefore account for context: what works in Kyiv may not work in a village or in a region whose infrastructure has been destroyed.

Consequently, digitalisation is a multifaceted process that cannot be adequately explained within a single conceptual framework. The systems approach provides a strategic vision but requires further specification. The process approach reflects the dynamics of change but lacks robust quantitative indicators. The functional approach is oriented towards practice, yet risks ignoring social and legal dimensions. The spatio temporal approach offers an understanding of context but remains difficult to operationalise and integrate into public policy.

2. International Experience of Economic Digitalisation: Comparative Lessons from the EU, the USA and China. International experience in the European Union, the United States and China demonstrates different trajectories of economic digitalisation. For example, in the European Union digital transformation is viewed as a key driver of competitiveness and social inclusion. The Digital Decade 2030 programme defines four pillars:

1. digital skills of the population
2. secure and resilient infrastructure
3. digital transformation of business
4. digitalisation of public services (European Commission, 2022).

Shashyna (2024) stresses that, for Ukraine, integration into the European digital space implies not only access to the single market, but also the need to harmonise the legal framework, from data protection to standards of electronic reporting. This provides an important benchmark for the country, while at the same time creating challenges in terms of resources and cybersecurity. Even within the European Union, however, there are substantial gaps between the countries of “old” and “new” Europe (Verbivska, 2023). A strength of the European approach is its institutional character: digital strategies are codified in official documents and supported by funding and control mechanisms. Its weakness lies in the high financial costs, which may be excessive for Ukraine under conditions of martial law. Digital integration therefore does not guarantee uniform progress, and Ukraine needs to take this experience into account in order to avoid internal digital inequality.

In the United States the digital economy has been driven primarily by private sector innovation and global IT corporations such as Google, Amazon, Meta and Microsoft. The main drivers include the development of cloud computing, artificial intelligence and machine learning, fintech and blockchain solutions, and the expansion of the gig economy through platforms like Uber, Upwork and Airbnb. In the United States the digital sector accounts for more than 10 percent of GDP and generates jobs with a high level of added value. However, scholarly works, including Xing and Sharif (2025), draw attention to social risks such as unequal access to digital benefits, employment instability in the platform economy and the need to regulate Big Tech. For Ukraine this model is of interest in terms of support for small and medium sized enterprises, which can become the principal carriers of innovation. Marchuk (2024) emphasises that the digitalisation of accounting in Ukrainian enterprises already contributes to enhanced competitiveness. In the Ukrainian context, however, copying the American model without social compensatory mechanisms risks deepening inequality and weakening social cohesion. It is therefore important for Ukraine to combine innovativeness with social responsibility by creating a legal environment that stimulates start-ups while simultaneously protecting workers.

The experience of China represents a different model, in which digitalisation is integrated into public administration and industrial policy.

The strategy Made in China 2025 and the digital economy development programme focus on large scale digital infrastructure, including 5G networks, big data centres and artificial intelligence, the integration of digital technologies into production in line with Industry 4.0 principles, state control over platforms and data flows, and the export of digital technologies as an element of geopolitics through the Digital Silk Road. Contemporary scholars note that digitalisation in China raises productivity and supports the rapid expansion of the fintech sector, but is accompanied by strengthened state control over data and restrictions on competition. Western researchers, including the OECD (2024), criticise the Chinese model for the risks of digital authoritarianism, whereby technologies are used for monitoring citizens. For Ukraine this experience may be of interest in terms of large scale infrastructure development, such as 5G networks, data centres and artificial intelligence systems for industry. At the same time, the Chinese model entails risks associated with extensive state control over data and limitations on competition. For a democratic Ukraine this aspect is unacceptable, although the positive elements, particularly large scale investment in digital technologies, could be adapted through international partnerships.

The experience of digital transformation in the European Union, the United States and China serves as a reference point for Ukraine, which is simultaneously integrating into the European space and confronting the challenges of war. According to Shashyna (2024), digitalisation is one of the key components of European integration, since the harmonisation of standards in the fields of data protection, electronic reporting and cybersecurity is a prerequisite for Ukraine's entry into the EU single digital market. In this context the international models are not mutually exclusive; elements of each can be selectively adapted to Ukrainian conditions.

Thus, the development of the digital economy requires an integrated approach that combines the strategic vision of the systems perspective, the dynamism of the process perspective, the applied focus of the functional perspective and the contextual sensitivity of the spatio temporal perspective. It is precisely their synergy that makes it possible to ensure the effectiveness of digital transformations and to avoid oversimplification in both scholarly and practical interpretations. In Ukraine, where digitalisation has become a strategic priority even during wartime, the integration of these approaches is essential for turning the digital economy into a factor of sustainable development.

3. Digital Transformation of Ukraine's Economy in 2020–2025: Public Services, Fintech and Business Adaptation. In Ukrainian academic discourse (Benko and Sopko, 2020; Marchuk, 2024) digitalisation is interpreted not only as a technological trend, but also as an institutional change that encompasses the legal framework, the financial system and managerial culture. This perspective makes it possible to conceptualise digitalisation as a complex process with both economic and socio political dimensions.

In the period 2020 to 2025 Ukraine has demonstrated significant progress in digital transformation (Table 2.21).

Table 2.21. State of the digitalisation of Ukraine's economy (2020–2025)

Indicators	2020	2022	2025
Share of enterprises using ERP/BAS systems	18%	25%	40%
Share of SMEs using only basic digital tools	62%	55%	45%
Mobile Internet penetration rate (4G/5G)	72%	82%	92%
Number of Diia users (million)	9,0	14,2	20,0+
Number of cyberattacks on the public sector (thousands)	1,2	2,8	3,5+

Sources: systematized by the author based on (OECD, 2024; Shcherban et al., 2025; ArXiv, 2025)

One of Ukraine's most important achievements in 2020–2025 has been the creation and development of the digital platform "Diia." This project of the Ministry of Digital Transformation has become a symbol of the integration of public services into the digital space. In 2020, Diia was launched as a mobile application providing access to digital documents, including the passport, driving licence and student card. In 2021–2022, more than seventy public services were added to the ecosystem, such as business registration, submission of tax declarations, payment of taxes and the administration of assistance for internally displaced persons. In 2023–2025, Diia evolved from a platform for public services into an instrument of social support during the war, enabling applications for cash assistance, access to compensation for destroyed housing and the issuance of certificates under wartime conditions (Wikipedia, 2023). Scholars (Shcherban et al., 2025) emphasise that Diia is a unique example of rapid digitalisation under crisis conditions. While most countries spend decades building systems of e government, Ukraine has managed within five years to construct an inclusive and flexible system.

A second direction of digital transformation has been the spread of electronic document management. In the public sector, since 2020 a mandatory transition to electronic document exchange between ministries and agencies has been implemented. This has made it possible to reduce paper-based document flows by 80 percent and to accelerate internal procedures. In the business sector, the introduction of electronic document management is occurring gradually. According to OECD (2024), as of 2023 more than 45 percent of medium and large enterprises used electronic systems for the management of contracts, invoices and tax documents. For small and medium-sized enterprises the process is more complex. Although affordable cloud solutions are available, low levels of digital literacy and insufficient funding remain significant barriers. Marchuk (2024) stresses that digital document management has a positive impact on the competitiveness of enterprises, as it reduces costs, accelerates capital turnover and enhances the transparency of financial information.

Financial technologies have become one of the most dynamic segments of Ukraine's digital economy. The banking sector is widely implementing mobile applications, online banking and instant payment systems. According to the National Bank of Ukraine, in 2023 more than 70 percent of retail transactions were carried out in non-cash form. Ukrainian companies such as Monobank and Privat24 have become examples of successful fintech solutions that are comparable with their Western counterparts. The segment of digital signatures and electronic identification is also developing, including integration with the BankID system. This is particularly important for accounting, taxation and auditing, where the authenticity and security of data are of critical significance. Scholars such as Saeed et al. (2023) note that fintech, in combination with digital government, creates a new level of transparency and convenience for citizens, while at the same time generating new risks of cybercrime.

Another major achievement has been the creation of the platform "Diia. Digital Education," which has been offering free courses on digital literacy since 2020. By 2024 more than 1.5 million Ukrainians had completed training, which has become an important factor in the development of digital skills in society. Particular attention has been paid to the training of accountants, civil servants and educators who must adapt to new digital tools. In his scholarly work, Vasyltsiv (2022) notes that human resource readiness is what largely determines the speed and quality of digital transformation. Even the most advanced technologies will not produce the desired effect without qualified specialists.

Small and medium-sized enterprises constitute the most vulnerable but also the most promising category in Ukraine's digital economy. According to OECD (2024), only about 40 percent of small enterprises actively use ERP or BAS systems, while the majority rely on basic tools such as Excel and email. The main barriers include low levels of digital literacy, a lack of resources to invest in information technologies and limited access to high quality internet in many regions. At the same time, the experience of 2022–2025 shows that those SMEs that have succeeded in migrating to digital platforms have adapted more rapidly to wartime conditions and preserved their competitiveness.

The full-scale war in Ukraine since 2022 has radically changed the conditions under which the digital economy operates. On the one hand, the war has stimulated the development of digital services, since many businesses and public institutions have been forced to transition to remote work models. On the other hand, new challenges have emerged, including cyber threats, the destruction of infrastructure and disruptions to electricity and internet connectivity. The report "The Impact of the Russia-Ukraine Conflict on the Cloud Computing Risk Landscape" (2025) stresses that the war has heightened attention to data sovereignty and information security requirements. Ukrainian enterprises have had to allocate greater resources to the protection of information systems, which increases costs but simultaneously fosters a culture of cyber resilience (ArXiv, 2025).

The Government of Ukraine is actively supporting digital infrastructure by creating alternative communication channels and backup systems. During the war, the Diia programme has become not only a service platform, but also an instrument for providing social and financial assistance. This confirms the conclusion of Shcherban et al. (2025) that digitalisation is not merely an economic phenomenon, but also a strategic factor in national security.

Thus, in 2020–2025 Ukraine has made substantial progress in the field of digital transformation, as evidenced by both public initiatives and business activity. A key step has been the creation of the Diia ecosystem, which has evolved into a platform for e government and social support for citizens. The introduction of electronic document management in the public and private sectors has reduced transaction costs and contributed to greater transparency in economic processes. The development of the fintech sector, particularly mobile banking and digital signatures, has positioned Ukraine among the regional leaders in financial innovation. At the same time, the expansion of digital education has played a crucial role. The platform "Diia. Digital Education" has supported the dissemination of basic digital skills among the population and the training of personnel for the digital economy. Small and medium-sized businesses have begun gradually to integrate ERP or BAS systems and cloud technologies, which enhances competitiveness in both domestic and external markets.

Nevertheless, the current state of digitalisation in Ukraine is not free from challenges. Regional disparities, insufficient levels of digital literacy and limited financial resources remain serious barriers. War has become an additional factor. It has complicated the functioning of digital systems through cyberattacks and energy disruptions, while at the same time stimulating the search for innovative solutions such as satellite internet, cloud data centres and strengthened cyber defences.

Digitalisation of Ukraine's economy is therefore a process of a dual nature. On the one hand it acts as an accelerator of innovation and European integration, while on the other hand it is a source of new risks and social challenges. Future success will depend on the ability of the state and business to integrate international best practices, strengthen digital infrastructure and ensure inclusiveness so that the digital economy becomes a catalyst for sustainable development even under crisis conditions.

The identified trends in the digitalisation of Ukraine's economy show that digital transformation extends beyond public administration and the financial sector and is gradually encompassing all spheres of social life. The issue of the digitalisation of accounting and taxation is becoming particularly salient, since these processes provide the basis for managerial decision making, ensure the transparency of the business environment and enhance trust in financial information. While the macroeconomic level of digitalisation determines the conditions of functioning, the accounting level represents its practical realisation in the daily activities of enterprises. For this reason, further scholarly analysis will focus on the theoretical and practical foundations of accounting digitalisation, the assessment of its impact on the quality of financial reporting and the identification of opportunities to improve information systems under martial law and in the face of global challenges.

4. International ERP Practices and the Integrated Model of Digital Accounting for Ukraine. Contemporary economic realities require a profound transformation of the accounting system driven by digitalisation, the automation of business processes and global integration into the digital environment. The introduction of innovative accounting solutions, in particular cloud services and corporate information systems, has become especially relevant, since these systems ensure efficiency, flexibility and transparency of management processes in enterprises of different ownership forms and scales.

Digital technologies are changing the very nature of accounting, transforming it from a routine procedure into an integrated component of the digital business model. One of the main vectors of this transformation is the use of cloud technologies, digital reporting under IFRS, including in the Inline XBRL format, as well as software solutions based on the BAS platform. Under martial law in Ukraine these tools acquire particular significance for maintaining the continuity of accounting processes, ensuring the transparency of financial information and strengthening economic security.

The development of accounting has always been associated with the application of new technologies to improve the accuracy and speed of information processing. If in the twentieth century the automation of accounting was limited to the use of computing equipment and software for basic calculations, then at the beginning of the twenty first century a profound transformation took place, and accounting became an integral part of information systems and technologies in enterprise management and taxation (Marchuk, 2024).

The first stage can be considered the transition from manual bookkeeping to computerised accounting software. The next step was the introduction of corporate information systems, including ERP and BAS, which ensured the integration of accounting data with production, logistics and financial processes. At the current stage, digital accounting is viewed as a comprehensive data management system that includes cloud technologies, big data analytics, artificial intelligence and automated reporting (Saeed et al., 2023).

In the academic literature the concept of digital accounting is interpreted in different ways, which reflects the multidimensional nature of its essence. Vasyltsiv (2022) defines digital accounting as the integration of accounting processes into the digital environment of an enterprise’s information systems and emphasises the importance of technological infrastructure. Marchuk (2024) highlights a paradigmatic shift in financial reporting, arguing that digital accounting generates transparent and accessible information in real time that supports timely managerial decision making. International studies use the term cloud accounting, which stresses the use of cloud technologies for the storage and processing of accounting information and strengthens its mobility and continuity (OECD, 2024).

The essence of digital accounting lies in its systemic character, namely the capacity to integrate accounting, taxation, auditing and management analysis within a single digital environment. It is not merely the automation of operations or the technical modernisation of procedures, but a qualitatively new level of organisation of financial and economic information in which data become a strategic resource. It is precisely the systems approach that makes it possible to conceptualise digital accounting as an ecosystem combining technologies, such as ERP and BAS, XBRL and blockchain, institutional mechanisms, including IFRS standards and tax legislation, and human capital, in particular the accountant analyst as user and interpreter of data.

Summarising the results of recent studies (Vasyltsiv, 2022; Marchuk, 2024; OECD, 2024) and drawing on the systems approach to the organisation of accounting processes, we propose the following interpretation, which reflects the novelty and practical significance of the category. Digital accounting is an integrated accounting and analytical system that operates on the basis of information technologies and ensures the comprehensive integration of financial, tax and management processes in a digital environment. Its essence lies not only in the automation of operations, but in the formation of a dynamic ecosystem for managing economic information that can guarantee the transparency, reliability and relevance of financial data in real time, thereby increasing the competitiveness and economic security of enterprises.

Thus, digital accounting is not simply a set of technical tools, but a system with integration potential that combines technologies, such as ERP and BAS, XBRL and blockchain, institutional mechanisms, including IFRS and tax legislation, and human capital in the form of the accountant analyst. This determines both its theoretical and practical novelty.

The use of modern information systems and technologies is a key factor in enhancing the competitiveness and economic security of enterprises. ERP systems have become a crucial instrument for implementing the concept of digital accounting. They provide for the integration of financial, tax, production and management accounting within a unified digital environment. In this context they embody the essence of the systems approach to digital accounting, since they link bookkeeping operations with management analytics, planning and control (OECD, 2024).

BAS systems, which are the successor to the 1C:Enterprise platform and have been adapted for the Ukrainian market, have become particularly widespread. They make it possible to maintain financial and tax accounting in accordance with Ukrainian legislation and to integrate with electronic document management and online reporting to tax authorities (Marchuk, 2024).

In Ukraine ERP and BAS systems perform the role of the core of business information systems. For example, small enterprises mainly use

BAS Accounting, which automates basic functions such as the accounting of assets, payroll and tax invoices. Medium sized businesses employ comprehensive BAS ERP solutions to manage finance, procurement and inventory, integrated with financial accounting. Large corporations and holdings often implement international ERP systems such as SAP or Oracle NetSuite, while local BAS modules remain relevant for tax and financial reporting because they better reflect Ukrainian legislation. In the public sector, BAS Budgeting was actively introduced in 2021–2024 to automate the budgeting process, control expenditures and generate electronic reports.

In international practice, ERP solutions function not only as technical instruments of automation, but also as the architecture of digital accounting that defines standards for integrating financial, production and management processes. Their role extends beyond accounting departments and forms the basis for strategic management and business transparency.

SAP S/4HANA, developed in Germany and widely used in the European Union, is a classic example of a European ERP model oriented towards large corporations. It provides comprehensive integration of financial, logistics and production accounting and supports international financial reporting standards, including IFRS and the Inline XBRL technology. A study by Gartner (2023) shows that more than 70 percent of Fortune 500 companies use SAP, which confirms its global status as a standard of corporate accounting. In the EU, the introduction of SAP often coincides with stringent reporting and regulatory control requirements, which makes it not only a business solution, but also an element of economic institutionalisation.

Oracle NetSuite, originating in the United States, represents a different, predominantly cloud based approach. The system is oriented towards global business and provides scalability, which is particularly valuable for companies that grow rapidly or operate in multiple jurisdictions. According to McKinsey (2023), NetSuite has become a basic tool for start ups in e commerce and fintech. One example is Shopify, which has integrated Oracle NetSuite to manage its global operations and tax obligations in different countries.

Microsoft Dynamics 365 is characterised by its versatility and focus on medium sized enterprises. A distinctive feature of this system is the integration of financial and management accounting with customer relationship management and business intelligence, which enables simultaneous control over financial indicators and customer relations. In practice this is important for companies in trade and services. For instance, Deloitte (2024) notes that retail companies in the United Kingdom use

Dynamics 365 to manage supply chains and forecast sales based on accounting data.

BAS ERP, used in Ukraine and other post-Soviet countries, is a localized solution that takes account of national legislation. Its competitive advantage lies in its adaptation to financial and tax accounting in transition economies. Academic research by Marchuk (2024) shows that BAS ERP remains optimal for small and medium sized businesses, since it combines the functions of a classical ERP system with an affordable price and relative ease of implementation. At the same time, critics point out that the limited analytical capabilities of BAS reduce its competitiveness in comparison with global analogues.

Generalising international practice, it should be emphasised that global ERP solutions, such as SAP, Oracle and Microsoft systems, establish worldwide standards of digital accounting and are oriented towards integration with global financial markets, whereas local solutions like BAS ERP ensure adaptation to the specifics of national markets.

The OECD (2024) notes that the current trend is a shift towards cloud-based ERP systems that ensure the continuity of business processes under crisis conditions, reduce infrastructure costs and open access to new analytical tools.

Table 2.22. Advantages and disadvantages of ERP and BAS systems

System	Distribution	Advantages	Disadvantages	Usage in Ukraine
SAP S/4HANA	EU, Global	Powerful analytics, support for IFRS, XBRL	High cost, complexity of implementation	Large corporations with foreign capital
Oracle NetSuite	US, Global	Cloud, scalability	High dependency on provider	IT companies, export-oriented business
Microsoft Dynamics 365	Global	Integration with CRM, BI	Cost, need for specialists	Medium business, retail
BAS ERP	Ukraine, CIS	Localization for legislation, accessibility	Less flexibility, limited analytics	SMEs, public sector

Sources: systematized by the author

An analysis of international practice shows that ERP systems shape the global architecture of digital accounting, while the specifics of their use differ substantially depending on the economic and institutional context. The European model, represented by SAP S/4HANA, focuses on harmonisation with IFRS standards and ensures high quality financial information for regulators and investors. The American model, exemplified by Oracle NetSuite and Microsoft Dynamics 365, is oriented towards innovativeness, scalability and integration with analytical and customer relationship systems. The Chinese approach, in which ERP forms part of state digital strategies, provides scale and control, but at the same time constrains business flexibility.

For Ukraine, where local BAS solutions coexist with international ERP platforms, it is important to build an integrated model. Its essence lies in combining

- global standards, including IFRS, Inline XBRL and cloud services, which facilitate integration with international markets
- localised tools, such as BAS ERP, which take account of tax legislation and remain accessible for small and medium sized enterprises
- analytical modules, including business intelligence and big data, which enhance the quality of managerial decision making.

Under wartime conditions ERP and BAS systems also perform a function of ensuring economic security. Centralised data storage, the use of cloud technologies and integration with government services such as Diia and e Reporting create conditions for the continuity of business processes even in crisis situations.

Thus, international experience with ERP systems has a dual significance for Ukraine. On the one hand, it serves as a source for adapting best practice, and on the other hand, as a catalyst for the development of domestic solutions that combine global integration with local relevance. In this context ERP and BAS should be viewed not only as technical tools, but as the strategic foundation of digital accounting, which will determine its future quality, transparency and competitiveness.

Prospects for development lie in the gradual transition to cloud based ERP solutions, harmonisation with IFRS and the strengthening of cybersecurity. This will make it possible to integrate Ukrainian business into the global digital space while preserving national specificities of accounting and taxation.

Traditionally the role of the accountant was limited to recording economic transactions, maintaining records of assets and liabilities and preparing reports for internal and external users. Digitalisation, however, is radically changing this paradigm. According to Marchuk (2024), the contemporary accountant can no longer perform only mechanical functions, since digital information systems automate routine tasks and free time for analytical work. In this context the accountant is gradually transforming into a financial analyst and strategic business partner. The academic literature identifies several approaches to conceptualising the role of the accountant under conditions of digitalisation.

Recent studies show that digitalisation has changed traditional views of the accounting profession, and scholarly debate now focuses on finding an optimal model for its development. The literature distinguishes several approaches that explain the role of the accountant in the context of digital transformation.

The technological approach to defining the role of the accountant is based on the assumption that the main function of the accountant is to interact with information systems and to control data reliability. Proponents of this approach (Saeed et al., 2023) argue that digital tools such as ERP and BAS, XBRL and cloud platforms automate most routine tasks, leaving the accountant with the role of system supervisor. Critics, however, point out that this approach narrows the profession excessively by reducing it to the function of a technical operator.

According to Vasyltsiv (2022), digitalisation expands the possibilities of the accountant by transforming the accountant from a registrar of economic transactions into an analyst who creates management information for strategic decisions. The analytical approach assumes that the accountant performs the function of translating data into knowledge, while ERP systems become the main source of objective information. The strength of this approach lies in its emphasis on the accountant's role in strategic management. At the same time, it risks neglecting the institutional dimension, including regulatory, tax and security aspects.

In more recent research scholars emphasise that the systems approach, as developed for example by Shcherban et al. (2025), views the accountant as an element of the enterprise's digital ecosystem operating at the intersection of financial, technological and managerial domains. The accountant does not only record and analyse data, but is also responsible for their security, legal compliance and integration into business processes. This broadens the scope of the profession and attributes to it the characteristics of a digital integrator and risk manager.

In our view, it is precisely the systems approach that most fully reflects the essence of the modern role of the accountant. Unlike the technological approach, which focuses only on work with software, and the analytical approach, which highlights the function of generating management information, the systems approach makes it possible to conceptualise the accountant as an integration hub in the digital economy.

Consequently, the contemporary accountant performs the following key functions:

- informational, involving the management of accounting and analytical data in ERP and BAS systems and their transformation into reports and forecasts
- regulatory, involving the assurance of compliance with IFRS standards, tax legislation and cybersecurity requirements
- strategic, involving participation in the formation of the enterprise's financial policy, risk assessment and support for managerial decisions
- integrative, involving the combination of economic, technological and legal components within the enterprise's digital ecosystem.

The role of the accountant in the digital economy therefore cannot be explained solely by the technological or analytical approach. It must be interpreted in systemic terms that reflect the complexity of the accountant's tasks. The contemporary accountant is not only a user of digital tools and not only a data analyst, but a systems integrator who combines accounting, taxation, analysis, risk management and cybersecurity. This perspective corresponds to current challenges and defines the strategic role of accounting in the digital transformation of the economy.

Current practice in the use of digital tools in accounting shows that these tools are not autonomous technologies, but function in close interaction with the professional activity of the accountant. The accountant is the central link that connects the capabilities of information systems with the tasks of management, taxation and financial control.

5. Digital Accounting Tools, Professional Transformation and Accounting Quality in the Context of Ukraine's Digitalisation

In Ukraine the key instruments of digital accounting are BAS ERP, electronic reporting systems and the state digital ecosystem Diia. The use of BAS ERP makes it possible to integrate financial and tax accounting, to ensure timely control over financial flows and to simplify interaction with the State Tax Service (Marchuk, 2024). However, the effectiveness of this tool depends on the accountant's ability to configure the system, monitor data accuracy and prepare reporting adapted to the requirements of IFRS and tax legislation. The accountant therefore becomes a system level user who performs both technical and analytical functions.

In the European Union the practical application of digital tools is most clearly manifested through the integration of SAP S/4HANA with the mandatory submission of financial statements in Inline XBRL format. This ensures transparency and standardisation of data at the level of the European Union and creates conditions for analysis by regulators and investors (Verbivska, 2023). For the accountant such integration implies a transition from operational work to the role of analytical communicator who not only prepares reports but also interprets them for different groups of users ranging from management to supervisory authorities.

In the United States ERP systems such as Oracle NetSuite and Microsoft Dynamics 365 are combined with fintech solutions that enable the automatic preparation of tax reports and the analysis of customer data. According to Deloitte (2024), in the United States the accountant increasingly performs the functions of a business analyst by integrating financial data with information on customers, markets and risks. This shows that digital tools are transforming the functional profile of the accountant from a traditional record keeper into a strategic adviser to the business.

Scholarly debates focus on the question of whether digital tools are merely means of optimising work, or whether they are transforming the profession of the accountant itself. Some researchers (Saeed et al., 2023) argue that ERP, BAS and XBRL only automate routine tasks, freeing the accountant for more complex activities. Others (Shcherban et al., 2025) emphasise that these instruments create a new model of the profession in which the accountant acts as an integrator of financial, technological and managerial processes.

The practice of using digital tools in accounting confirms that they do not diminish the role of the accountant but rather strengthen its strategic character. ERP and BAS systems, Inline XBRL, fintech platforms and state services are only technical solutions whose effectiveness depends on the accountant’s competence. In the digital economy the accountant becomes a system integrator who ensures not only the correctness of data, but also their analytical interpretation, security and practical relevance for management. For this reason, contemporary digital tools should not be viewed as an alternative to the profession, but as its new institutional and functional context.

One of the key challenges of accounting digitalisation in Ukraine and worldwide is human resource adaptation. ERP, BAS, Inline XBRL and fintech platforms change the professional role of the accountant and require new competencies. Whereas in the past the main requirements were knowledge of financial accounting and tax legislation, today the following attributes are gaining priority:

- digital literacy, including the ability to work with ERP and BAS systems, analytical modules and cloud platforms;
- analytical skills, including the interpretation of large data sets and the forecasting of financial outcomes;
- knowledge in the field of cybersecurity, including the protection of financial information and the management of data leakage risks.

The main problem for Ukrainian enterprises is that the training of accountants remains largely oriented toward traditional accounting, while the market requires digital analysts (Vasyltsiv, 2022). This generates a gap between educational programmes and the practical needs of business.

The second dimension of the problem concerns the regulatory framework. Ukraine is gradually transitioning to international financial reporting standards and using Inline XBRL technology. At the same time, a number of barriers persist. Tax legislation is frequently amended, which complicates the integration of its provisions into ERP systems (Marchuk, 2024). Issues of cybersecurity remain insufficiently regulated, and existing law only partially covers the protection of accounting information. There is also a lack of harmonisation with European practices, and the absence of uniform requirements for digital reporting limits the possibility for Ukrainian enterprises to integrate into the European market. OECD (2024) stresses that in EU member states and the United States regulatory policy treats digitalisation as an element of economic strategy, whereas in Ukraine regulatory support is often reactive and adapts to new challenges after the fact.

Human resource and regulatory challenges have a direct impact on the transformation of the accounting profession. On the one hand, digital tools require the accountant to perform the functions of a system integrator. Accountants must not only maintain records, but also ensure that data comply with international standards, supervise data protection and establish interaction with state e services. On the other hand, insufficient staff training and an imperfect legal framework create the risk that the accountant will become a hostage to the system when technical requirements exceed professional capabilities.

Empirical evidence shows that about 40 percent of accountants in small and medium sized enterprises experience difficulties in using ERP and BAS systems due to a lack of digital skills, whereas in large corporations this indicator is significantly lower thanks to internal training programmes (Shcherban et al., 2025). This confirms the need to expand digital education and to prepare accountants for work in a digital economy.

The adaptation of human resources and the improvement of the regulatory framework are two interrelated factors that determine the effectiveness of accounting digitalisation. From a systems perspective the accountant cannot fulfil the new role of analyst, integrator and guarantor of data reliability without adequate educational support and regulatory consistency.

The analysis of the theoretical and practical foundations of accounting digitalisation shows that the current transformation of the accounting sphere is systemic in nature and extends far beyond technological automation. The evolution of the concept of digital accounting demonstrates that, starting from the primary computerisation of economic transactions and the creation of stand alone accounting programmes, enterprises have moved toward the formation of comprehensive information ecosystems integrated into all business processes. Digital accounting has acquired the characteristics of an integrated accounting and analytical system that combines financial, tax and managerial processes and ensures the transparency and reliability of financial information.

ERP and BAS systems are an important instrument for implementing this concept. International practice with SAP, Oracle NetSuite and Microsoft Dynamics 365 demonstrates a focus on global standards, cloud technologies and advanced analytical capabilities, while BAS ERP in Ukraine is oriented toward adaptation to national legislation and accessibility for small and medium sized enterprises. Comparative analysis shows that digital accounting is formed at the intersection of globalisation trends and local institutional needs, and that the promising direction lies in combining these two dimensions.

Scholarly approaches to defining the role of the accountant under conditions of digitalisation show that this role is shifting from operational to strategic. The technological approach conceptualises the accountant as a user of digital tools, the analytical approach positions the accountant as a producer of management information, and the systems approach views the accountant as an integrator of financial, technological and managerial processes. From the author’s standpoint it is the systems approach that most adequately reflects the new paradigm. The accountant becomes a system analyst and guarantor of data reliability who ensures economic security and the competitiveness of the enterprise.

Practical examples from Ukraine, the European Union and the United States confirm that digital tools do not reduce the role of the accountant, but increase its importance. In Ukraine this is evident through BAS ERP and integration with the Diia ecosystem. In the European Union this is reflected in the mandatory application of Inline XBRL and harmonisation with IFRS, and in the United States in the synergy between ERP systems, fintech innovations and business analytics. Digital accounting thus transforms the accountant into a key actor in the digital economy capable of combining technical expertise with analytical and strategic competencies.

At the same time the identified human resource and regulatory barriers remain significant. These include low levels of digital competence among some accountants, insufficient harmonisation of legislation with international standards and fragmented regulation in the area of cybersecurity. Such factors constrain the ability to fully integrate digital tools and slow the development of the accounting profession. Overcoming these barriers requires a comprehensive approach that includes the reform of educational programmes, the development of continuous professional training, the harmonisation of legislation with European standards and the creation of conditions for the secure operation of digital platforms.

Digitalisation of accounting is therefore not only a technological innovation, but also a conceptual transformation of the accounting profession. It defines new competency requirements, shapes the strategic role of accounting in the digital economy and creates the preconditions for Ukraine's integration into the global financial and economic space. In this context digital accounting should be regarded as a fundamental element of digital transformation that integrates information systems, regulatory standards and human capital into a unified system for managing knowledge and resources.

The study of the theoretical and practical foundations of accounting digitalisation has shown that contemporary information systems, including ERP, BAS and Inline XBRL, are forming a new architecture of accounting processes in which the accountant acts as an integrator of financial, technological and managerial domains. Equally important, however, is the question of how digitalisation affects accounting quality, since the reliability of financial information, the transparency of management decisions and trust in reporting at both macro and micro levels depend on this.

Traditional views of accounting quality are based on the criteria of reliability, relevance, timeliness and comparability. In the digital age these characteristics acquire a new meaning. Information becomes available in real time, integrated into unified digital ecosystems and, at the same time, vulnerable to cyber threats. The next stage of the research should therefore focus on analysing the key aspects of the impact of digitalisation on accounting quality, beginning with the theoretical foundations of this category.

The concept of accounting quality is a fundamental category in financial and economic research, since the effectiveness of management decisions and the level of trust in financial information directly depend on it. In the traditional scientific paradigm accounting quality is defined through the ability of financial data to reflect the real state of the enterprise, to meet user needs and to ensure the transparency of economic processes (Mills and Yamamoto, 2021).

International Financial Reporting Standards and Generally Accepted Accounting Principles identify a number of key qualitative characteristics of financial information. These include relevance, faithful representation, comparability, timeliness, verifiability and understandability (IFRS Foundation, 2022). These criteria form a basic framework for assessing accounting quality in the global dimension and define universal parameters of transparency and reliability.

In recent years, however, the academic literature has introduced new emphases into the concept of accounting quality. Vasyltsiv (2022) argues that the quality of accounting in a digital environment depends on the integration of financial and tax processes into a unified information environment. In this conception quality is identified not only with the correctness of data, but also with the possibility of their harmonious integration into business processes.

Marchuk (2024) stresses that transparency and real time accessibility of data are becoming the main indicators of trust in financial information. Timeliness thus ceases to be merely a technical criterion and acquires strategic significance under conditions of global crises in which the speed of access to information determines the resilience of the enterprise.

Shcherban et al. (2025) emphasise data security as an integral element of accounting quality. In the context of active cyber threats the reliability of financial information can no longer be considered separately from the level of protection of the systems in which it is generated and stored. Accounting quality therefore appears as a multidimensional concept that includes classical financial criteria as well as technological and legal aspects.

The synthesis of contemporary approaches makes it possible to trace the evolution of accounting quality criteria:

- reliability is transformed into a requirement for the verifiability of algorithms and the accuracy of automated data processing;
- timeliness is reinterpreted as the availability of data in real time;
- comparability is strengthened through standardisation and the use of Inline XBRL;
- transparency is expanded to include the requirement of openness in the global digital environment;
- security emerges as a new key dimension without which other criteria lose relevance.

Digitalisation does not cancel the classical characteristics of quality, but supplements them with new parameters that reflect the conditions of the digital economy.

Taking contemporary research into account, accounting quality in a digital environment can be defined as a complex characteristic of financial information that combines the classical criteria of IFRS with new requirements of the digital economy, including integration, accessibility and security. A systems approach makes it possible to encompass all these aspects and to view quality as a balance between data accuracy, the speed of access, protection and the ability to integrate into global information flows.

Having defined the theoretical foundations of accounting quality and traced their evolution under the influence of the digital economy, it is appropriate to move on to analysing specific digital technologies and assessing how they affect the quality of financial information. In this context particular attention should be paid to cloud systems, Inline XBRL, big data and artificial intelligence that currently form the core of the digital transformation of accounting. Their impact will be the focus of the next subsection.

Digital technologies radically change not only the organisation of accounting, but also the criteria for its quality. If traditionally accounting quality was associated with the reliability, timeliness and comparability of financial information, then in the digital economy these characteristics acquire new content. Cloud services, ERP and BAS solutions, Inline XBRL, big data and artificial intelligence create a new environment in which accounting information becomes not only an outcome, but also a resource for strategic management.

Researchers emphasise that digitalisation has a dual effect. On the one hand it increases the accuracy, accessibility and transparency of data. On the other hand it generates risks of technical dependence and cyber threats (Saeed et al., 2023; Shcherban et al., 2025). The impact of digital technologies on accounting quality should therefore be considered in systemic terms as an interaction between technical capabilities, institutional conditions and the professional role of the accountant.

Cloud services have become one of the key drivers of accounting transformation. They allow enterprises to store and process accounting data on remote servers and to ensure access to information at any time and from any location. This significantly increases the timeliness and transparency of financial information, which are basic criteria of its quality (Marchuk, 2024).

In international practice cloud systems such as Oracle NetSuite, QuickBooks Online and Xero facilitate the integration of accounting data with tax and management modules. In EU member states they are linked to regulatory requirements for the submission of digital reports, which guarantees data comparability at the supranational level (OECD, 2024).

In Ukraine the development of cloud solutions is taking place in parallel with the spread of BAS ERP. Although BAS has traditionally been installed on local servers, integration with state digital services, including Diia and e reporting, effectively creates conditions for partial cloud operation. For the accountant this means a new function, namely the management of digital channels for information exchange and the assurance of data reliability in real time.

Inline eXtensible Business Reporting Language is one of the most important tools for ensuring the quality of accounting information worldwide. It standardises the presentation of financial data and makes them comparable across countries, regulators and investors. In EU member states the use of Inline XBRL is mandatory for companies reporting under IFRS. It enables the automatic verification of data accuracy and simplifies access for a wide range of users (IFRS Foundation, 2022).

In Ukraine the introduction of Inline XBRL began in 2020 and has become an important step toward harmonisation with European practice. However, Shcherban et al. (2025) note that enterprises experience difficulties with adaptation due to a shortage of staff with the necessary competencies and technical integration problems. As a result the accountant must act not only as a record keeper, but also as a digital coordinator responsible for the correct coding of financial indicators in an international format.

The use of big data and artificial intelligence in accounting opens new possibilities for improving information quality. Machine learning algorithms can analyse large volumes of financial data, identify patterns, forecast risks and generate recommendations for management.

According to Deloitte (2024), the application of artificial intelligence in accounting reduces the share of errors in reporting by 20 to 30 percent and doubles the speed of audit procedures. At the same time, questions arise regarding whether data generated by algorithms can be considered sufficiently reliable. Brynjolfsson and McAfee (2021) emphasise that automated systems may reproduce biases embedded in the initial algorithms, thereby calling objectivity into question.

From the perspective of the accountant’s role this means that the accountant must act not only as a user of artificial intelligence, but also as a critical analyst capable of assessing the reliability and relevance of machine generated data.

The impact of digital technologies on accounting quality is multidimensional. Cloud services ensure accessibility and transparency, Inline XBRL provides standardisation and comparability, and big data and artificial intelligence open new horizons for analytics. These advantages, however, are accompanied by risks including dependence on algorithms, vulnerability to cyber attacks and shortages of qualified personnel. From the author's perspective accounting quality in the digital age should be viewed as a dynamic balance between accuracy, accessibility and data security that is ensured through a combination of technological solutions and the professional competencies of the accountant. Only a systems approach, in which the accountant performs the function of integrator and guarantor of information reliability, allows digital technologies to be transformed from a source of risk into an instrument for improving accounting quality.

Having examined the influence of digital technologies in the global dimension, it is appropriate to turn to an analysis of the practical aspects of their implementation in Ukraine. The national cases of BAS ERP, Diia and electronic reporting demonstrate how global digitalisation trends are adapted to local conditions and how they affect accounting quality in the Ukrainian context.

Although accounting digitalisation clearly offers advantages including greater transparency, timeliness and reliability of data, it also creates a number of new risks. Contemporary literature (Saeed et al., 2023; Shcherban et al., 2025) treats these risks as a key factor that determines the real impact of digital technologies on accounting quality. They encompass technical, human resource, legal and organisational aspects and form a complex system of challenges for enterprises.

One of the most serious challenges is the protection of financial data. With the development of cloud services and online reporting enterprises become vulnerable to cyber attacks, phishing, data leaks and unauthorised access to accounting systems. International practice documents numerous cases in which financial data were compromised through hacking attacks on ERP systems, including SAP and Oracle (PwC, 2023).

In Ukraine this problem is exacerbated by wartime conditions, in which cyber threats also acquire a geopolitical dimension. According to the State Service of Special Communications, between 2022 and 2024 the number of attacks on public and corporate resources more than doubled. These risks undermine trust in the reliability of accounting data and thus directly affect accounting quality.

Accounting quality in a digital environment also depends significantly on the stability of legislation. In Ukraine frequent changes to tax law and incomplete harmonisation with international standards create problems for integration into global markets (Marchuk, 2024). Inline XBRL represents a step forward in this context, but its implementation is taking place under conditions of regulatory uncertainty, which complicates the work of accountants. Moreover, data protection issues have yet to be regulated at a level that corresponds to EU standards.

The risks of accounting digitalisation therefore have a systemic character and directly influence accounting quality. Cyber threats cast doubt on data reliability, human resource problems reduce timeliness and accuracy, regulatory instability hinders comparability and organisational barriers limit transparency. From the author's perspective accounting quality in the digital age depends on the enterprise's ability to ensure a systemic balance between technology implementation, staff training, data protection and regulatory stability. Without such a balance digitalisation may not improve, and may even lower, accounting quality by turning it into a source of risk.

The identified advantages and risks of digitalisation demonstrate that enhancing accounting quality cannot be achieved merely by technical upgrades. It requires a comprehensive approach that combines the modernisation of information systems, the reform of educational programmes, the harmonisation of regulatory frameworks and the strengthening of institutional trust in digital solutions.

Theoretical and practical analysis has shown that digitalisation fundamentally changes conceptions of accounting quality. If traditionally it was defined by reliability, timeliness, comparability and understandability, then in the digital economy these parameters acquire new content. Alongside classical characteristics, new features emerge, including integration, real time accessibility and data security. These are responses to the challenges of the information society.

Cloud services, ERP and BAS systems, Inline XBRL, big data and artificial intelligence reveal substantial potential to improve the quality of financial information by reducing errors, ensuring comparability and openness and expanding analytical possibilities. At the same time digitalisation generates risks, including cyber threats, human resource constraints and regulatory instability, which may diminish trust in reporting. In this context the accountant plays a key role. The accountant is no longer just a record keeper, but a system integrator of financial, technological and managerial processes.

Ukrainian practice has shown that the implementation of BAS ERP, the Diia ecosystem and Inline XBRL constitutes an important step toward enhancing accounting quality. Their effectiveness, however, depends directly on the level of digital competence among staff and on the harmonisation of legislation with international standards. Accounting quality under conditions of digitalisation should therefore be viewed as a dynamic balance between technologies, regulatory frameworks and professional competencies. Only a systems approach can ensure that digitalisation becomes a factor that strengthens the transparency, reliability and credibility of financial information and thus supports Ukraine's integration into the global economic space. The practice of digitalising accounting in Ukraine demonstrates that its impact on quality is multifaceted. ERP and BAS systems support automation and timeliness, Diia creates a transparent ecosystem for interaction between business and the state, and Inline XBRL integrates financial reporting into the global environment. At the same time significant challenges remain, including insufficient staff qualifications, high costs of implementing new technologies and cybersecurity threats. From the author's perspective it is precisely a systems approach, which involves the simultaneous modernisation of software solutions, legislation and accountant training, that can ensure improvements in accounting quality in Ukraine.

Conclusion. The research on accounting digitalisation and the digital economy in Ukraine has shown that current digital transformation processes are systemic in nature and affect not only the technical level of accounting, but also the conceptual foundations of economic science. The concept of digital accounting extends beyond the automation of primary operations and acquires the features of a comprehensive information system that integrates management, analytical and control functions.

The analysis of contemporary approaches confirms that the quality of accounting in a digital environment is determined not only by the reliability and timeliness of data, but also by characteristics such as integration into business processes, security, real time accessibility and compliance with global standards, including Inline XBRL and IFRS. New scholarly debates on the transformation of classical accounting principles are thus emerging.

The study of international ERP practices, including SAP, Oracle and Microsoft Dynamics, and Ukrainian analogues such as BAS ERP, Diia and Inline XBRL, indicates that global systems are oriented toward scalability and integration into international markets. Ukrainian solutions, by contrast, are adapted to national legislation and accessible for small and medium sized enterprises, but have limitations in terms of global integration.

Digitalisation of accounting has had a positive influence on the timeliness and transparency of reporting, yet has also generated a number of risks, including cyber threats, a shortage of staff with digital competencies and fragmented regulatory oversight. Under conditions of martial law the importance of these challenges increases further, making accounting a vulnerable element of economic security.

The role of the accountant is shifting from record keeper to system integrator. The accountant must combine knowledge in accounting, information technology and law, ensuring not only the preparation of reports, but also strategic analysis and risk management.

Digitalisation of accounting in Ukraine therefore has a dual effect. On the one hand it creates new opportunities for transparency and integration into global financial markets. On the other hand it generates challenges associated with cybersecurity, human resources and regulatory barriers. A scholarly approach makes it possible to conceptualise digital accounting as a multilevel system in which technologies, education and regulatory support form the basis for high quality financial information.

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

Conflict of interest. The author 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 author 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 author 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. Benko, M. M., & Sopko, V. V. (2011). Bukhgalterskyi oblik u skladi informatsiinoi systemy pidpryiemstva yak obiektu informatsiinykh tekhnolohii [Accounting as part of the information system of the enterprise as an object of information technologies]. *Bukhgalterskyi oblik i audyt*, (3), 117–124. Retrieved from the Vernadsky National Library of Ukraine database. URL: http://www.business-navigator.ks.ua/journals/2011/24_2011/24_2011.pdf#page=115
2. Borblik, K. (2022). *Digitalization of the Ukrainian economy: Global challenges and local dilemmas*. MRU CRIS Repository. https://cris.mruni.eu/server/api/core/bitstreams/6fe83e53-6c39-4bf7-956c-46f59ccb0942/content
3. Ingram, G., & Vora, P. (2024). *Ukraine: Digital resilience in a time of war* (Working Paper 185). Brookings Institution. URL: https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf

4. Ivanova, N. (2024). Digital transformation of Ukraine: Impact on the economy, quality of life and achievement of sustainable development goals. *Economics of Systems Development*, 6(1). https://doi.org/10.32782/2707-8019/2024-1-9
5. Kovalov, B., Karintseva, O., Kharchenko, M., Khymchenko, Y., & Tarasov, V. (2023). Methods of evaluating digitization and digital transformation of business and economy: The experience of OECD and EU countries. *Economics of Systems Development*, 5(1), 18–25. https://doi.org/10.32782/2707-8019/2023-1-3
6. OECD (2024), *Enhancing Resilience by Boosting Digital Business Transformation in Ukraine*, OECD Publishing, Paris, https://doi.org/10.1787/4b13b0bb-en.
7. OECD (2024), *OECD Digital Economy Outlook 2024 (Volume 2): Strengthening Connectivity, Innovation and Trust*, OECD Publishing, Paris, https://doi.org/10.1787/3adf705b-en.
8. Selivanova, N. M., Kalabina, V. O., & Minzhyrian, N. I. (2024). Digitalization of accounting and financial reporting in Ukraine. *Economics: Time Realities*, (4[74]), 89–98. https://doi.org/10.15276/ETR.04.2024.10
9. Shevchuk, O. (2024). Transformation of the fundamental principles of accounting and control in the system of electronic transactions. *Herald of Economics*, no. 2, Aug. 2024, pp. 131-49, https://doi.org/10.35774/visnyk2024.02.131.
10. Tenyukh, Z., Pelekh, U., & Khocha, N. (2022). Application of digital technologies in accounting and auditing at enterprises of Ukraine. Scientific Bulletin of Mukachevo State University. Series "Economics", 9(4), 46-55. https://doi.org/10.52566/msu-econ.9(4).2022.46-55
11. Vasyltsiv, T., Mulska, O., Levytska, O., Lupak, R., Semak, B., & Shtets, T. (2024). Factors of the Development of Ukraine's Digital Economy: Identification and Evaluation. *Science and Innovation*, *18*(2), 44–58. https://doi.org/10.15407/scine18.02.044
12. Verbivska, L., Abramova, M., Gudz, M., Lyfar, V., & Khilukha, O. (2023). Digitalization of the Ukrainian economy during a state of war is a necessity of the time. *Amazonia Investiga*, *12*(68), 184-194. https://doi.org/10.34069/AI/2023.68.08.17

Section 2.3. Quality of digital reporting: risks, precautions, and government oversight mechanisms

Zinaida Zhyvko[1]

[1]Doctor of Science (Economics), Professor, Professor of the Department of Aviation Management, Ukrainian State Flight Academy, Kropyvnytskyi, Ukraine, ORCID: https://orcid.org/0000-0002-4045-669X

Citation:
Zhyvko, Z. (2025). Quality of digital reporting: risks, precautions, and government oversight mechanisms. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 132-153). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-132-153

Abstract. *The study examines how the rapid spread of structured digital reporting formats is transforming the quality, risks and supervision of financial and non-financial disclosures in capital markets and public governance systems. The objective is to develop an integrated conceptual and comparative framework for assessing the quality of digital reporting, distinguishing between technical, semantic and pragmatic dimensions and linking them to specific regulatory architectures and oversight tools. Methodologically, the research relies on doctrinal analysis of international standards and taxonomies for financial and sustainability reporting, comparative review of regulatory regimes in the European Union, the United States and selected emerging markets, and analytical generalisation based on typologies and risk matrices embedded in the text and tables. The main results show that digital financial reporting is converging on XBRL and Inline XBRL but remains heterogeneous with respect to tagging scope, validation rules and the institutionalisation of data quality committees, while digital non-financial reporting is being reshaped by CSRD and ESRS in the EU, the IFRS Sustainability Disclosure Taxonomy at global level and the gradual digitalisation of voluntary ESG regimes. High quality digital presentation is identified as a double edged phenomenon that enables transparency and automated analytics yet simultaneously creates new channels for impression management, greenwashing, semantic opacity and information overload. The analysis further demonstrates that effective preventive measures combine prescriptive taxonomies, automated validation, SupTech based anomaly detection and robust digital operational resilience frameworks, while also highlighting proportionality challenges for smaller entities and less mature markets. Conclusions emphasise that the quality of digital reporting depends on the coherence of content standards, internal governance and supervisory architectures, and that fragmented or under enforced regimes can turn digital data into an amplifier of risk rather than a safeguard of transparency. Directions for further research include empirical testing of the proposed typologies and risk matrices, evaluation of the real-world impact of SupTech on enforcement outcomes, and investigation of digital literacy and behavioural aspects that shape how different user groups interpret high quality but complex digital reports.*

Keywords: *digital financial reporting; digital non-financial reporting; European Single Electronic Format; corporate sustainability reporting; data quality; greenwashing; SupTech; RegTech; operational resilience; government oversight.*

https://doi.org/10.36690/PUBADM

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

1. Types of digital financial reporting and quality requirements in different jurisdictions. Digital financial reporting has progressively moved from static electronic documents, such as PDF or basic HTML, to structured, machine readable formats that embed accounting semantics in each disclosed figure. In the early phase, regulators accepted electronic submissions that merely replicated paper reports, which improved accessibility but did not fundamentally change the way data could be analysed. With the introduction of XBRL and later Inline XBRL, the unit of disclosure shifted from the document to the tagged data point. Each item in the financial statements is associated with an element in a taxonomy, usually derived from IFRS or local GAAP, which allows automated aggregation, validation and comparison across entities and time (IFRS Foundation, 2020; Valentinetti, 2012). In this sense, "types" of digital reporting can be distinguished along a spectrum from unstructured electronic reports to highly structured, tagged and validated submissions.

The European Union is often cited as a leading example of structured digital financial reporting through the European Single Electronic Format. Under the ESEF Regulation, all issuers whose securities are admitted to trading on an EU regulated market must prepare their annual financial reports in XHTML with embedded Inline XBRL tags based on the ESEF taxonomy, which is anchored to the IFRS Taxonomy (ESMA, 2025). The ESEF Reporting Manual specifies detailed quality requirements. Issuers are required to select appropriate taxonomy elements, design extensions only when necessary, anchor extensions to base taxonomy concepts of the same nature, and ensure that all primary financial statements are fully tagged. The manual also describes a comprehensive set of technical validation rules that check the syntax of the XHTML and XBRL, the consistency of units and periods, the correctness of calculation relationships and the uniqueness of identifiers (ESMA, 2025; ESMA, 2017). These rules are implemented in supervisory tools used by national competent authorities and by software vendors, which means that quality is enforced both at the point of preparation and at the point of filing.

Recent updates to the ESEF Reporting Manual further illustrate how regulators use digital reporting to improve comparability and analytical value. The 2025 update aligns the ESEF taxonomy with the latest IFRS Taxonomy, including provisions for new standards such as IFRS 18 and IFRS 19, and introduces clarifications on how to handle empty values, block tags and complex extension structures (ESMA, 2025). By tightening guidance on these technical matters, ESMA aims to reduce diversity in practice that would otherwise undermine the usefulness of digital data for

https://doi.org/10.36690/PUBADM

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

cross country analysis. In effect, ESEF defines a specific type of digital reporting: Inline XBRL embedded in a regulated XHTML container, accompanied by a prescriptive manual and mandatory validation, which together create a relatively high and measurable quality baseline for financial data across the Union.

In the United States, the Securities and Exchange Commission has followed a slightly different trajectory but has converged on a similar technology. Public companies are required to submit structured financial statement data to EDGAR using XBRL, and more recently Inline XBRL, in connection with filings such as Forms 10 K, 10 Q and 20 F (SEC, 2018). The SEC's EDGAR Filer Manual, alongside the separate EDGAR XBRL Guide, sets out technical requirements for filing formats, taxonomy use, linkbases and validation (SEC, 2025). In addition to basic syntactic checks, the United States has developed an institutional mechanism for improving semantic and pragmatic quality: the XBRL US Data Quality Committee. The DQC issues freely available validation rules that target common data quality problems, such as inappropriate negative values, inconsistent axis member combinations or improbable relationships between tagged items (XBRL US, 2022). These rules can be implemented in preparer software or run independently, allowing both filers and users to diagnose and correct errors before they affect market analysis.

This layered approach means that "digital financial reporting" in the US context is best described not simply as using Inline XBRL, but as submitting structured data that complies with SEC taxonomies, EDGAR technical specifications and DQC rule sets. Studies of XBRL adoption suggest that the existence of such rule sets and guidance improves the reliability of digital data for investors and researchers, although quality still varies with preparer expertise and software support (Alles, 2012; Valentinetti, 2012). The SEC has also begun to embed selected DQC rules in the U S GAAP Taxonomy through the DQCRT, which further institutionalises these quality checks (FASB, 2020).

Outside the EU and US, several jurisdictions, including Japan, Korea and a number of EU candidate and neighbouring countries, operate XBRL based filing systems with their own taxonomies and quality regimes. In Japan, for example, the Financial Services Agency requires listed companies to file in XBRL and provides a set of validation rules to ensure basic completeness and arithmetic consistency. In many of these systems, tagging is initially limited to primary statements, with gradual extension to notes and disclosures as preparers become more familiar with the technology (IFRS Foundation, 2020; Bonsón et al., 2009). Emerging markets often adopt the

IFRS Taxonomy as a starting point and localise it to reflect domestic reporting practices, a process that raises its own quality questions about extension governance and taxonomy maintenance (Valentinetti, 2012).

From a conceptual standpoint, researchers distinguish several dimensions of digital reporting quality. Technical or syntactic quality refers to whether the digital file conforms to XBRL and filing specifications and can be processed by standard tools. Semantic quality concerns the appropriateness of element selection, the correct representation of economic phenomena and the disciplined use of extensions. Pragmatic quality relates to the usefulness of the data for decision making by investors, regulators and other users, which depends on comparability, timeliness and the absence of systematic bias (IFRS Foundation, 2020; Alles, 2012). Regulators such as ESMA and the SEC directly control syntactic quality through validation engines and filing checks. Semantic and pragmatic quality are influenced by guidance documents, market feedback, data quality committees and the maturity of the preparer community.

The IFRS Foundation has emphasised that the benefits of digital reporting are realised only when the entire ecosystem of standard setters, regulators, software vendors and preparers works with a common understanding of data quality objectives. In a widely cited speech on digital reporting, IFRS representatives highlight four key stakeholder groups: issuers and auditors, standard setters and regulators, investors and data aggregators, and academics (IFRS Foundation, 2020). Each group has different expectations of quality and different capacities to detect and correct errors. For example, investors are primarily concerned with consistency across entities and periods, while regulators focus on compliance and risk monitoring. This diversity of perspectives reinforces the need for explicit quality frameworks that define what good digital reporting looks like and how it can be verified.

The resulting global landscape can be summarised as a set of archetypal regimes that differ in format, taxonomy basis and quality mechanisms.

This comparison shows that the “type” of digital financial reporting in a given jurisdiction is not defined solely by the file format, but by the combination of format, taxonomy and institutionalised quality mechanisms. Where regulatory regimes require comprehensive tagging, provide detailed manuals and deploy automated validation and feedback, digital reports tend to achieve higher levels of syntactic and semantic quality, which in turn supports more reliable secondary use of data by investors, supervisors and researchers.

Table 2.23. Main regimes of digital financial reporting and associated quality mechanisms

Regime type	Typical jurisdictional examples	Digital format and taxonomy basis	Main quality mechanisms
Highly structured and regulated Inline XBRL	European Union issuers under ESEF; large filers in advanced markets	XHTML with embedded Inline XBRL, ESEF taxonomy aligned with IFRS Taxonomy	Mandatory tagging of primary statements, prescriptive guidance in ESEF Reporting Manual, regulator operated validation engines, strong feedback loops with software vendors and filers (ESMA, 2025).
Structured XBRL or Inline XBRL with market driven quality enhancement	United States SEC filers	Inline XBRL for core filings, US GAAP or IFRS taxonomies, EDGAR technical standards	EDGAR Filer Manual, SEC structured data rules, XBRL US Data Quality Committee rule sets, emerging integration of DQC rules into taxonomies (SEC, 2018; SEC, 2025; XBRL US, 2022).
Developing XBRL regimes	Japan, Korea, selected emerging markets	XBRL or Inline XBRL instances, national taxonomies based on IFRS or local GAAP	Basic validation for completeness and arithmetic consistency, phased expansion of tagging scope, gradual refinement of taxonomies as experience accumulates (IFRS Foundation, 2020; Bonsón et al., 2009).
Semi structured or document centric electronic reporting	Jurisdictions using PDF or HTML without tagging	PDF or untagged HTML, narrative focus, ad hoc structure	Limited formal quality mechanisms beyond traditional accounting and auditing standards, reliance on manual review and data aggregation, low machine readability and comparability (IFRS Foundation, 2020).

Sources: systematized by the author

Where such mechanisms are weak or absent, the promise of digital reporting remains only partially fulfilled, and much of the burden of quality assurance shifts downstream to data users.

In sum, types of digital financial reporting should be understood as combinations of format, taxonomy and enforcement. Jurisdictions that move decisively toward structured, tagged and validated reporting create an environment in which the quality of presentation can be monitored and improved systematically. Conversely, where digital reporting is limited to PDFs or lightly regulated XBRL instances, the potential of digital technologies for improving transparency and comparability remains only partially realised, and much of the effort shifts from regulators to data aggregators and users, who must clean and reconcile inconsistent data on their own.

2. Types of digital non-financial reporting and quality requirements in different jurisdictions. Digital non-financial reporting has evolved from isolated narrative sustainability reports to a layered global ecosystem that increasingly relies on taxonomies, machine readable formats and supervisory scrutiny. At present, it is useful to distinguish three broad regimes. The first is mandatory, standardised and digitally structured sustainability reporting, most advanced in the European Union under the Corporate Sustainability Reporting Directive (CSRD) and European Sustainability Reporting Standards (ESRS). The second consists of global baseline frameworks with associated digital taxonomies, particularly IFRS S1 and S2 together with the IFRS Sustainability Disclosure Taxonomy issued by the International Sustainability Standards Board. The third is a still very large space of voluntary or semi-regulated ESG reporting, where frameworks such as GRI are often used, and which is now itself undergoing digitalisation through the newly launched GRI Sustainability Taxonomy. These regimes differ not only in normative scope, but also in how they conceptualise and operationalise quality in a digital environment.

In the European Union, the CSRD has transformed sustainability reporting from an essentially voluntary practice into a mandatory, standard-set and digital component of the management report. Companies in scope must report in accordance with ESRS and integrate sustainability disclosures into the management report which, under the broader digital reporting architecture, is expected to be prepared in a single electronic reporting format compatible with XHTML and Inline XBRL, aligned with ESEF and the future European Single Access Point (ESAP) (European Commission, 2023). EFRAG has been mandated to develop the ESRS XBRL taxonomies that will digitise sustainability statements, that is, to provide the technical vocabulary that allows each disclosure requirement in ESRS to be expressed as a tagged data point (EFRAG, 2025). The resulting digital regime does not simply require companies to publish a sustainability report. It requires them to map hundreds of qualitative and quantitative datapoints to a structured taxonomy that is used by supervisors, investors and data aggregators, and to file those tagged reports into ESAP where they can be analysed at scale (KeyESG, 2025).

The quality of digital non-financial reporting in the EU context is therefore shaped by three interlinked layers. First, content quality is anchored in the ESRS themselves, which define detailed, topic specific and cross-cutting disclosure requirements that must be applied on the basis of double materiality. This narrows the scope for highly selective or marketing driven sustainability narratives because many key disclosures are mandatory unless an explicit materiality rebuttal is justified (EFRAG, 2023). Second, digital quality is operationalised through the ESRS XBRL taxonomy and the associated technical rules. Each disclosure requirement is linked to taxonomy elements, labels, data types and validation rules. In practice this means that omissions, inconsistencies or illogical combinations become visible to supervisors and users when they analyse ESAP data sets rather than reading reports one by one (XBRL International, 2025). Third, assurance quality is introduced through the CSRD requirement for mandatory limited assurance from the first year of reporting, with a later move to reasonable assurance. This covers not only narrative content but also the processes and controls that generate sustainability data, including the digital representation of that data (ICAEW, 2025; Straková, 2025).

These characteristics allow CSRD and ESRS to be seen as a distinct type of digital non-financial reporting. It is highly structured, since thousands of potential datapoints will eventually be tagged in XBRL. It is mandatory and enforced, since non-compliance can trigger administrative sanctions. It is assured, since professional and sometimes non-accounting assurance providers must express an opinion on the sustainability statement. Finally, it is interoperable with digital financial reporting, since ESEF, ESRS and ESAP are being designed as a single infrastructure for corporate digital data (European Commission, 2023).

At the global level, the ISSB has created a parallel but conceptually different digital regime. IFRS S1 and S2 define a global baseline of sustainability related financial disclosures aimed primarily at the information needs of investors. In April 2024 the ISSB issued the IFRS Sustainability Disclosure Taxonomy, which translates those requirements into XBRL elements and structures (IFRS Foundation, 2024). The taxonomy is designed to be used by jurisdictions that adopt or adapt IFRS S1 and S2, and it is explicitly built to connect with digital financial reporting taxonomies. This connectivity means that sustainability-related financial information can be tagged in the same filings as the financial statements, allowing users to analyse, for example, how climate-related risks disclosed under IFRS S2 relate to impairment losses or cash-flow forecasts reported under IFRS Accounting Standards.

In this regime, digital quality is defined in terms of global comparability, internal consistency and connectivity with financial information. The ISSB emphasises that the taxonomy provides a common digital language that, when used consistently, allows investors to query data on risk exposures, transition plans or scenario analyses across entities and jurisdictions (IFRS Foundation, 2024). However, because ISSB standards and the taxonomy are not directly mandatory at the global level, the degree of enforcement and assurance will depend on how individual jurisdictions embed them in their regulatory systems. Some countries are considering requiring ISSB-aligned digital tagging as part of their listing rules, while others may treat them as voluntary guidance. This creates a more heterogeneous landscape for non-financial digital reporting quality than in the EU, even if the technical tools are in place.

A third and still dominant part of the global landscape consists of voluntary or semi-regulated ESG and sustainability reporting that uses frameworks such as the Global Reporting Initiative Standards, often in PDF or HTML formats. Until recently, these reports were digital only in a trivial sense. They were published on websites but lacked machine readable structure. This is now beginning to change. GRI has launched the GRI Sustainability Taxonomy, an XBRL based taxonomy that covers all GRI Standards and allows organisations to file GRI aligned sustainability disclosures in a structured digital format (GRI, 2025). The taxonomy can be used through dedicated web forms or by integrating XBRL functionality into reporting tools. Its explicit aim is to strengthen interoperability with other standards and to improve access to sustainability data for multiple stakeholders.

However, the quality mechanisms in this voluntary regime are weaker and more fragmented. Content quality is driven mainly by internal governance, board oversight and reputational incentives, with varying degrees of adherence to GRI's own recommendations on completeness and balance. Digital quality depends on whether entities actually adopt the GRI Taxonomy, whether they implement validation rules correctly and whether any assurance is commissioned on digital files, which is not currently required in most jurisdictions. As a result, empirical research continues to find considerable diversity in the completeness, consistency and comparability of ESG indicators, even among firms claiming GRI compliance (Accountancy Europe, 2023; OECD, 2025).

To clarify these differences, the main types of digital non-financial reporting can be summarised as follows.

From a quality of presentation perspective, the move toward structured, tagged non-financial reporting is explicitly linked to concerns about greenwashing and the reliability of environmental and social claims. OECD work on misleading environmental claims shows that vague, unsubstantiated or unverifiable statements are widely used and can distort consumer decisions (OECD, 2011; OECD, 2025). Digitalisation interacts with these concerns in two ways. On the one hand, structured taxonomies and XBRL tagging can make inconsistencies, omissions and implausible claims easier to detect through automated analysis. On the other hand, digital channels can amplify the spread of misleading claims if data are not properly validated or contextualised.

https://doi.org/10.36690/PUBADM

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

Table 2.24. Types of digital non-financial reporting and associated quality mechanisms

Regime type	Digital format and structuring	Scope and standards	Main quality mechanisms
CSRD plus ESRS in the EU	Sustainability statement as part of XHTML management report, tagged with ESRS XBRL taxonomy, integrated with ESEF and ESAP	Double materiality sustainability information covering environmental, social, governance and cross-cutting topics for in-scope EU and certain non-EU entities	Detailed ESRS disclosure requirements, mandatory digital tagging, supervisory validation, centralised access via ESAP, mandatory limited and later reasonable assurance on sustainability information (European Commission, 2023; EFRAG, 2023; ICAEW, 2025).
IFRS S1/S2 plus IFRS Sustainability Disclosure Taxonomy	XBRL based taxonomy for sustainability-related financial information that can be embedded in digital financial filings	Global baseline disclosures on sustainability-related risks and opportunities that affect enterprise value, focused on investors' needs	Taxonomy governance by ISSB, public due process, alignment with IFRS S1 and S2, emphasis on connectivity with financial reporting, jurisdiction specific enforcement and assurance where adopted (IFRS Foundation, 2024).
GRI based and other voluntary ESG reports	Traditionally PDF or HTML, now increasingly supported by GRI Sustainability Taxonomy for XBRL filing	Broad ESG and sustainable development disclosures, often beyond financially material issues, typically framed by GRI Standards or similar	Internal governance, market expectations, voluntary assurance, optional use of GRI XBRL taxonomy; absence of mandatory tagging limits cross-entity comparability and automated analysis (GRI, 2025; OECD, 2025).

Sources: systematized by the author

This is why both CSRD and the ISSB taxonomy stress connectivity with financial information and verifiability as central quality criteria, while GRI positions its taxonomy as a tool to improve accessibility and comparability of sustainability data rather than as a purely technical exercise (European Commission, 2023; IFRS Foundation, 2024; GRI, 2025).

Quality of digital non-financial reporting can therefore be decomposed into several dimensions that cut across regimes. Technical or syntactic quality refers to whether digital files conform to XBRL specifications, taxonomy constraints and filing rules, so that they are machine readable and free from structural errors. Semantic quality is concerned with whether the selected elements and reported values faithfully represent the underlying sustainability phenomena, which is threatened by inappropriate use of extensions, mis-tagging or selective omission. Pragmatic quality relates to the usefulness of the digital data for decision making and supervision, which depends on comparability, timeliness and the ability to link sustainability datapoints to financial and operational indicators. Recent OECD work on digital tools for environmental information emphasises that these dimensions are interdependent: technical precision without semantic integrity does not prevent greenwashing, and semantically rich narratives that are not digitally structured are difficult to monitor at scale (OECD, 2025).

In the EU regime, all three dimensions are addressed through the combination of ESRS content requirements, XBRL taxonomies and assurance obligations. In the ISSB regime, technical and semantic quality are embedded in the taxonomy and standards, while pragmatic quality will depend on how jurisdictions integrate sustainability data into their supervisory and market infrastructures. In the voluntary GRI regime, quality is more uneven. The new taxonomy improves technical and potentially semantic quality, but pragmatic quality will still depend heavily on user demand, data aggregators and any soft enforcement by stock exchanges or lenders.

Overall, the emerging architecture of digital non-financial reporting illustrates a clear policy trend. Standard setters and regulators are using digital taxonomies, XBRL based filing and assurance obligations as instruments to transform sustainability reporting from a marketing oriented narrative into an auditable, analysable dataset. At the same time, there is a growing recognition that smaller entities and emerging markets will need proportionate standards and digital tools if they are to participate meaningfully in this ecosystem (ITS Rio Institute, 2017). The result is a differentiated landscape, in which high quality, structured non-financial digital reporting is gradually becoming mandatory for large issuers in major markets, while voluntary and semi-structured reporting continues elsewhere. For any study of quality in digital reporting, this heterogeneity is central. The same concept of sustainability disclosure is now implemented through very different digital arrangements, and any assessment of quality needs to take into account not only what is reported, but how it is structured, tagged, validated and supervised.

3. High quality digital presentation of reporting and the risks it creates. In contemporary capital markets and public governance, high quality digital presentation of reporting is widely promoted as a prerequisite for transparency, accountability and informed decision making. Inline XBRL based filings, interactive annual reports, ESG dashboards and sustainability microsites are presented as hallmarks of good disclosure practice. From a technical perspective, these formats indeed facilitate machine readability, enable automated analytics and improve user navigation. However, research on impression management, greenwashing and information overload demonstrates that sophisticated digital presentation can also become an instrument of strategic communication that shapes perception more than it enhances understanding (Merkl Davies & Brennan, 2017; Boiral, 2013; OECD, 2024). High quality form can coexist with, and sometimes obscure, weaknesses in content, selective disclosure and biased framing. In a digital environment where users experience cognitive constraints and rely on visual cues, this tension between form and substance becomes a central risk for both financial and non financial reporting.

A first group of examples relates to digital financial reporting where technologically advanced formats coexist with subtle forms of earnings cosmetics. Listed companies are increasingly required to file their financial statements in structured formats such as Inline XBRL under ESEF or SEC rules. These filings are often accompanied by interactive web based annual reports that present graphs, key performance indicators and narrative highlights. Studies of online annual reports show that management systematically uses visual and textual devices to emphasise favourable outcomes and downplay unfavourable ones. For example, positive performance trends are more likely to be graphed, while negative trends are either not graphed or are presented on compressed scales that visually minimise their deterioration (Beattie & Jones, 2008; Cho et al., 2010). When these techniques are embedded in high quality interactive interfaces, users may be drawn to visually salient metrics, such as adjusted earnings or alternative performance measures, while paying less attention to more conservative or risk related indicators. Inline XBRL tagging ensures that the underlying data can be extracted and analysed by sophisticated users and regulators, yet the primary interaction for many investors, journalists or citizens remains the visual interface. High quality presentation therefore creates a risk of perception bias, where technical compliance and professional design are unconsciously interpreted as evidence of balanced disclosure.

The risk is amplified when complex but technically valid tagging strategies are combined with polished front ends. XBRL based reporting allows issuers to use extensions, dimensional modelling and aggregation choices that are formally acceptable but economically opaque. Research on XBRL filings has shown that some preparers strategically select broader taxonomy elements or create custom extensions in a way that reduces the visibility of specific items, such as certain categories of expenses or risk exposures, while still passing all syntactic validation checks (Preciado & Robinson, 2016). From a supervisory perspective, such filings appear high quality because they conform to schema rules and data quality checks. From

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

a user perspective, however, the combination of visually persuasive dashboards and semantically opaque tagging can hinder the reconstruction of the entity's true financial position. The risk here is not overt misstatement, which enforcement can address, but subtle semantic dilution that makes economically important facts harder to isolate in both human and machine analysis.

A second group of examples concerns digital non financial reporting, in particular sustainability and ESG disclosures. Modern ESG communication frequently takes the form of multimedia microsites, interactive materiality matrices, SDG maps and impact dashboards that visually highlight positive contributions. Under CSRD and ESRS, such disclosures are increasingly being integrated into the management report and tagged using XBRL taxonomies. Parallel developments at the global level, such as the IFRS Sustainability Disclosure Taxonomy and the GRI Sustainability Taxonomy, aim to standardise digital access to ESG data. In principle, these initiatives support better quality and comparability. Empirical research, however, indicates that firms with weaker environmental performance or more controversies often produce longer and more rhetorically complex sustainability reports, with an emphasis on aspirations, initiatives and future commitments at the expense of frank discussion of negative impacts (Boiral, 2013; Delmas & Burbano, 2011). OECD work on misleading environmental claims confirms that vague, non specific and selectively substantiated ESG claims remain widespread, including in digital channels (OECD, 2024).

In such a context, high quality digital presentation can facilitate greenwashing in sophisticated ways. Attractive ESG dashboards may prominently feature intensity metrics that show gradual improvement, such as emissions per unit of revenue, while absolute emissions or scope 3 categories are relegated to less visible tables or left untagged. Sustainability microsites may offer rich interactive content on community projects and diversity programmes while providing minimal or highly aggregated information on supply chain risks or environmental incidents. When these materials are tagged, taxonomies can be used selectively. Preparers may comply with minimum tagging requirements but underuse more granular elements that would allow stakeholders to disaggregate impacts. The result is a high quality digital artefact that satisfies formal disclosure rules yet still presents an overly favourable sustainability narrative. The risk is that users, including regulators under resource constraints, accept digital sophistication and taxonomic compliance as proxies for substantive reliability, which can delay detection of greenwashing until external events, investigative journalism or litigation expose discrepancies.

A third set of risks arises from the interaction between high quality digital presentation and human cognitive limits. Behavioural research on disclosure shows that when individuals are confronted with very large volumes of complex information, they rely more heavily on heuristics, summary indicators and visual cues (Hirshleifer & Teoh, 2003). Digital reporting environments, especially ESG data portals and integrated financial reporting sites, can easily overwhelm users with hundreds of indicators, scenarios and narratives. Even if all information is technically available and tagged, only a fraction is actually processed. This creates an opportunity for strategic agenda setting through design. By deciding which metrics appear on landing pages, which are interactive, and which require several clicks to access, preparers can influence attention. Well designed but highly dense "data books" can also create an illusion of completeness that discourages further critical inquiry. In this sense, high quality presentation can be a vehicle for subtle framing effects that shape what users consider important, without any explicit misstatement.

These dynamics can be summarised in an expanded risk matrix that links typical features of high quality digital presentation to specific channels of potential harm.

From a regulatory and governance perspective, the central challenge is to distinguish high quality presentation that genuinely supports informed decision making from high quality presentation that primarily optimises perception. This requires oversight mechanisms that look beyond syntactic checks and visual polish. Several directions are already emerging in policy debates. First, regulators are expanding the scope of mandatory tagging to include not only primary statements but also key non GAAP measures, risk disclosures and, under CSRD, a wide range of sustainability datapoints. This reduces the scope for leaving critical information unstructured and therefore less visible to automated analysis. Second, supervisory authorities and standard setting bodies are developing guidance on the use of extensions, with an emphasis on limiting unnecessary customisation that undermines comparability. Third, some regulators and stock exchanges are starting to consider requirements that negative events, controversies and certain classes of risk be explicitly tagged or reported in standardised formats, which may constrain purely positive storytelling.

Table 2.25. High quality digital presentation: illustrative configurations and risk channels

Presentation feature	Typical configuration	Apparent quality benefits	Underlying risk channels
Interactive dashboards in annual reports	Web based interface with filters by segment, region and time, graphs linked to Inline XBRL tagged data	Improved user engagement, quick access to key indicators, machine readability	Visual emphasis on selected metrics, omission or deprioritisation of unfavourable indicators, perception bias that a professional interface implies balanced content
ESG microsites and impact portals	Dedicated sustainability website with SDG icons, story telling videos, interactive maps of projects	Perception of strong ESG focus, easy navigation by topic, alignment with global agendas	Greenwashing through selective topic emphasis, relegation of controversies, incomplete tagging of material environmental and social risks
Complex but valid XBRL tagging structures	Extensive use of extensions, broad taxonomy elements, nested dimensions under ESEF or ESRS taxonomies	Flexibility to reflect entity specifics, full technical validation, compatibility with supervisory systems	Semantic opacity, difficulty for users to understand economic meaning of tags, scope for hiding detail in aggregated elements while remaining technically compliant
Comprehensive ESG or financial data books	Long, well structured PDF or XLSX annexes with hundreds of KPIs, geographies and segments	Impression of exceptional transparency, availability of machine friendly data sets for analysts	Information overload, reliance on third party ratings instead of primary analysis, framing through selection and grouping of indicators
High production value narratives	Professionally written and designed management commentary, integrated financial and sustainability story	Enhanced readability, coherent narrative about strategy and performance	Sophisticated impression management, emphasis on strategic themes and future outlook while minimising concrete discussion of risks, uncertainties and failures

Sources: systematized by the author

At the same time, purely technical solutions cannot fully manage the risks created by high quality digital presentation. Qualitative supervision and assurance remain indispensable. Sustainability assurance under CSRD, for instance, is expected to evaluate not only data accuracy but also the completeness and balance of disclosures in light of double materiality. Independent auditors and assurance providers will need competencies in both digital reporting technologies and content analysis in order to assess whether the way data are presented, tagged and contextualised is consistent with underlying evidence. Academic and policy work on greenwashing suggests that regulators should also consider targeted thematic reviews that focus on the alignment between companies' digital ESG narratives and external data sources, such as emissions registries, litigation databases or NGO reports (OECD, 2024).

Finally, there is an educational dimension. If high quality digital presentation is to serve transparency rather than manipulation, users must have the skills to interpret both financial and ESG data critically. This includes understanding the difference between audited and unaudited information, between GAAP or IFRS measures and alternative performance indicators, and between mandatory and voluntary sustainability disclosures. Public authorities, professional bodies and academic institutions have an important role in building this literacy, particularly for small investors, civil society and journalists who increasingly rely on digital portals and dashboards rather than raw filings.

In summary, high quality digital presentation of financial and non financial reporting is a double edged phenomenon. It can significantly enhance access, comparability and analytical possibilities. At the same time, it creates new avenues for impression management, greenwashing, semantic opacity and information overload. Recognising these risks is essential for the design of digital reporting standards, supervisory tools and assurance practices that ensure that technical and visual sophistication support, rather than substitute for, genuine transparency and accountability.

4. Preventive Measures and Government Oversight Mechanisms for Digital Reporting Quality. Preventive measures and government oversight of digital reporting quality increasingly rely on a layered architecture that combines ex ante standard setting, real time validation, risk based supervision and ex post enforcement. In most jurisdictions, the first line of prevention is the design of the reporting framework itself: detailed taxonomies, tagging rules, filing manuals and data quality rules that constrain how entities prepare and submit digital reports. In the European Union, the European Single Electronic Format (ESEF) Reporting Manual issued by ESMA performs this function for listed companies, specifying mandatory use of Inline XBRL, anchoring practices for extensions and validation principles that issuers and software vendors must follow when preparing annual financial reports.

In the United States, the SEC, FASB and the XBRL US Data Quality Committee (DQC) provide a complementary set of rules and technical guidance that embed automated data quality checks directly into the U S GAAP taxonomy and into filing preparation tools, effectively operationalizing preventive control at the point of submission. Similar frameworks are emerging in other capital markets, where regulators publish binding or quasi binding technical guidance on tagging, validation and error correction for digital financial statements.

To structure these instruments analytically, it is useful to distinguish between governance of technical form, governance of semantic content and governance of operational resilience and data protection. Table 4 summarizes key preventive tools that authorities deploy at each of these levels and identifies the main quality dimensions they are intended to protect.

Table 2.26. Preventive tools for digital reporting quality and their primary quality dimensions

Level of prevention	Main tools and actors	Targeted quality dimensions
Technical form of reports	XBRL and iXBRL taxonomies, filing manuals, ESEF reporting manual, SEC EDGAR Filer Manual, automated schema and instance validation, DQC rule sets	Syntactic correctness, internal consistency, comparability across entities and periods
Semantic content of data	Supervisory guidance on tagging choices, industry specific reporting templates, pre defined analytic ratios, plausibility checks and cross statement reconciliations	Faithful representation, relevance, substantive comparability, detectability of misstatements
Operational resilience and data protection	Digital Operational Resilience Act (DORA) in the EU, guidelines on ICT and security risk management, national cyber security frameworks and incident reporting regimes	Availability, integrity and confidentiality of digital reports, continuity of access for users, resistance to cyber incidents

Sources: systematized by the author

These tools are preventive in the sense that they aim to reduce the probability of low quality or unreliable data entering official repositories. At the same time, they shape the incentives of preparers and software providers, who must internalize quality requirements into their system design and internal controls. The growing importance of operational resilience regulation, such as DORA in the European Union, confirms that digital reporting quality is now seen not only as an accounting issue but also as a component of broader ICT and cyber risk management.

Beyond standard setting, contemporary oversight relies heavily on supervisory technology (SupTech) and regulatory technology (RegTech) to embed quality control into supervisory workflows. Early analytical work by central banks showed that SupTech applications for data collection and analysis can increase the effectiveness and timeliness of supervisory reviews, while reducing manual effort and improving anomaly detection.

The Financial Stability Board has documented how authorities use SupTech tools to automatically validate digital submissions, run cross sectional outlier analyses, flag missing or inconsistent tags and integrate market and macroeconomic data to contextualize filers' financial signals. In practical terms, this means that digital reports are no longer assessed only during periodic off site reviews but are screened continuously through rules engines and machine learning models that identify statistical and logical irregularities. SupTech platforms also support dashboards that allow supervisors to rank entities by the severity and recurrence of data quality issues, enabling risk based allocation of inspection resources.

Preventive measures in this context often follow a feedback logic. Authorities first codify known problems in the form of validation rules or DQC style checks that are applied automatically at or before filing. The results are then communicated back to preparers in the form of warnings, automatic rejections or mandatory correction workflows. Over time, as new patterns of misreporting or tagging errors emerge, rule sets are updated and integrated into both official filing systems and commercial reporting software. ESMA's regular updates of the ESEF Reporting Manual, for example, explicitly aim to refine anchoring and tagging practices in response to observed weaknesses and to tighten data quality expectations for future reporting cycles.

A second pillar of preventive oversight is the integration of digital reporting quality into broader prudential and market conduct supervision. Financial supervisors increasingly treat persistent data quality weaknesses as red flags for deficiencies in governance, internal control and risk management. FSB case studies show that some authorities now incorporate metrics such as the frequency of filing errors, corrections and late submissions into their institution risk scoring frameworks, which can trigger on site inspections or targeted thematic reviews. In securities markets, supervisors use comparative analytics on digital annual reports to identify issuers whose disclosures systematically diverge from sectoral norms, for example through unusual revenue recognition patterns, leverage profiles or fair value measurements, thereby linking data quality monitoring directly to fraud and earnings management risk.

Preventive supervision also has an important soft law component that goes beyond rules and enforcement. Many regulators and stock exchanges provide preparer education, sandboxes and test environments for digital reporting, where entities can experiment with tagging and validation without legal consequences. Regulatory handbooks and Q&A documents explain common errors, best practices and interpretative expectations regarding the application of taxonomies and reporting standards. In emerging markets, international organizations such as the OECD and the World Bank support capacity building projects that help authorities design proportionate digital reporting regimes and train both supervisors and preparers, with particular attention to small and medium sized enterprises that lack internal IT resources.

Operational and cyber risk management is the third critical dimension of preventive oversight. The Digital Operational Resilience Act in the EU, together with updated guidelines of the European Banking Authority on ICT and security risk management, requires financial entities to implement robust controls over data storage, processing and transmission, to conduct regular resilience testing and to report major ICT incidents to competent authorities.

These requirements cover both internal systems and critical external service providers, including cloud platforms that host digital reporting data. Recent implementation steps under DORA, such as the designation of certain cloud and data providers as "critical" third parties, show that regulators now view the continuity and integrity of digital reporting infrastructures as a systemic issue that warrants direct oversight of technology vendors.

Table 2.27 illustrates how these operational resilience measures intersect with digital reporting quality, highlighting the channels through which ICT failures or cyber incidents can undermine the reliability and usability of financial and non financial data.

Table 2.27. Digital operational resilience and its implications for reporting quality

Regulatory focus area	Typical requirements under DORA and ICT guidelines	Implications for digital reporting quality
ICT risk management	Governance of ICT risk, asset inventories, risk assessments, control frameworks	Reduces risk of corrupted or lost reporting data, supports traceability of changes and audit trails
Incident reporting and response	Mandatory classification and reporting of ICT incidents, response and recovery plans	Enhances transparency about disruptions that may affect reporting timeliness or integrity, supports ex post validation of data gaps or anomalies
Resilience testing	Penetration tests, threat led testing of critical systems, backup and recovery drills	Provides assurance that reporting platforms can withstand attacks and recover without data loss, strengthens confidence in long term data availability
Third party risk management	Due diligence and oversight of cloud and ICT providers, contractual safeguards, concentration risk monitoring	Mitigates dependence on a small number of providers, reduces risk of systemic outages affecting multiple reporting entities simultaneously
Information sharing	Sector wide sharing of threat intelligence and vulnerabilities among authorities and entities	Enables rapid updating of preventive controls and validation rules in response to new attack patterns or fraud schemes

Sources: systematized by the author

For digital reporting quality, these measures perform a preventive function that is complementary to taxonomies and validation rules. Even perfectly tagged and validated reports lose their value if they are not available when needed, if they are compromised by unauthorized modification or if they cannot be trusted due to frequent ICT disruptions. By embedding digital reporting infrastructures within a broader operational resilience regime, governments seek to ensure that quality is sustained across the full life cycle of data, from preparation and submission to storage, analysis and public dissemination.

At the same time, the expansion of preventive and supervisory mechanisms raises important questions about proportionality, transparency and the risk of over engineering. Smaller entities may struggle to comply with complex validation schemes and ICT governance requirements, especially in low income or crisis affected countries where resources and digital skills are limited. SupTech applications that rely on opaque algorithms can introduce their own model risk, including false positives that burden compliant entities and false negatives that offer a misleading sense of security.

Finally, fragmented national approaches to digital reporting quality, particularly outside harmonized regions such as the EU, can increase compliance costs for multinational groups and limit the comparability of data across jurisdictions.

In light of these tensions, effective government oversight of digital reporting quality is increasingly framed as a dynamic balancing exercise. Authorities must design preventive measures that are rigorous enough to deter misreporting and to protect users, yet flexible enough to accommodate innovation, market diversity and differing levels of technological maturity. The most promising strategies combine clear and publicly documented data quality expectations, extensive use of automated validation and SupTech analytics, strong ICT and cyber resilience requirements, and continuous dialogue with preparers, auditors, software vendors and users of digital data. Where this balance is achieved, digital reporting can deliver its promised benefits of higher transparency, timeliness and analytical richness, while maintaining a high level of trust in the reliability of financial and non financial information.

Conclusions. Across jurisdictions, digital reporting has evolved from a technical complement to paper based disclosure into the core infrastructure for financial and non-financial transparency. Types of digital financial reporting are converging around XBRL and Inline XBRL based formats, yet important differences remain in the scope of mandatory tagging, the sophistication of validation rules and the intensity of enforcement. Non-financial reporting is moving rapidly toward similar structured digital regimes through instruments such as CSRD, ESRS and the IFRS

Sustainability Disclosure Taxonomy, which aim to bring the quality of sustainability information closer to that of traditional financial statements.

The quality of digital reporting is shaped by three interdependent elements. First, content standards and digital taxonomies define what must be reported and how it is structured. Second, internal governance at the entity level determines how carefully data are prepared, tagged, validated and protected against cyber risks. Third, preventive and supervisory mechanisms at the state level ensure that minimum quality thresholds are met and that poor practices are corrected through feedback and, if necessary, sanctions. Where these elements are coherent and mutually reinforcing, digital reporting enhances comparability, reduces information asymmetry and supports evidence based public and corporate governance. Where they are weak or fragmented, digital reports can amplify risks, obscure real performance and undermine trust. Future reforms should therefore focus on strengthening interoperability of taxonomies, aligning financial and sustainability reporting architectures, and investing in the digital competencies of preparers and supervisors so that digital reporting becomes a stable foundation for transparent and accountable economic development.

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

Conflict of interest. The author 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 author 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 author 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. Accountancy Europe. (2021). *Response to the European Commission consultation on strengthening the quality of corporate reporting and its enforcement* [Position paper]. https://accountancyeurope.eu/wp-content/uploads/2022/12/Accountancy_Europe_response_to-_EC_corporate_reporting_quality-enforcement_2021.pdf
2. Alles, M., & Gray, G. L. (2012). The pros and cons of XBRL adoption in Greece. *International Journal of Economics and Business Administration, 1*(1), 91–106. https://ideas.repec.org/a/tei/journl/v1y2012i1p91-106.html
3. Bonsón, E., Cortijo, V., & Escobar, T. (2009). Towards the global adoption of XBRL using International Financial Reporting Standards (IFRS). *International Journal of*

Accounting Information Systems, 10(1), 46–60. https://doi.org/10.1016/j.accinf.2008.10.002

4. Brookings Institution. (2024). *Ukraine: Digital resilience in a time of war*. Brookings. https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf
5. Deloitte. (2024). *Artificial intelligence in finance and accounting: From automation to augmentation* [Report]. Deloitte Insights. https://www2.deloitte.com
6. EFRAG. (2023). *European Sustainability Reporting Standards (ESRS) – Set 1* [Standards]. European Financial Reporting Advisory Group. https://xbrl.efrag.org/e-esrs/esrs-set1-2023.html
7. European Commission. (2022). *Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 as regards corporate sustainability reporting (Corporate Sustainability Reporting Directive)*. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2464/oj
8. European Securities and Markets Authority. (2017). *European Single Electronic Format (ESEF) Reporting Manual*(ESMA32-60-254). ESMA. https://www.esma.europa.eu/document/esef-reporting-manual
9. European Securities and Markets Authority. (2025). *ESEF Reporting Manual – Preparation of annual financial reports in ESEF format (Update October 2025)* (ESMA32-60-254 Rev). ESMA. https://www.esma.europa.eu/sites/default/files/library/esma32-60-254_esef_reporting_manual.pdf
10. FASB. (2023). *US GAAP Financial Reporting Taxonomy – 2023 release*. Financial Accounting Standards Board. https://www.fasb.org/page/PageContent?pageId=1.1.10
11. Global Reporting Initiative. (2021). *GRI 1: Foundation 2021; GRI 2: General Disclosures 2021; GRI 3: Material Topics 2021 (Universal Standards)*. GRI. https://www.globalreporting.org/standards/standards-development/universal-standards/
12. ICAEW. (2024). *How standards can help squash the greenwash*. Institute of Chartered Accountants in England and Wales. https://www.icaew.com/insights/viewpoints-on-the-news/2024/sep-2024/how-standards-can-help-squash-the-greenwash
13. IFRS Foundation. (2020). *IFRS Taxonomy 2020 – Illustrated*. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs-taxonomy/
14. IFRS Foundation. (2023). *IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information; IFRS S2 Climate-related Disclosures*. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs-sustainability-standards
15. IOSCO. (2021). *Environmental, social and governance (ESG) ratings and data providers: Final report*. International Organization of Securities Commissions. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD690.pdf
16. Key ESG. (2023). *Building a sustainable future: A practical guide to ESG reporting and carbon accounting for infrastructure investors*. KEY ESG. https://www.keyesg.com/article/building-a-sustainable-future-a-practical-guide-to-esg-reporting-and-carbon-accounting-for-infrastructure-investors

17. OECD. (2011). *Regulatory policy and governance: Supporting economic growth and serving the public interest*. OECD Publishing. https://doi.org/10.1787/9789264116573-en
18. OECD. (2024). *OECD Digital Economy Outlook 2024, Volume 2: Strengthening connectivity, innovation and trust*. OECD Publishing. https://doi.org/10.1787/3adf705b-en
19. PwC. (2022). *Strengthening the quality of corporate reporting and its enforcement: PwC response to the European Commission consultation* [Submission]. PricewaterhouseCoopers. https://www.pwc.com/gx/en/about/assets/response-corporate-reporting-improving-its-quality-and-enforcement-2022.pdf
20. U.S. Securities and Exchange Commission. (2018). *Inline XBRL filing of tagged data* (Release No. 33-10514; 34-83551; IC-33148). U.S. SEC. https://www.sec.gov/rules/final/2018/33-10514.pdf
21. Valentinetti, D., & Rea, M. A. (2013). XBRL for financial reporting: Evidence on Italian GAAP. *International Journal of Accounting Information Systems, 14*(1), 45–63. https://doi.org/10.1016/j.accinf.2012.09.001
22. XBRL International. (2024). *About XBRL: Improving business reporting*. XBRL International. https://www.xbrl.org/the-standard/what/an-overview-of-xbrl/
23. XBRL US. (2022). *Data Quality Committee (DQC) rules and guidance*. XBRL US. https://xbrl.us/data-quality/rules-guidance/

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

Chapter 3
Public Administration in the Architecture of Security: National, Economic, and Energy Policy Contexts

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

Section 3.1. The Role and Significance of Public Administration in the System of Ensuring National Security of EU Countries Against the Background of a Full-Scale Invasion of Ukraine

Julian Maj[1], Tomasz Gorski[2], Paulina Kolisnichenko[3]

[1]Gen. dyw. Professor. Dr. Hab., Rector, WSHIU University, Poznan, Poland, ORCID: https://orcid.org/0009-0007-5517-0217

[2]Mgr., WSHIU University, Poznan, Poland, ORCID: https://orcid.org/0009-0001-3343-9672

[3]Ph.D. in Economics, Vice Rector for International Cooperation, WSHIU University, Poznan, Poland, ORCID: https://orcid.org/0000-0001-6730-1236

Citation:

Maj, Ju., Gorski, T. & Kolisnichenko, P. (2025). The Role and Significance of Public Administration in the System of Ensuring National Security of EU Countries Against the Background of a Full-Scale Invasion of Ukraine. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 155-181). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-155-181

Abstract. *Russia's full-scale invasion of Ukraine has reshaped how European Union countries conceptualize national security by demonstrating that high-intensity war can rapidly cascade into disruptions of governance, markets, energy supply, critical infrastructure, and social stability. In this context, public administration functions as the institutional core that converts political commitments into coordinated procedures, lawful emergency regimes, and implementable programs capable of sustaining continuity of government and public trust. The study argues that, under wartime conditions, the effectiveness of national security responses depends on governance quality, especially interagency coordination, legal robustness, resource mobilization, procurement integrity, and accountability. Methodologically, the research combines conceptual analysis of EU security and resilience policy shifts with a comparative generalization of national administrative solutions across defence support, energy governance, cybersecurity, information resilience, and humanitarian management. The findings show that EU-level instruments provide a shared strategic and regulatory architecture, while national administrations act as the execution layer by translating common priorities into planning routines, crisis coordination protocols, regulatory enforcement, and reporting systems. Energy security governance is reframed through accelerated diversification and clean energy deployment, cybersecurity is strengthened through stricter supervisory and incident-reporting requirements, and humanitarian protection evolves from short-term crisis response toward long-term service delivery and integration capacity at central and local levels. Overall, the wartime security performance in the EU is increasingly determined not only by available resources, but by administrative capacity to deliver rapid action while preserving legality, democratic oversight, and societal cohesion.*

Keywords: *public administration; national security; European Union; war-induced transformation; strategic resilience; energy security; clean energy transition; cybersecurity governance; critical infrastructure; information resilience; crisis coordination; temporary protection.*

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

1. Characteristics of the essence and significance of public administration in the system of ensuring national security. Russia's full-scale invasion of Ukraine became a turning point for security thinking in the European Union because it revealed how rapidly armed conflict can cascade into disruptions of governance, markets, and social stability (Sytnyk, 2011; Pilko, 2014). This experience strengthened a broader understanding of national security as a multidimensional condition of protection that includes not only defence, but also the continuity of public institutions, the functioning of critical infrastructure, the stability of energy supply, cybersecurity, information integrity, and the capacity of society to sustain cohesion under pressure (Yarova & Mishenin, 2019; Dumchykov et al., 2022). In such conditions, public administration becomes the institutional core of security because it is responsible for converting political decisions into executable mechanisms through law, procedures, budgets, procurement, staffing, oversight, and interagency coordination (Bielai et al., 2024; Bielai et al., 2021). The significance of this role lies in the fact that security outcomes are produced not by declarations, but by implementation systems that can mobilize resources rapidly while preserving legality, accountability, and predictability, which are essential for public trust (Prav, 2021; OECD, 2022).

From an analytical perspective, public administration in the national security system can be conceptualized as an integrated cycle of governance that begins with risk identification and priority-setting, continues through regulatory design and allocation of resources, and ends with monitoring, evaluation, and institutional learning. This cycle is security-relevant because modern threats are complex and interdependent, meaning that failure in one domain, such as energy or information, can undermine defence readiness and social order. Therefore, public administration must ensure coherence among ministries, regulators, local governments, and public service providers, while also building stable channels of cooperation with critical private operators in energy, communications, transport, and finance (Kryshtanovych et al., 2022; Kupchak et al., 2023). A key implication is that national security increasingly depends on governance quality, including integrity in spending, clarity of responsibility, reliability of services, and transparent communication with citizens, because legitimacy conditions society's willingness to comply and cooperate during prolonged crises (Sytnyk, 2011; OECD, 2022).

The European context intensifies these requirements because security governance is multilevel. EU institutions establish shared priorities and binding standards, while Member States carry the main responsibility for implementation through domestic administrative systems. The Strategic

Compass for Security and Defence illustrates the logic of “security through governance capacity” because it sets out a large set of concrete actions, but their real effect depends on whether Member States can translate them into planning routines, procurement decisions, training systems, crisis coordination protocols, and accountability procedures (European External Action Service, 2022).

Similarly, long-term support for Ukraine has required legally robust and administratively manageable financing frameworks, which reinforces the role of public administration as a guarantor of continuity, compliance, and credibility in security policy (European Union, 2024).

To make the governance contribution of public administration more explicit, Table 3.1 structures the main national security domains and the administrative functions that operationalize resilience across the state, economy, and society.

Table 3.1. Public administration functions across key national security domains

Security domain	Core challenge under crisis conditions	Public administration functions	Security-relevant implementation outputs
Defence and civil protection	rapid escalation; mobilisation; continuity of command	strategic planning; mobilisation governance; procurement and logistics; interagency command routines	readiness and sustainment; lawful emergency measures; operational continuity
Critical infrastructure	cascading failures across energy, transport, telecom, water	identification of critical entities; national risk assessments; resilience requirements; inspections	continuity of essential services; reduced downtime; faster recovery capacity
Cybersecurity	systemic cyber incidents; supply-chain vulnerabilities	mandatory risk management; incident reporting; supervisory enforcement	faster detection and response; shared situational awareness; reduced systemic exposure
Information integrity	disinformation; foreign information manipulation; trust erosion	strategic communication; transparency; coordination with platforms and media	reduced panic and polarization; higher compliance; legitimacy maintenance
Energy security	price shocks; supply disruption; external dependence	diversification policy; investment prioritisation; emergency pricing instruments	improved supply stability; reduced dependency; predictable transition pathways
Social cohesion and humanitarian stability	displacement; inequality pressure; service overload	service continuity; local coordination; social protection delivery	sustained access to services; reduced social fragmentation; social endurance

Source: systematized by the authors

https://doi.org/10.36690/PUBADM

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

The Table 3.1 shows that public administration is not merely supportive to security policy. It is the operational architecture through which security is produced, because it integrates rules, resources, coordination, and oversight into functioning capacities (Bielai et al., 2024; Kryshtanovych et al., 2022).

A defining feature of the post-2022 environment is the regulatory institutionalization of resilience, which makes administrative capacity a measurable determinant of security outcomes. Cybersecurity governance in the EU is strengthened by Directive (EU) 2022/2555 (NIS2), which expands the scope of covered entities and reinforces obligations regarding risk management, incident reporting, and supervision, thereby turning compliance and enforcement into core resilience mechanisms (European Union, 2022; Dumchykov et al., 2022).

The resilience of critical entities is similarly institutionalized by Directive (EU) 2022/2557, which requires Member States to identify critical entities, conduct risk assessments, and support resilience measures across key sectors (European Union, 2022).

In practical governance terms, these instruments require professional regulators, clear institutional mandates, interoperable reporting systems, and enforcement capacity. Without these administrative conditions, legal frameworks remain formal and do not produce real reductions in vulnerability.

Public trust is another security variable that public administration shapes directly. Crisis governance depends on trust because citizens and businesses must follow guidance, accept temporary restrictions or economic costs, and cooperate with public authorities. OECD research conceptualizes trust in government through five drivers, namely reliability, responsiveness, integrity, openness, and fairness, which can be translated into specific administrative practices relevant to security governance (OECD, 2022).

This is consistent with Ukrainian and comparative scholarship that links security effectiveness to legitimacy, accountability, and the coherence of institutional action, especially under conditions of uncertainty and stress (Sytnyk, 2011; Prav, 2021). For this reason, security-relevant public administration must combine speed with legal correctness and transparent justification, because rapid but opaque decisions can undermine trust and reduce compliance, which ultimately weakens resilience.

Because multilevel governance is central for EU security, Table 3.2 links key EU instruments to the concrete administrative requirements they impose at the national and local levels.

Table 3.2. EU security-related instruments and core implementation requirements for public administration

EU instrument	Security objective	Administrative requirements for implementation	Typical coordination level
Strategic Compass for Security and Defence	improve EU capacity to act; strengthen resilience and capabilities	national planning alignment; procurement governance; training routines; reporting and accountability	EU level guidance with national execution (European External Action Service, 2022)
NIS2 Directive (Directive (EU) 2022/2555)	high common level of cybersecurity	supervisory authorities; compliance monitoring; incident reporting systems; risk management enforcement	national regulators with cross-border cooperation (European Union, 2022)
Critical Entities Resilience Directive (Directive (EU) 2022/2557)	resilience of critical entities	national risk assessments; identification of critical entities; resilience support and oversight	national and local implementation with sector operators (European Union, 2022)
Temporary Protection activation for Ukraine	rapid humanitarian protection and service access	registration systems; service delivery capacity; central-local coordination; integration mechanisms	EU decision with national-local service delivery (European Commission, 2025)
REPowerEU	reduce dependence on Russian fossil fuels; accelerate transition	investment programming; permitting and coordination; energy savings policies; market regulation	EU framework with national implementation (European Commission, 2022)
Ukraine Facility (Regulation (EU) 2024/792)	predictable financial support and policy continuity	fiscal governance; monitoring and reporting; accountability for funds	EU funding framework with national coordination (European Union, 2024)

Source: systematized by the authors

The Table 3.2 highlights that EU security policy depends on national administrative capacity as the final production stage of resilience. In effect, Member States' public administrations serve as the execution layer of EU-level security commitments, which makes managerial coherence and institutional discipline strategically important.

Digital transformation and AI-enabled tools are increasingly relevant within this governance architecture, especially for early warning, anomaly detection in cyber incidents, and analysis of large-scale information environments. Yet the security value of these tools is mediated by governance conditions, including lawful data management, clear rules of use, professional competence, and accountability for decisions, because technology can amplify errors, bias, or misuse if institutional safeguards are weak (Bielai et al., 2024; OECD, 2022). This is why security research increasingly treats digital instruments as supportive components within a broader administrative system, rather than as substitutes for governance capacity and legitimacy.

Finally, the formation of long-term state capacity is a distinct security function of public administration in wartime conditions. It includes the ability to sustain institutions over time, prevent institutional exhaustion, and maintain social cooperation through consistent and transparent communication. UNDP frameworks on crisis response and governance resilience emphasize strengthening core government functions, accountability, inclusion, and service delivery under crisis conditions, which directly corresponds to the security needs observed in Europe after 2022 (UNDP, 2022).

In synthesis, public administration should be interpreted as the institutional core of national security because it integrates strategic leadership with implementation discipline, interagency coordination, legal robustness, transparent resource use, democratic control, and trust-preserving communication, which together determine whether a country can withstand pressure and recover without losing legitimacy (Sytnyk, 2011; Bielai et al., 2024; OECD, 2022).

2. The impact of Russia's full-scale invasion of Ukraine on national security agendas in EU countries and on public administration systems. Russia's full-scale invasion of Ukraine reintroduced high-intensity interstate war to Europe and, in doing so, forced EU countries to reconsider national security as a multidimensional governance problem rather than a narrowly military one. The central analytical shift is that threats are now treated as systemic and cross-sectoral, combining kinetic risks with coercion through energy, cyber operations, critical infrastructure disruption, and foreign information manipulation. As a result, public administration moved from predominantly planned security governance toward crisis-capable governance, where speed of coordination, lawful emergency decision-making, and sustained implementation capacity under uncertainty became decisive. In this setting, national security is increasingly operationalized as continuity of government, resilience of critical functions, and societal stability, including the ability to maintain legitimacy and trust while managing prolonged shocks (Sytnyk, 2011; Bielai et al., 2024; OECD, 2024). This transformation was reinforced at EU level through a more explicit security and defence agenda, including a structured set of capability and coordination priorities under the Strategic Compass adopted in March 2022 (European External Action Service [EEAS], 2022). Consequently, the war has not only expanded what counts as "security," but also tightened the coupling between supranational instruments and national administrative routines, especially in defence support, energy governance, cybersecurity regulation, and migration management (European Commission, 2025a, 2025b).

Table 3.3 summarizes how the war accelerated a transition from programmatic, medium-term security management to a crisis-oriented governance mode focused on continuity, resilience, and adaptive implementation.

Table 3.3. Administrative transformation of security governance in EU countries after February 2022

Dimension	Pre-2022 dominant pattern	Post-2022 dominant pattern	Core administrative implication
Threat model	Predominantly risk-based and compartmentalized	Systemic, cross-domain, and hybrid	Whole-of-government coordination becomes routine
Planning logic	Multi-year sector strategies, incremental reform	Crisis planning, rapid reprioritization, stress testing	Faster decision cycles and stronger executive coordination
Instruments	Standard regulation and budget programs	Emergency measures plus accelerated regulatory packages	Legal design must enable speed without eroding accountability
Resource governance	Stable allocations, gradual procurement	Surge spending, urgent procurement, logistics scaling	Integrity controls and transparency requirements intensify
Public legitimacy	Policy performance mainly evaluated in “normal times”	Trust and cohesion become security variables	Communication capacity and service continuity gain security value

Source: systematized by the authors

The key point is that the administrative “success condition” shifts from policy elegance to operational reliability: the ability to keep essential functions running, mobilize resources, and coordinate across sectors without losing legality and public confidence (OECD, 2024; Bielai et al., 2024).

EU-level responses translated these shifts into concrete governance requirements. The Strategic Compass signaled a more structured capability agenda and a stronger expectation of coordinated implementation across Member States (EEAS, 2022). In parallel, EU military assistance mechanisms created practical administrative workloads inside Member States, including procurement governance, training pipelines, logistics coordination, auditability, and reporting. A central financial instrument is the European Peace Facility (EPF), through which the EU has mobilized substantial support to strengthen Ukraine’s defence capacity, while requiring standardized administrative procedures for costs, accountability, and conditionality (Council of the European Union, 2022a, 2024a). The EU Military Assistance Mission in support of Ukraine (EUMAM) similarly institutionalized training support and introduced common-cost financing and equipment provisions that depend on interoperable administrative routines and budget discipline across national systems (Council of the European Union, 2025a). In other words, the war made security cooperation "administratively real," not only politically declared, and this reality pushed national public administrations toward higher implementation maturity.

Table 3.4 maps the most consequential EU-level instruments to the administrative functions they require at national level, showing why the war increased the interdependence of supranational policy and domestic implementation capacity.

Table 3.4. EU security instruments activated or strengthened after 2022 and their administrative implications

EU instrument	Security purpose	What it requires from national public administration
Strategic Compass (2022)	Common priorities for security and defence action	Faster planning cycles, capability governance, coordinated implementation (EEAS, 2022)
European Peace Facility (EPF)	Financing military support measures	Procurement integrity, financial control, reporting, audit trails (Council of the European Union, 2022a, 2024a)
EUMAM Ukraine	Training coordination and common-cost financing	Training governance, logistics, standardized reporting and budgeting (Council of the European Union, 2025a)
REPowerEU (2022) and the 2025 roadmap to end dependency	Energy security through diversification, savings, clean transition, and phase-out of Russian energy	Rapid regulatory change, infrastructure permitting, targeted support, market monitoring (Council of the European Union, 2022b; European Commission, 2025b)
NIS2 (Directive (EU) 2022/2555)	Higher common level of cybersecurity across critical sectors	National strategies, supervision, incident reporting, cross-border cooperation (European Commission, 2022; EUR-Lex, 2022)
Critical Entities Resilience (Directive (EU) 2022/2557)	Physical resilience of essential services	Risk assessments, resilience planning, supervision of critical entities (EUR-Lex, 2023)
Temporary Protection (activated 2022; extended)	Large-scale protection framework for displaced persons	Long-term service coordination, funding transparency, local capacity scaling (Council of the European Union, 2024b)

Source: systematized by the authors

The administrative burden of these instruments is not a side effect, it is the mechanism of effectiveness: EU commitments matter to the extent that national administrations can convert them into procurements, permits, oversight, service delivery, and credible reporting (Council of the European Union, 2022a, 2025a; European Commission, 2025b).

Energy security became one of the most immediate bridges between external war risk and internal governance stability. REPowerEU framed energy dependence as a security vulnerability and linked diversification, energy savings, and accelerated clean energy deployment to resilience objectives (Council of the European Union, 2022b; European Commission, 2025a). The governance consequence is that energy policy now functions as part of national security management, which forces public administrations to manage trade-offs among security, affordability, and competitiveness. The European Commission's 2025 roadmap to fully end EU dependency on Russian energy, including a stated goal of stopping all imports of Russian gas by the end of 2027 and restricting spot contracts by the end of 2025, illustrates how a security threat is translated into staged regulatory and monitoring requirements that must be executed domestically (European Commission, 2025b). These dynamics also reshape industrial policy and budget design, because infrastructure investment, market regulation, and targeted household support become elements of one security loop where administrative error can trigger both economic and security effects.

Table 3.5 consolidates the core national-security components that became tightly coupled after 2022 and specifies the corresponding responsibilities of public administration.

Table 3.5. Public administration roles across security domains under wartime-related shocks

Security component	Core public administration responsibilities	Illustrative instruments and routines
Defence and military security	Strategic planning, procurement legality, readiness coordination, democratic oversight	Capability roadmaps, procurement governance, civil protection coordination (EEAS, 2022; Bielai et al., 2021)
Energy security and economic resilience	Dependency reduction, infrastructure investment, crisis buffers, affordability safeguards	Diversification, strategic reserves, emergency demand measures, targeted compensation (Council of the European Union, 2022b; European Commission, 2025b)
Cybersecurity and infrastructure protection	Mandatory standards, supervision, incident response capacity, cross-border coordination	NIS2 risk management, reporting regimes, national CSIRTs, audits (European Commission, 2022; EUR-Lex, 2022)
Physical resilience of essential services	Risk assessment, continuity planning, oversight of critical entities	CER-based resilience plans, stress testing, supervision (EUR-Lex, 2023)
Information security and societal resilience	Countering manipulation, strategic communication, trust maintenance, cohesion policies	FIMI response coordination, public communication routines, media literacy support (EEAS, 2025; OECD, 2024)
Humanitarian and migration governance	Protection regimes, service capacity scaling, local coordination, long-term integration	Temporary protection implementation, education and health capacity planning (Council of the European Union, 2024b)

Source: systematized by the authors

The Table 3.5 underscores that the modern security problem is administrative integration: outcomes depend on whether governments can connect legal authority, resources, and delivery capacity across domains, while sustaining legitimacy and trust (Sytnyk, 2011; OECD, 2024).

Cybersecurity and critical infrastructure protection became especially salient because hybrid pressure exploits both digital and physical vulnerabilities. NIS2 strengthens requirements for cybersecurity risk management, incident reporting, supervision, and cross-border cooperation across critical sectors, which compels Member States to adjust institutional architectures, allocate enforcement capacity, and standardize interaction with private operators of essential services (European Commission, 2022; EUR-Lex, 2022). In parallel, the Critical Entities Resilience framework targets physical resilience and continuity of essential services, pushing administrations to institutionalize risk assessments, resilience planning, and oversight (EUR-Lex, 2023). The information environment constitutes another security field, where the EU conceptualizes foreign information manipulation and interference (FIMI) as a pattern of coordinated behavior that can harm democratic processes and societal cohesion, thus requiring structured public-sector responses that combine communication capacity with legal safeguards (EEAS, 2025). While data-driven tools, including AI-enabled analytics, can strengthen early warning and anomaly detection, their governance value depends on data quality, clear mandates, accountability, and rights-respecting oversight, which returns the analysis to the centrality of public administration capacity rather than technology alone (Yemanov et al., 2022; OECD, 2023).

Table 3.6 presents governance trade-offs that became sharper after 2022 and proposes administratively measurable indicators for managing them in a lawful, trust-preserving way.

Table 3.6. Governance trade-offs in EU security management after 2022 and suggested administrative indicators

Trade-off	Why it intensified after 2022	Practical indicators for monitoring
Speed vs legality	Crisis pressure demands rapid action under legal constraints	Time-to-decision; share of emergency acts reviewed ex post; audit findings
Secrecy vs transparency	Defence and security spending rose, public demand for integrity increased	Procurement transparency rate; conflict-of-interest checks; reporting completeness
Central control vs local delivery	Refugee support and resilience depend on municipalities	Funding flow time; service capacity utilization; local implementation variance
Security vs affordability	Energy shocks raise social sensitivity and political risk	Targeting accuracy of support; energy poverty proxies; price volatility measures
Innovation vs accountability	AI and digital tools expand capability but create rights and bias risks	Data governance compliance; model documentation coverage; incident rates

Source: systematized by the authors

These indicators operationalize the core claim: resilience is not only a matter of resources, but of governable processes that preserve legality, effectiveness, and public trust under stress (Bielai et al., 2024; OECD, 2024).

Finally, the humanitarian dimension created long-horizon governance demands that affect internal stability. The activation and extension of temporary protection for people fleeing the war required Member States to scale education, health care, housing, and labor-market access, shifting governance from short-term emergency response to sustained integration policy with strong central-local coordination and predictable financing (Council of the European Union, 2024b). From a national security perspective, this becomes a question of societal resilience, because integration capacity influences cohesion and trust, which are now treated as security-relevant variables (OECD, 2024). In aggregate, the war's impact is best understood as a multivector transformation in which security becomes a cross-cutting category of public administration. The effectiveness of EU countries increasingly depends on whether administrations can combine rapid action with legal correctness, interagency coordination, transparent resource use, and credible communication, thereby maintaining trust while implementing long-term adaptation to a durable security shock (Sytnyk, 2011; Bielai et al., 2024; European Commission, 2025b).

3. Multilevel governance of national security in the EU: coordination architecture, implementation mechanisms, and accountability. Russia's full-scale invasion of Ukraine made multilevel governance a practical condition of security management in the European Union because strategic direction, regulatory frameworks, and financing are increasingly shaped at the EU level, while operational capacity is delivered through national, regional, and local administrations. In this architecture, the EU contributes coordination instruments that enable collective action under cross-border pressure, whereas Member States retain primary responsibility for national security and translate shared priorities into budgets, procurement, enforcement, and service delivery. The war strengthened the demand for fast, interoperable procedures because defence support, sanctions enforcement, energy diversification, cyber resilience, critical infrastructure protection, and humanitarian governance must now be managed simultaneously and over a prolonged period (Council of the European Union, 2022; European Commission, 2022). As a result, the effectiveness of security policy depends less on isolated sectoral decisions and more on the quality of administrative interfaces, including who decides, who implements, how information moves, and how accountability is preserved during emergency governance.

https://doi.org/10.36690/PUBADM

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

At the EU level, multilevel coordination operates through strategic and operational mechanisms that reduce fragmentation in crisis response. The Strategic Compass institutionalized a common set of capability priorities and implementation actions, thereby increasing expectations that national administrations will align planning cycles, readiness targets, and procurement governance with shared commitments (Council of the European Union, 2022). In crisis coordination, the Integrated Political Crisis Response arrangements support rapid political decision-making and scaling of coordination across institutions when crises are major and complex (Council of the European Union, 2024a). In parallel, the EU Civil Protection Mechanism, through the Emergency Response Coordination Centre, coordinates assistance delivery and links national civil protection authorities to an EU-level operational hub, which is increasingly relevant when security shocks generate cascading impacts across infrastructure and society (European Commission, 2025a). These instruments do not replace national authority, but they reshape national administrative routines by increasing the need for standardized reporting, joint situational awareness, and disciplined implementation.

At the national level, multilevel governance transforms security management from a predominantly ministerial model into a whole-of-government system. Defence and security decisions increasingly require integrated policy design that links capability development, procurement integrity, industrial policy, and social resilience, which raises the importance of interministerial coordination bodies and legally robust emergency instruments. The governance burden intensifies where implementation depends on public-private interfaces, for example in energy markets and critical infrastructure, because operators of essential services must comply with regulatory obligations, share incident information, and participate in stress testing and continuity planning. In energy governance, EU-level market integration and security objectives are reinforced by bodies such as ACER, which supports coordination across national regulators and contributes to integrated market functioning, thus shaping national regulatory practice and cross-border coordination (European Union, 2025). In addition, humanitarian governance has become structurally long-term through the EU temporary protection framework for persons fleeing Ukraine, which requires sustained coordination across central and local levels in education, health, housing, and labour markets (Council of the European Union, 2022a).

Table 3.7 summarizes how responsibilities are distributed across governance levels and where coordination interfaces are most decisive for reliable implementation during prolonged crisis conditions.

Table 3.7. Multilevel governance roles in the national security system of EU countries

Governance level	Primary security responsibilities	Core coordination interfaces	Typical implementation risks
EU level	Strategic coordination; common legal frameworks; financial instruments; cross-border alignment	Standardized reporting; interoperability requirements; conditionality and auditability	Policy coherence without operational capacity; uneven national uptake
National level	Strategy and budgeting; defence procurement; regulation; national crisis management	Interministerial coordination; regulator-government cooperation; public-private coordination	Fragmented mandates; procurement bottlenecks; weak integrity controls
Regional level	Territorial resilience; civil protection coordination; continuity planning for infrastructure and services	Vertical coordination with ministries; regional emergency planning; escalation procedures	Unequal capacity; inconsistent procedures; delayed escalation
Local level	Frontline service delivery; community resilience; integration of displaced persons; trust maintenance	Municipal coordination with national agencies; data exchange; crisis communication	Resource overload; service deterioration; legitimacy erosion

Source: systematized by the authors

The distribution of roles indicates that security effectiveness depends on governance connectivity across levels. When interfaces are institutionalized and responsibilities are clear, multilevel governance strengthens resilience; when coordination is ad hoc, the same structure increases delays and accountability gaps (Council of the European Union, 2024a; European Commission, 2025a).

Multilevel governance also requires explicit accountability design, because accelerated action increases the risk of procedural shortcuts in procurement, subsidy allocation, and emergency regulation. In practice, accountability is maintained through auditability requirements, reporting regimes, parliamentary scrutiny, and performance monitoring tied to EU instruments and national budgets. The war exposed a core administrative dilemma: speed is operationally necessary, but legitimacy and sustainability require legal correctness, transparent criteria for resource allocation, and documented decision chains that remain reviewable after the crisis phase. Therefore, multilevel governance should be treated as an administrative capability, not only a constitutional arrangement, because it demands professional competence in coordination, compliance, financial management, and communication under high uncertainty (Bielai et al., 2024; Prav, 2021).

Table 3.8 systematizes the most common implementation mechanisms through which EU-level security priorities become national administrative action, and it highlights the accountability instruments that prevent governance degradation under emergency pressure.

Table 3.8. Implementation mechanisms and accountability instruments in EU multilevel security governance

Mechanism type	EU-level instruments and examples	National administrative translation	Accountability and control levers
Strategic coordination	Strategic Compass; crisis coordination tools such as IPCR	Alignment of national strategies, readiness plans, and crisis governance routines	Parliamentary scrutiny; public reporting; ex post evaluation of implementation
Legal harmonization	Directives and regulations in cyber and infrastructure resilience	Transposition, enforcement mandates, supervision models, sanctioning regimes	Compliance monitoring; regulator audits; judicial review
Financial instruments	Funding streams linked to energy transition and resilience measures	Program design, procurement, subsidy schemes, infrastructure permitting	Audit trails; anti-fraud controls; performance indicators
Operational coordination	EU Civil Protection Mechanism and ERCC coordination	National civil protection integration; interoperability in response and logistics	After-action reviews; interoperability testing; continuity audits
Humanitarian governance	Temporary protection framework for displaced persons from Ukraine	Service delivery coordination across local budgets, schools, health systems	Monitoring of service outcomes; social cohesion indicators; fiscal transparency

Source: systematized by the authors

Multilevel governance becomes credible when implementation mechanisms are paired with accountability instruments that preserve legality, transparency, and learning. Without these safeguards, resource intensity increases while public trust and policy sustainability decline, which directly weakens national resilience (Sytnyk, 2011; Bielai et al., 2021).

4. Digital transformation and AI-enabled tools in public administration for national security: opportunities, constraints, and governance safeguards. The war accelerated digital transformation in EU public administrations because contemporary threats operate at high speed and often target data-intensive systems, including cyber infrastructure, energy networks, logistics chains, and the information environment. Digital governance improves security when it strengthens situational awareness, enables coordinated response, and protects continuity of essential services. However, digitalization also creates new dependencies, including reliance on interoperable registers, platform availability, and secure communications, which must be treated as critical governance assets. The decisive factor is governance quality, because technology amplifies both competence and errors, especially under crisis pressure (Bielai et al., 2024; Yemanov et al., 2022).

In cybersecurity governance, EU requirements increasingly shape national administrative design through harmonized obligations and supervision expectations. The NIS2 Directive strengthens requirements for risk management measures and incident reporting across sectors and obliges Member States to build enforcement capacity, supervisory practice, and coordinated national frameworks (European Union, 2022a). In parallel, the Critical Entities Resilience Directive extends resilience governance beyond cyber issues to include risk assessment, continuity planning, and supervision for critical entities that provide essential services, thereby reinforcing an integrated approach to security and continuity (European Union, 2022b). For public administration, these frameworks imply a shift from voluntary guidance to enforceable compliance, where authorities must establish clear mandates, audit capability, and consistent procedures for information sharing with operators of essential services.

In the information domain, digital governance intersects with democratic resilience because foreign information manipulation and disinformation campaigns influence trust, compliance, and social cohesion during prolonged crises. Public administrations increasingly operationalize information security through strategic communication units, rapid rebuttal coordination, and partnerships with media and platforms within legal constraints. The Digital Services Act reinforces platform responsibilities for systemic risk management and transparency, which indirectly affects public governance by creating new cooperation and oversight dynamics in areas linked to information integrity and risk mitigation (European Union, 2022c). Yet, state action must remain rights-respecting because overreach in content governance can undermine legitimacy, which is a core component of resilience (Pilko, 2014; Prav, 2021).

AI-enabled tools can strengthen national security governance, but only if they are governed as accountable public-sector capabilities. The EU AI Act establishes a risk-based approach to AI, with stricter obligations for high-risk uses, which is particularly relevant where AI may influence security-sensitive decisions or affect fundamental rights (European Union, 2024). In practical terms, AI is most defensible in public administration when it supports decision preparation rather than replacing accountable decision-makers, and when it is embedded in clear procedures, validated data pipelines, audit trails, and human review, especially in high-stakes contexts.

Table 3.9 groups core AI-related use cases in security governance and links them to administrative prerequisites and safeguards that preserve legality and trust.

Table 3.9. AI-enabled use cases in public administration for national security and required safeguards

Use case	Security value	Administrative prerequisites	Core safeguards
Cyber anomaly detection	Faster detection and triage of incidents	Standardized reporting; trained analysts; interoperable data flows	Audit logs; model validation; clear escalation procedures (European Union, 2022a)
Disinformation monitoring	Earlier identification of coordinated influence patterns	Strategic communication capacity; interagency coordination; lawful data access	Transparency rules; human review; rights protections (European Union, 2022c)
Critical infrastructure risk analytics	Prioritization of protective measures and continuity planning	Risk registers; cooperation with operators; scenario planning	Data governance; accountability for decisions; stress testing (European Union, 2022b)
Crisis logistics and resource allocation	Reduced bottlenecks and faster distribution of assistance	Integrated supply data; procurement analytics; coordination routines	Integrity controls; anti-corruption checks; explainability for high-stakes decisions (Bielai et al., 2021)

Source: systematized by the authors

AI contributes to security only when it is governed through clear mandates, validated processes, and accountable decision chains. In crisis conditions, safeguards are not barriers to speed; they are the conditions for durable effectiveness and legitimacy (European Union, 2024; Bielai et al., 2024).

Digital transformation also changes the institutional logic of crisis response, because it increases the value of interoperability and disciplined information exchange between levels of government. This is visible in the practical need to link national decision centres with regional and municipal service delivery, particularly in humanitarian governance under temporary protection, where registries, benefits administration, school placement, and labour market integration require reliable data flows and secure processing (Council of the European Union, 2022a). At the same time, digital systems raise continuity risks, so public administrations must integrate continuity planning, vendor and procurement integrity controls, and cybersecurity obligations into routine governance, rather than treating them as emergency-only tasks (Bielai et al., 2021; Dumchykov et al., 2022).

Table 3.10 outlines typical governance risks created or amplified by digitalization and identifies administrative mitigations aligned with EU legal frameworks.

https://doi.org/10.36690/PUBADM

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

Table 3.10. Digital governance risks in national security administration and mitigation measures

Risk category	How it weakens security governance	Administrative mitigation	Normative anchor
Data fragmentation	Slower coordination and inconsistent decisions	Interoperability standards; unified risk registers; data stewardship roles	NIS2 requirements for coordinated frameworks (European Union, 2022a)
Over-automation	Unaccountable decisions and legitimacy loss	Human-in-the-loop rules; documented decision chains; review procedures	AI Act risk-based governance (European Union, 2024)
Platform dependency	Service disruption and loss of continuity	Continuity planning; redundancy; incident response integration	Critical Entities Resilience requirements (European Union, 2022b)
Integrity and procurement risks	Corruption vulnerabilities under emergency spending	Audit trails; integrity screening; transparent criteria and reporting	National integrity controls and auditability practices (Bielai et al., 2021)
Information overreach	Rights violations and trust erosion	Proportionality tests; transparency; legal safeguards and oversight	DSA systemic risk governance context (European Union, 2022c)

Source: systematized by the authors

Digital resilience is inseparable from institutional resilience because the quality of governance determines whether digital systems enhance coordination or amplify vulnerability. Effective security governance therefore requires a continuous cycle of monitoring, learning, and procedural correction, not only technological upgrades (Pilko, 2014; Yarova & Mishenin, 2019).

In synthesis, the war demonstrated that national security governance in EU countries increasingly depends on two mutually reinforcing capabilities. The first is multilevel coordination that translates shared European frameworks into stable national implementation while preserving accountability under crisis pressure (Council of the European Union, 2022; Council of the European Union, 2024a). The second is digitally enabled administration that improves speed and situational awareness without weakening legality, integrity, and public trust, which remain decisive for resilience in prolonged conflict-related volatility (European Union, 2022a; European Union, 2024).

5. Governance capacity, performance measurement, and public trust in wartime security management. In wartime conditions, national security governance in EU countries increasingly depends on the administrative capacity to sustain continuous decision-making, deliver essential services under stress, and coordinate cross-sector actions over an extended period. This capacity is not limited to formal mandates, because it also includes the operational ability to mobilize resources lawfully, maintain procurement integrity, and learn from incidents quickly enough to prevent repeated failures. Contemporary public governance research emphasizes that resilience is strengthened when institutions combine competence with value-based performance, especially reliability, responsiveness, openness, fairness, and integrity, because these factors shape both outcomes and trust (OECD, 2024a). At the same time, the EU's growing use of performance-oriented instruments has highlighted a persistent challenge: without clear information on results, efficiency, and actual costs, governments and citizens struggle to evaluate whether emergency spending and reforms deliver value for money, which undermines legitimacy (European Court of Auditors, 2025). Therefore, wartime security management requires an integrated framework that links governance capacity to measurable performance and to public trust as a security resource.

Table 3.11 conceptualizes governance capacity as a multi-dimensional system in which weak links, for example procurement integrity or interagency coordination, can degrade the effectiveness of otherwise well-funded security policies.

Governance capacity is best understood as a system in which operational resilience depends on the alignment of rules, coordination routines, integrity controls, and staff capabilities. When one dimension fails, the security effect of investments declines and public trust becomes harder to sustain (OECD, 2023; UNDP, 2022).

Performance measurement is the mechanism that connects administrative effort to security outcomes and prevents crisis governance from becoming purely reactive. In wartime, measurement must be selective and decision-oriented, because overly complex dashboards create reporting burdens that reduce implementation speed. Yet the absence of performance evidence weakens accountability and can reproduce the problem identified by EU auditors in performance-based funding systems, where progress metrics may dominate while information on results and efficiency remains limited (European Court of Auditors, 2025). A workable approach is to measure outcomes that matter for continuity and resilience, while also monitoring process integrity in high-risk areas such as procurement, cyber incident response, and emergency social support.

https://doi.org/10.36690/PUBADM

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

Table 3.11. Core dimensions of governance capacity for wartime security management in EU countries

Capacity dimension	What it includes in wartime security governance	Typical bottlenecks and failure modes	Practical strengthening measures
Strategic and legal readiness	Updated strategies, lawful emergency regimes, delegated authorities, clear mandates	Legal ambiguity, contradictory mandates, slow activation of emergency tools	Pre-approved crisis protocols; legal stress testing; clear delegation rules (Sytnyk, 2011; Prav, 2021)
Interagency coordination	Whole-of-government coordination, joint planning, unified situational awareness	"Stovepipes," duplicated efforts, delayed escalation	Permanent interagency task forces; common operating picture; joint exercises (Bielai et al., 2024)
Financial and procurement governance	Rapid spending with auditability, competition where possible, anti-fraud controls	Emergency procurement opacity, weak documentation, corruption risks	Digital procurement traceability; risk-based audits; disclosure standards (Bielai et al., 2021)
Human and organizational capacity	Skilled staff, surge staffing, continuity of operations, institutional memory	Burnout, turnover, skill gaps in cyber and data, fragile routines	Surge rosters; training pipelines; after-action learning cycles (OECD, 2023)
Digital and data capacity	Interoperable registries, secure communications, incident reporting, analytics	Fragmented data, insecure systems, slow information exchange	Standardization; secure data-sharing; resilience-by-design (Dumchykov et al., 2022; OECD, 2023)
Societal interface and communication	Strategic communication, service quality, grievance handling, inclusion policies	Polarization, distrust, rumor cascades, low compliance	Transparent messaging; feedback loops; community-level engagement (OECD, 2024a; UNDP, 2022)

Source: systematized by the authors

Table 3.12 proposes a compact performance logic that links inputs, processes, outputs, and outcomes, allowing governments to demonstrate effectiveness without losing administrative agility.

A balanced measurement model prevents the substitution of activity for impact and supports learning under uncertainty. This is crucial because performance-oriented governance without credible evidence on results can erode accountability and public confidence (European Court of Auditors, 2025; OECD, 2024a).

Public trust is not only a political outcome but also an operational enabler of national security, because compliance with emergency measures, willingness to accept temporary costs, and readiness to cooperate with authorities depend on perceived legitimacy. OECD evidence indicates that trust is structured by perceptions of reliability, responsiveness, openness, fairness, and integrity, which means that trust can be strengthened through concrete governance behaviors, not only through messaging (OECD, 2024a).

Table 3.12. Performance measurement framework for wartime national security governance

Measurement level	Illustrative indicators	Why it matters for security	Example data sources inside government
Inputs and readiness	Reserve funds availability; surge staffing coverage; critical stock levels	Determines response capacity under shock	Treasury systems; HR rosters; stock registries
Process integrity	Share of emergency contracts with full documentation; audit findings; time to publish procurement data	Reduces fraud and legitimacy loss under surge spending	E-procurement platforms; internal audit reports
Operational outputs	Time to activate crisis coordination; number of joint exercises; incident response cycle time	Measures coordination speed and institutional discipline	Crisis center logs; exercise reports; CERT records
Service continuity	Critical service uptime; health and education capacity under displacement; municipal service backlogs	Captures continuity of governance and social stability	Service registries; local dashboards; sector regulators
Strategic outcomes	Reduced dependency on high-risk supplies; reduced severe cyber incidents; improved compliance rates	Reflects resilience improvements rather than activity	Energy regulators; cybersecurity authorities; compliance reports
Trust and legitimacy	Trust levels; perceived fairness; satisfaction with key services	Trust supports compliance and resilience during prolonged crisis	Surveys; ombudsman data; complaints systems (OECD, 2024a)

Source: systematized by the authors

In wartime conditions, the trust function becomes more demanding because society evaluates government simultaneously on competence and values, especially fairness in burden-sharing and integrity in emergency spending. This connects directly to security capacity because perceived corruption, opaque procurement, or inconsistent rules create vulnerability that adversaries can exploit through disinformation and societal polarization (OECD, 2023; Pilko, 2014).

Table 3.13 translates the core trust drivers into practical wartime governance tasks, emphasizing that trust is produced through observable administrative routines.

Trust rises when wartime governance is consistent, transparent, and fair, because citizens interpret administrative behavior as evidence of competence and values. This is aligned with empirical trust frameworks that treat governance quality as the main driver of trust dynamics (OECD, 2024a; OECD, 2023).

Table 3.13. Trust drivers and wartime governance practices in public administration

Trust driver	What citizens typically evaluate	Wartime administrative practices that build trust	Common trust-damaging patterns
Reliability	Predictable rules, continuity of services	Stable emergency procedures; clear eligibility rules for support; continuity planning (UNDP, 2022)	Frequent rule changes; unclear responsibilities
Responsiveness	Speed and usefulness of state reaction	Fast coordination; one-stop services; rapid problem resolution	Delayed decisions; administrative silence
Openness	Transparency of decisions and spending	Public reporting; accessible procurement data; clear rationales	Non-transparent procurement; vague justifications
Fairness	Equity in burden-sharing and access	Targeted protection for vulnerable groups; consistent enforcement	Unequal enforcement; perceived favoritism
Integrity	Clean use of funds and power	Conflict-of-interest controls; auditability; sanctions for abuse	Emergency corruption scandals; weak documentation

Source: systematized by the authors

A final element that connects capacity, performance, and trust is accountability design. In crisis conditions, governments often adopt accelerated procurement and simplified procedures; however, comparative evidence from emergency contexts shows that procurement opacity and weak disclosure amplify integrity risks and legitimacy loss (Bielai et al., 2021; Fiscal Transparency Innovation Fund, 2022). EU audit practice similarly underscores that large-scale financing instruments require stronger result visibility and clearer accountability if they are to sustain public confidence over time (European Court of Auditors, 2025). Therefore, wartime security governance should institutionalize ex ante controls, real-time monitoring, and ex post review in a way that does not paralyze implementation but preserves auditability and democratic oversight.

In synthesis, wartime national security management in EU countries depends on governance capacity that can sustain coordinated action, performance measurement that demonstrates real outcomes rather than activity, and trust-building routines that preserve legitimacy in prolonged crisis. These elements reinforce each other: capacity without trust reduces compliance, trust without performance evidence is fragile, and performance without integrity undermines legitimacy. Consequently, the most resilient public administrations are those that institutionalize coordination, protect integrity under surge spending, measure what matters for continuity and resilience, and communicate transparently while maintaining fairness and rights protections (OECD, 2024a; European Court of Auditors, 2025;

UNDP, 2022).

Conclusions. The analysis confirms that Russia's full-scale invasion of Ukraine fundamentally reshaped how EU countries conceptualize national security. Security is no longer interpreted primarily as military defence, but as a complex, interdependent system in which continuity of governance, protection of critical infrastructure, cyber resilience, information stability, energy sustainability, and social cohesion are treated as mutually reinforcing conditions of state resilience. In this expanded framework, public administration functions as the institutional core that converts strategic priorities into operational mechanisms, including lawful emergency regimes, interagency coordination routines, budget mobilisation, procurement governance, oversight, and delivery of essential public services under stress. The war demonstrated that even strong strategic intentions produce limited effects when administrative systems cannot act quickly while maintaining legal correctness, procedural discipline, and transparent accountability, because these attributes condition compliance and societal endurance in prolonged crises.

A central conclusion is that contemporary security governance in the EU has become structurally multilevel. EU-level strategic and regulatory frameworks increasingly shape national administrative agendas, while outcomes remain dependent on the quality of domestic implementation capacity. Shared directions and agreed actions acquire practical value only when Member States institutionalise them through planning cycles, capability development, procurement integrity controls, training systems, and crisis coordination procedures that remain auditable and politically sustainable. In this sense, the war made security cooperation administratively concrete: collective commitments require standardised procedures, measurable outputs, and credible reporting that can withstand domestic political cycles and fiscal scrutiny.

The findings also show that energy governance has been transformed into an explicit element of national security management. Public administrations must manage strategic dependencies, ensure supply continuity, protect households and firms from destabilising shocks, and accelerate clean-energy pathways in parallel. This requires rapid regulatory action, infrastructure investment capacity, market supervision, and targeted social protection tools that reduce vulnerability without undermining competitiveness. The war thus reinforced a governance logic in which energy policy, industrial policy, and social policy are operationally linked within a single resilience loop, and misalignment among these instruments can generate cascading security risks.

Cybersecurity and critical infrastructure resilience have become similarly central, not only as technical domains but as regulatory and administrative systems that require enforcement capacity. The war environment increased the relevance of mandatory risk management, incident reporting, supervision, and cross-border cooperation expectations, which elevated institutional design choices, regulator competence, and compliance routines to determinants of security outcomes rather than administrative formalities. This also applies to the information environment, where foreign information manipulation and disinformation pressures make trust, legitimacy, and coherent strategic communication operational variables of national resilience. Digital tools and AI-enabled analytics can strengthen monitoring and early warning, yet their value depends on governance safeguards, data quality, accountable decision chains, and rights-respecting oversight, because legitimacy losses in the information sphere directly weaken security capacity.

The humanitarian dimension further demonstrates the security relevance of administrative capacity. Large-scale displacement requires long-term service coordination across central and local levels, sustainable financing, integration policies, and effective communication with society. In national security terms, the decisive issue is whether administrations can absorb prolonged pressures on education, health care, housing, and labour markets without eroding social cohesion and trust, because societal stability is a prerequisite for resilience in extended crises. This shifts governance from short-term crisis response toward medium- and long-term adaptation, where capacity building and institutional learning become strategic security tasks.

Finally, the overarching conclusion is that wartime security management depends on the interaction of governance capacity, performance measurement, and public trust. Governance capacity should be understood as a multidimensional system that includes legal readiness, interagency coordination, financial and procurement integrity, human resources, data infrastructure, and continuity planning. Performance measurement is required to demonstrate results, avoid the substitution of activity for impact, and sustain accountability under pressure, especially in contexts of large-scale spending and accelerated procedures. Trust operates as a strategic resource because it supports compliance, stabilises expectations, and reduces vulnerability to manipulation; it is shaped by reliability, responsiveness, openness, fairness, and integrity that citizens observe in daily administrative practice. Therefore, the principal lesson is that EU security in the post-2022 environment is increasingly produced through governance, meaning the ability of public administration to act quickly, lawfully, coherently, and transparently across sectors, while sustaining democratic accountability and public trust over time.

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. Bielai, S. V., Kobzar, O. F., Yevtushenko, I. V., Korniienko, V. O., & Koba, O. V. (2021). The legal regulation of service and combat activities of the security and defense sector of Ukraine in crisis situations. *Journal of the National Academy of Legal Sciences of Ukraine, 28*(2), 76–85. https://doi.org/10.37635/jnalsu.28(2).2021.76-85
2. Bielai, S., Antonova, L., Hololobov, S., Yevtushenko, I., & Sporyshev, K. (2024). The impact of a practice-oriented paradigm on public administration and national security. *International Journal of Sustainable Development and Planning, 19*(1), 277–288. https://doi.org/10.18280/ijsdp.190126
3. Council Decision (CFSP) 2022/1968 of 17 October 2022 on a European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine). (2022). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dec/2022/1968/oj
4. Council Decision (CFSP) 2024/890 of 18 March 2024 amending Decision (CFSP) 2021/509 establishing a European Peace Facility. (2024). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024D0890
5. Council Implementing Decision (EU) 2022/382 of 4 March 2022 establishing the existence of a mass influx of displaced persons from Ukraine within the meaning of Article 5 of Directive 2001/55/EC, and having the effect of introducing temporary protection. (2022). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dec_impl/2022/382/oj
6. Council Implementing Decision (EU) 2025/1460 of 15 July 2025 extending temporary protection as introduced by Implementing Decision (EU) 2022/382. (2025). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dec_impl/2025/1460/oj
7. Council of the European Union. (2022, March 21). *A Strategic Compass for Security and Defence*. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-security-and-defence/

8. Council of the European Union. (2022, March 23). *European Peace Facility: Council doubles funding to support the Ukrainian armed forces*. https://www.consilium.europa.eu/en/press/press-releases/2022/03/23/european-peace-facility-council-doubles-funding-to-support-the-ukrainian-armed-forces/
9. Council of the European Union. (2024, June 25). *Temporary protection: Council agrees to extend temporary protection for people fleeing from Ukraine*. https://www.consilium.europa.eu/en/press/press-releases/2024/06/25/temporary-protection-council-agrees-to-extend-temporary-protection-for-people-fleeing-from-ukraine/
10. Council of the European Union. (2024). *Integrated Political Crisis Response (IPCR) arrangements*. https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/
11. Dumchykov, M., Utkina, M., & Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering, 12*(4), 481–490. https://doi.org/10.18280/ijsse.120409
12. European Commission. (2022, May 18). *REPowerEU plan* (COM(2022) 230 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0230
13. European Commission. (2025, June 17). *Commission proposes a roadmap to phase out Russian gas and oil imports by 2027*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1540
14. European Commission. (2025, May 6). *REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu_en
15. European Commission. (2025). *Emergency Response Coordination Centre (ERCC)*. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en
16. European Court of Auditors. (2025). *The Recovery and Resilience Facility's contribution to the digital transition in the EU: Risks to delivering EU ambitions* (Special Report 13/2025). https://www.eca.europa.eu/en/publications/sr-2025-13
17. European External Action Service. (2022). *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
18. European External Action Service. (2025). *Third report on Foreign Information Manipulation and Interference (FIMI) threat*. https://www.eeas.europa.eu/eeas/third-report-foreign-information-manipulation-and-interference-fimi-threat_en
19. European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
20. European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557

21. European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj
22. 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). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
23. Kryshtanovych, M., Antonova, L., Filippova, V., Dombrovska, S., & Pidlisna, T. (2022). Influence of COVID-19 on the functional device of state governance of economic growth of countries in the context of ensuring security. *International Journal of Safety and Security Engineering, 12*(2), 193–199. https://doi.org/10.18280/ijsse.120207
24. Kryshtanovych, M., Kupchak, V., Voronov, O., Larina, N., & Humeniuk, A. (2023). Formation of social leadership in the system of public safety and security through the use of modern modeling techniques. *International Journal of Safety and Security Engineering, 13*(2), 317–324. https://doi.org/10.18280/ijsse.130213
25. Organisation for Economic Co-operation and Development. (2022). *Building trust to reinforce democracy*. OECD Publishing. https://www.oecd.org/en/publications/building-trust-to-reinforce-democracy_bb2ff49e-en.html
26. Organisation for Economic Co-operation and Development. (2024a). *OECD Survey on Drivers of Trust in Public Institutions: 2024 results*. OECD Publishing. https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_a6fc7d55-en.html
27. Organisation for Economic Co-operation and Development. (2024b). *Trust in public institutions: Trends and drivers*(OECD Trust Survey data and insights). https://www.oecd.org/en/topics/trust-in-government.html
28. Pilko, A. (2014). Evolution of models and perspective directions of development of security studies. In *Economic security in the conditions of globalization of the world economy: Collective monograph* (Vol. 1, pp. 166–177). FOP Drobyazko S. I. https://lib-repo.pnu.edu.ua/bitstream/123456789/6785/1/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F%20%D0%9F%D1%96%D0%BB%D1%8C%D0%BA%D0%BE%202014.pdf
29. Prav, R. (2021). Ways to improve the efficiency of mechanisms for ensuring the national security of Ukraine in the context of European experience. *Scientific Perspectives, 9*(15), 197–206. https://doi.org/10.52058/2708-7530-2021-9(15)-197-206
30. Sytnyk, G. (2011). Institutional and civilizational paradigm of research of problems and public administration aspects of national security. *Bulletin of the National Academy for Public Administration under the President of Ukraine, 2*, 25–34.
31. Sytnyk, H. (2011). Institutional and civilizational paradigm of research of problems and public administration aspects of national security. *Bulletin of the National Academy for Public Administration under the President of Ukraine, 2*, 25–34. https://irbis-nbuv.gov.ua/cgi-

bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&Z21ID=&Image_file_name=PDF/Vnadu_2011_2_6.pdf

32. United Nations Development Programme. (2021). *UNDP strategic plan, 2022-2025*. https://strategicplan.undp.org
33. Yarova, I., Mishenin, Y. Methodology of formation of economic and socio-ecological indicators of economic activity in the context of national security. In Emergence of Public Development: Financial and Legal Aspects: Collective Monograph. Agenda Publishing House, Coventry, United Kingdom. 2019, pp. 373-383.
34. Yemanov, V., Belay, S., & Sporyshev, K. (2022). Information-analytical method of improving the efficiency of technical intelligence of the technical support units of the National Guard of Ukraine. *Collection of Scientific Papers of the National Academy of the National Guard of Ukraine, 1*(39), 104–110. https://doi.org/10.33405/2409-7470/2022/1/39/263376

Section 3.2. Public Administration in Ensuring the Economic Security of the State: Digital Tools and Management Innovations

Yana Koval,[1] Alona Zahorodnia[2]

[1]Ph.D. (Public administration), Associate Professor, Associate Professor of International Management Department, State University of Trade and Economics, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-6578-2996

[2]Ph.D., Associate Professor of the Department of International Relations and Political Consulting, Institute of Law and Public Relations, Open International University of Human Development "Ukraine", Kyiv, Ukraine, ORCID: https://orcid.org/0000-0003-2741-1953

Citation:

Koval, Ya. & Zahorodnia, A. (2025). Public Administration in Ensuring the Economic Security of the State: Digital Tools and Management Innovations. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance.* 262 p. (pp. 182-205). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-182-205

Abstract. *The study examines the role of public administration in ensuring the economic security of the state in conditions of global transformations, digitalization and geopolitical instability. Its objective is to substantiate conceptual and applied approaches to strengthening economic security through the use of digital tools and management innovations in Ukraine. The methodology combines systemic, institutional and comparative approaches, analysis of regulatory frameworks and international documents, as well as generalization of statistical and analytical data on globalization, international trade, activity of global economic institutions and national security indicators. The main results include clarification of the essence and structure of economic security, identification of its key components and indicators, and demonstration of the dual impact of globalization that simultaneously opens access to markets, investment and technology and increases vulnerability to external shocks, financial dependence and technological risks. Special attention is paid to the role of the IMF, World Bank and WTO in shaping the global environment of economic security, as well as to modern forms and trends of international trade that transform the risk profile of national economies. For Ukraine, the study substantiates priority directions of strengthening economic security: regulation of foreign participation in strategic sectors, support of national producers, development of technological and production independence, improvement of financial monitoring and institutional strengthening of the economic security system. Directions for further research include development of quantitative models for assessing the impact of digital tools on economic security, creation of integrated dashboards for real time monitoring of external and internal threats, and analysis of the effectiveness of public policy instruments in conditions of prolonged war and post war recovery.*

Keywords: *public administration; economic security; innovation; globalization; digital tools; threats; foreign economic activity; competitiveness.*

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

1. Economic security of the state in the context of digital transformation. In the current context of global transformations, geopolitical instability, and the digital revolution, the issue of ensuring the economic security of the state is becoming particularly important. The ability of the state to maintain its sovereignty, the stability of the national economy, social stability, and competitiveness in the global arena depends on the level of economic security. However, in the era of the digital economy and the intensive development of information technologies, traditional approaches to state management of economic security are gradually losing their effectiveness, which necessitates an innovative rethinking of the state's role in this process.

Modern economic security is shaped by the digital transformation of management processes, with the growing importance of analytical data, artificial intelligence algorithms, automated risk monitoring systems, cybersecurity, and e-government platforms. These technological changes not only open up new opportunities for improving the efficiency of public administration, but also create new threats related to cyber risks, dependence on external technological resources, information wars, and the technological vulnerability of critical infrastructure.

In the context of Ukrainian realities, the issue of economic security has an even more complex dimension. Armed aggression against Ukraine, disruption of energy chains, destruction of industrial potential, and the outflow of labor resources and financial capital require new public management approaches to the restoration, protection, and development of the economic system. It is public administration based on the principles of innovation, openness, and digital interaction that can ensure a timely response to threats, optimal use of resources, and increased resilience of the state to crisis impacts (Koval, 2024; Pihariiev & Kosteniuk, 2021; Syrotin, 2023).

The use of digital tools in public administration – such as analytical risk management platforms, electronic budget flow control systems, smart regulatory analytics, and digital security dashboards – opens up new prospects for improving the effectiveness of management decisions. At the same time, this requires rethinking management models, developing the digital analytics skills of civil servants, and creating a unified information space for economic security management.

Recent studies indicate a deterioration in the economic, social, and political situation at both the global and national levels. The beginning of the 21st century was marked by deeper economic integration between countries, which simultaneously strengthened economic interdependence and increased global instability. The growing interdependence of countries in the international economic space makes national economies more vulnerable to external influences. At the same time, focusing on narrow specialization in line with the concept of "comparative advantage" often requires complex reforms and painful adaptation of a country's production structure.

In addition, international capital flows are growing every year, which in times of crisis can seriously destabilize the economies of developing countries. These countries are forced to deal with volatile and intense financial flows, and their ability to exercise effective control over them is quite limited. As a result, a country's integration into the global economic space is sometimes accompanied by a weakening of its ability to implement independent financial and economic policies (Dyba & Osadchy, 2014; Levitt, 2025; Robertson, 1992; Zakharov, 2016).

Thus, the economic security of countries is increasingly intertwined with the processes of globalization. At the same time, there's still debate among scholars about the nature and strength of globalization's impact on countries' economic protection. To get an objective assessment of this impact, we need to use a system of key indicators that let us measure a country's economic security.

2. Globalization, international trade and international institutions as factors of economic security. Globalization is a process through which countries and societies become economically, politically, and culturally interdependent. Globalization is the result of a profound transformation of the modern world, in which societies are rethinking their values, changing their ideologies, and transforming key institutions.

The changes taking place also affect the fundamental foundations responsible for the security of nations in one area or another. One such foundation is economic security.

Economic security is a phenomenon that characterizes the state of the economy in which key economic indicators meet the needs of interested parties, individuals, societies, or entire countries. It should be noted that due to limited resources, in order to achieve or maintain economic security, conflicts of interest often arise between entities, which is a source of further competition (Fedorenko et al., 2022; Reznik et al., 2021; Vlasyuk, 2008).

Economic security is a priority area of state activity. The need to ensure the security of society is always necessary. However, the classification of economic security into specific categories is a relatively recent development.

Contemporary scientific sources offer various definitions of the concept of "economic security," including:

- it is a characteristic of an economic system that reflects its ability to preserve itself and develop in the face of both predictable and unpredictable internal and external threats;
- it is a state in which resources are used as efficiently as possible to ensure stability today and in the future;
- it is the level of protection of an economic entity from external and internal threats in order to realize its own strategic interests;
- it is a continuous process of adapting the economy to changes in the external environment in order to achieve set goals (Datskiv, 2004; Economic security, 2009; Vorobyov, 2011).

Considering the above, it is advisable to form our own concept of "economic security," which we propose to understand as the state and ability of the economic system to function effectively, maintain stability, and ensure development in changing internal and external conditions through the rational use of resources, protection from potential threats, and ensuring the implementation of strategic goals in the long term.

At the same time, the economic security of the state is a key element of the national security system, which has a complex internal structure. Its elements sometimes overlap with other aspects of national security defined at the legislative level, which is the subject of discussion and criticism among scholars and practitioners.

The vast majority of researchers agree that an analysis of Ukraine's economic security needs to take into account the following key components (Kovalenko et al., 2009; Shemaeva, 2009; Shlemko & Binko, 1997; Sukhorukov & Ladyuk, 2007):

- *Raw material and resource security* – this component reflects the state's ability to meet its own needs for natural resources – mineral, water, land, forest, etc. It involves the rational use of available reserves, their reproduction, and reducing dependence on raw material imports. The environmental component is also important – the extraction and processing of resources must be carried out without harming the environment and with sustainable development in mind;
- *Energy security* means stable, reliable, and cost-effective energy supply for the country. It includes diversifying energy sources, developing domestic energy potential, modernizing infrastructure, and improving energy efficiency. For Ukraine, this component is strategic due to its historical dependence on energy imports, primarily gas and oil;
- *Financial security* - characterizes the stability of the financial system, the state's ability to effectively manage the budget, debt, and money supply. It involves controlling inflation, balancing public finances, ensuring the

stability of the banking system, and creating a favorable investment climate. Violations of financial security can lead to crises such as currency devaluation or an increase in the budget deficit;

- *Social security* - covers the standard of living of the population, social stability, access to education, healthcare, employment, and protection of vulnerable groups. It is a guarantee of the preservation of human potential, social harmony, and trust in state institutions. A decline in social security can lead to rising unemployment, emigration, and social tension;
- *Innovation and technological security* - this component determines the ability of the economy to develop through the introduction of new technologies, scientific developments, and increased labor productivity. It involves supporting the research and development sector, developing digitalization, protecting intellectual property, and stimulating innovative entrepreneurship;
- *Food security* means a country's ability to provide its population with high-quality and affordable food in the necessary quantities. It requires stable functioning of the agricultural sector, development of domestic production, protection of the domestic market from excessive imports, and support for food exports. This component is of great importance for Ukraine due to its role as one of the world's leading agricultural exporters;
- *Foreign economic security* - determines a country's ability to effectively integrate into the global economy while maintaining control over strategic sectors and national interests. It includes diversification of trading partners, protection of the domestic market, participation in international organizations, and ensuring a positive trade balance. Violations of foreign economic security can lead to dependence on individual countries or currency instability.

As mentioned above, the level of economic security can be assessed using key economic indicators. One such indicator is the indicator describing foreign trade. Since ancient times, countries have been engaged in mutually beneficial exchange of resources, which today is represented by foreign trade. By exporting goods and services, countries receive funds. They also import goods and services that are missing or in short supply. The next important indicator is unemployment. Finally, the most common indicator characterizing the development of the region's economy is the gross domestic product (GDP). This indicator reflects the market value of all final goods and services produced in the country during the year (Methodology for calculating the level of economic security of Ukraine, 2025; OECD, 2025; WTO, 2025).

At the same time, in the current context of globalization, the world economy functions as a single system of interconnected elements, in which national economies are becoming increasingly dependent on each other. Globalization processes have a dual impact on the economic security of a state: on the one hand, they open up new opportunities for economic growth, innovation, investment attraction, and expansion of foreign markets; on the other hand, they increase the risks of financial instability, technological dependence, and loss of economic sovereignty. Therefore, it is important to determine in which areas globalization can contribute to strengthening or, conversely, weakening a country's economic security.

Below is a summary table reflecting the main aspects of the relationship between globalization processes and the state of a country's economic security (Table 3.14).

Table 3.14. Systemic characteristics of the impact of globalization processes on the economic security of the state

The aspect of interconnection	A manifestation of globalization	Impact on economic security	Nature of impact (positive/negative)
Financial	International integration of financial markets, free movement of capital	Attracting foreign investment, but also the risk of financial dependence and crises	Dual: positive with stable control, negative with excessive openness
Trading	Liberalization of foreign trade, reduction of tariff barriers	Expansion of sales markets, but increased competition from TNCs	Mostly positive, but subject to protection of the national producer
Technological	Active technology transfer, digitalization of the economy	Productivity improvement, production modernization, but the possibility of technological dependence	Positive, subject to localization and development of own innovations
Social	Migration processes, labor exchange, information openness	Enrichment of experience, development of human capital, but also “brain drain”	Dual: positive in control, negative in uncontrolled migration
Political	Growing influence of international institutions, integration into world structures	Possibility of participation in global decisions, but risk of losing part of sovereignty	Depends on the level of independence of the state
Energetic	Dependence on global energy markets and resource imports	Access to resources, but risk of energy instability and price fluctuations	Negative without diversification of supply sources
Informative	Global information flows, development of IT technologies	Expanding access to knowledge, but increasing risk of cyberattacks and disinformation	Dual: positive with high level of data protection

Source: compiled by the author based on data from (Fedorenko and Zahorodnia, 2024; Zahorodnia and Sharma, 2024; Vlasyuk, 2008; Syrotin, 2023)

Thus, globalization is both a factor in development and a source of potential risks to the economic security of the state. Its impact is multidimensional and encompasses the financial, social, technological, energy, and other spheres of the national economy. For Ukraine, the key task is to use the positive opportunities of globalization, such as attracting investment and innovation, while strengthening mechanisms to protect against external economic threats and ensuring the stability of the national economy (Dyba & Osadchy, 2014; Levitt, 2025; Robertson, 1992).

Having identified the main indicators that constitute the level of economic security, we can consider the impact of globalization on these indicators, since the inherent inequality in the distribution of natural resources between different localities has led to the emergence of international trade. Globalization and international trade are closely linked, as both phenomena make societies and states more interdependent (Datskiv, 2004; Kutsyk et al., 2015; Varnalii et al., 2009).

In the context of the economy, globalization is usually associated with the evolution of capitalism as the dominant economic system, often based on the idea of a self-regulating market. It is believed that globalization processes have contributed to the spread of economic freedom and an overall increase in the level of prosperity in the world, although at the same time there is a continuing trend towards a widening gap between the wealthy and the poor (Dyba & Osadchy, 2014; Robertson, 1992; Yuskiv, 2009).

One of the key manifestations of globalization has been the expansion of international trade and the global redistribution of the production of goods and services. This has been made possible by the gradual removal of trade barriers, such as customs duties, import quotas, and export taxes, as well as the relaxation of regulations on the movement of capital and investments (Levitt, 2025; WTO, 2025).

There has also been an increase in outsourcing and the relocation of production to peripheral countries. Transnational corporations (TNCs) are increasingly using the resources of small and medium-sized enterprises, focusing on the lowest cost on a global scale. In turn, it is becoming increasingly difficult for small and medium-sized businesses to withstand international competition and guarantee decent working conditions. It is difficult to hold TNCs accountable for human rights violations, as such corporations are usually registered in one country, while their activities take place in a completely different one (Levitt, 2025; Manual on education in the field of human rights with the participation of youth, 2025; MacFarlane & Khong, 2006).

Globalization has also influenced the privatization of public resources and sectors, such as water supply, healthcare, security, and even the prison system. Recently, other resources have also been affected by economic commercialization, such as seeds and medicines, which have become part of international trade agreements (Manual on education in the field of human rights with the participation of youth, 2025; WTO, 2025).

At the same time, globalization has contributed to the development of corporate social responsibility and increased attention to the accountability of non-state actors–primarily TNCs–for their impact on the environment, communities, and the social sphere. Currently, the number of companies implementing internal codes of ethical conduct is growing. Consumer boycott movements and public campaigns are increasingly forcing corporations to take into account the social risks and reputational consequences of their activities (Levitt, 2025; Robertson, 1992).

Global international economic institutions. The International Monetary Fund (IMF) plays an important role in providing financial support and economic policy advice to member countries facing economic challenges. In addition, the Fund actively cooperates with developing countries to achieve macroeconomic stability and overcome poverty. The conditions imposed by the IMF in exchange for financial assistance consist of a set of policy measures and reforms that the borrowing country must implement. At the same time, human rights are largely ignored in the Fund's approaches, as its main focus is on economic and monetary aspects (MacFarlane & Khong, 2006; Pasternak-Taranushenko, 1994).

The World Bank, for its part, provides financing to developing countries with the primary goal of reducing poverty. The Bank also promotes foreign capital inflows, international trade, and investment. Although 187 countries are formally represented in the World Bank's management, real influence belongs to a limited circle of economically powerful states. In the 1990s, both the World Bank and the IMF implemented policies that included trade liberalization, market deregulation, privatization of property, and downsizing of the public sector (MacFarlane & Khong, 2006; Manual on education in the field of human rights with the participation of youth, 2025).

The International Monetary Fund (IMF) provides policy and financing advice to member countries experiencing economic difficulties and works with developing countries to help them achieve macroeconomic stability and poverty reduction. IMF conditions are a set of strategies or “conditions” that the IMF requires in exchange for financial resources. Human rights are not integrated or are very little integrated into the policies of the International

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

Monetary Fund, whose main areas of work are economic and monetary order (MacFarlane & Khong, 2006; Pasternak-Taranushenko, 1994).

The World Bank provides loans to developing countries with the aim of reducing poverty, making decisions on commitments to promote foreign investment, international trade, and facilitate capital investment. Despite its significant influence on developing countries and the fact that it represents 187 countries, the World Bank is controlled by a small number of economically powerful countries. In the 1990s, the World Bank and the International Monetary Fund shaped policies that included deregulation and liberalization of markets, privatization, and reduction of the public sector (MacFarlane & Khong, 2006; Manual on education in the field of human rights with the participation of youth, 2025).

Thanks to globalization and technological progress, trade has become faster and more profitable. In 1995, the World Trade Organization (WTO) was established with the aim of regulating trade and political relations between member countries. The World Trade Organization (WTO) is an international organization that began operating on January 1, 1995, with the aim of liberalizing international trade and regulating trade and political relations between member countries (WTO, 2025).

In recent years, the World Trade Organization has significantly expanded its powers, going far beyond the scope of purely trade interaction between states. Today, the WTO is an influential international institution that plays a key role in regulating global economic processes. Joining the WTO has become almost a mandatory step for countries seeking to fully integrate into the global economy (WTO, 2025).

The process of forming, developing, and expanding the World Trade Organization has been complex and ambiguous. Despite the significant growth of the WTO's regulatory framework over the past three decades, the organization continues to function on the basis of bilateral negotiations between member countries on the mutual opening of markets. When agreeing on the terms of accession of new members, each member state puts forward requirements aimed at protecting its own economic interests, supporting national production, and preserving jobs. This makes the negotiation process complex and lengthy (WTO, 2025).

As of 2024, the World Trade Organization (WTO) has 166 members, including both states and customs territories. The WTO officially began its work on January 1, 1995, as the successor to the General Agreement on Tariffs and Trade (GATT), which was signed back in 1947. Its creation was preceded by many years of Uruguay Round negotiations, in which 123 countries participated–they became the founders of the new organization (WTO, 2025).

In the following years, WTO membership gradually expanded. In particular, between 1996 and 2008, 25 new countries joined the organization, including Bulgaria (1996), Mongolia (1997), Kyrgyzstan and Latvia (1998), Estonia (1999), as well as Georgia, Croatia, Albania, Jordan, Oman, Panama, Moldova, and others. In 2007, Vietnam became a member of the WTO, and in 2008, Ukraine (May 16) and Cape Verde (July 23) joined (WTO, 2025).

In recent years, the process of joining the WTO has continued, although it has been much slower due to complex negotiation procedures. In December 2015, Afghanistan and Liberia joined the organization. These countries were admitted during the 10th WTO Ministerial Conference held in Nairobi, Kenya. The accession process for Afghanistan was particularly difficult, lasting more than 11 years. The latest, 166th member of the WTO is Timor-Leste, which officially joined the organization on August 30, 2024 (WTO, 2025).

Thus, WTO membership has become almost a prerequisite for countries seeking to become full participants in the global economic space. Joining the WTO requires compliance with strict trade liberalization requirements, adaptation of national legislation to international standards, and opening markets to international competition. All these factors make the process of joining the organization extremely complex and lengthy, but strategically important for countries seeking to integrate into the global economy (Figure 3.1). Ukraine became a full member of the WTO on May 16, 2008 (WTO, 2025; Zakharov, 2016).

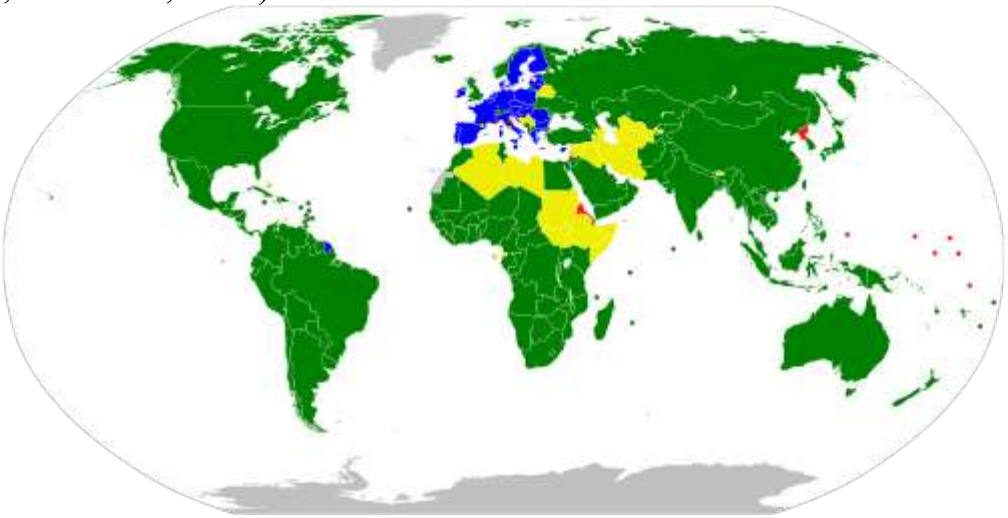

Figure 3.1. WTO members and observers

Source: compiled based on data from (Koval et al., 2024)

https://doi.org/10.36690/PUBADM

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

The WTO protects domestic producers in foreign markets, which allows exports and imports to proceed more efficiently. By exporting goods, countries receive income and ensure the growth of their GDP. Importing goods allows for a significant diversification of choice for consumers.

However, foreign trade also has its drawbacks. First, focusing on exports as the main driver of a country's economy makes the economy unstable and dependent on foreign trade agreements. Second, when importing a certain type of goods, the production of its analogues in the country may decline significantly due to the lack of need for their production.

The danger lies in the fact that if the supply of these goods to the country is suddenly suspended, there will be no viable alternative on the local market. To strengthen its economic security, the state needs to become more independent of foreign trade (Zahorodnia, 2024).

World trade covers a wide range of economic activities related to the exchange of goods, services, capital, and technologies between countries. Based on the nature of transactions and the objects of exchange, there are several main types of international trade (Figure 3.2).

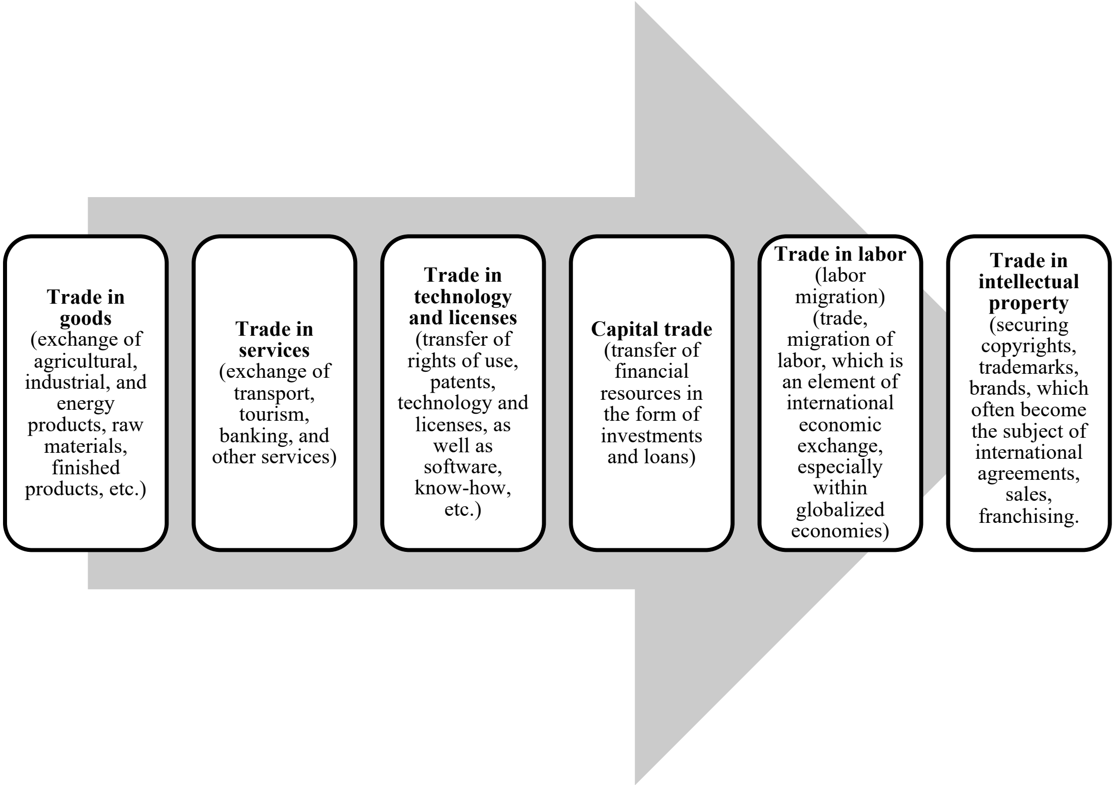
Trade in goods (exchange of agricultural, industrial, and energy products, raw materials, finished products, etc.)
Trade in services (exchange of transport, tourism, banking, and other services)
Trade in technology and licenses (transfer of rights of use, patents, technology and licenses, as well as software, know-how, etc.)
Capital trade (transfer of financial resources in the form of investments and loans)
Trade in labor (labor migration) (trade, migration of labor, which is an element of international economic exchange, especially within globalized economies)
Trade in intellectual property (securing copyrights, trademarks, brands, which often become the subject of international agreements, sales, franchising.

Figure 3.2. Structural diagram of the main forms of international trade

Source: compiled by the author based on (Zakharov, 2015, 2016; Kovalenko et al., 2009; Kryvovyazyuk, 2013)

Let us consider each of these forms in more detail:

1. *Trade in goods (material trade)* is the most common form of international trade, covering the exchange of agricultural, industrial, and energy products, raw materials, finished products, etc. Such trade is the basis of the balance of payments for most countries. It includes exports (export of goods) and imports (import of goods).

2. *Trade in services (intangible trade)* - this type covers the international exchange of services such as transportation, tourism, banking, insurance, education, consulting, information, communication, digital, etc. Every year, the share of trade in services in the overall structure of international trade is growing, which is associated with the development of information technology and the digitization of the economy.

3. *Trade in technology and licenses* - this type of trade involves the transfer of rights to use patents, inventions, technological processes, software, know-how, etc. It is particularly common among developed countries and transnational corporations (Fedorenko et al., 2022).

4. *Trade in capital involves* the movement of financial resources between countries in the form of investments (direct and portfolio), credits, and loans. Such trade is linked to international financial markets and institutions.

5. *Trade in labor (labor migration)* - although not always directly considered trade, labor migration is also an element of international economic exchange, especially within globalized economies. It affects labor supply and demand, wage levels, and the transfer of technology and experience.

6. *Trade in intellectual property* - in today's world, the importance of copyrights, trademarks, and brands is growing, and they often become the subject of international agreements, sales, and franchising (Laptiev et al., 2024).

Thus, world trade encompasses not only physical goods, but also a wide range of intangible assets and services. The diversity of forms and directions of international trade necessitates flexible regulation, participation in international organizations, and the adaptation of national legislation to the conditions of the global market.

Main trends and forecasts for the development of international trade. In the 21st century, international trade continues to develop dynamically under the influence of both traditional economic factors and new global processes, in particular digitalization, geopolitical changes, and environmental challenges. Both the structure of trade and its geography are changing, and the role of new technologies and global value chains is growing.

One of the key trends is the intensification of globalization. The global economy is becoming increasingly integrated, leading to growth in the volume of exports and imports of goods and services. Transnational corporations are actively involved in these processes, forming supply, production, and distribution networks in different countries.

Digital platforms and innovative technologies play a significant role in the development of international trade. E-commerce, automation, artificial intelligence, and blockchain are changing the classic models of logistics, contracting, and settlements. As a result, international trade is becoming faster, more convenient, and more accessible even for small and medium-sized businesses.

Another trend is the regionalization of trade relations. Within regional integration associations (EU, USMCA, ASEAN, etc.), internal trade is deepening, while protectionist measures are increasing at the global level (Lukyanenko et al., 2010).

There is also growing attention to sustainable development and the "green economy." The climate agreement (Paris Agreement), decarbonization policies, and CO_2 emissions controls are increasingly influencing the structure of trade. Countries are focusing on environmentally friendly technologies, carbon regulation, and certification of goods according to "green" standards.

Forecasts by international organizations, including the World Trade Organization (WTO), the IMF, and the World Bank, indicate further growth in world trade, albeit with periodic slowdowns due to global crises (such as the COVID-19 pandemic or geopolitical conflicts).

In the future, competition is expected to intensify, the need to adapt to rapid technological changes will arise, and the focus will shift from quantitative trade indicators to the quality, ethics, and sustainability of trade relations.

As for the globalization of the world economy, globalization has become a powerful factor shaping economic, political, social, and cultural processes in the modern world. It significantly influences the nature of international trade, economic relations between states, the activities of transnational businesses, and the functioning of the global market as a whole. The world economy is turning into a single integrated space where national borders are increasingly less of a barrier to the movement of goods, capital, information, and labor (Methodology for calculating the level of economic security of Ukraine, 2025).

Globalization affects not only the economy, but also political relations, cultural identity, and the information space, so its impact on the development of world trade requires systematic analysis. In this context, it is particularly important to study the preconditions for globalization processes, their positive and negative consequences, and possible ways to respond to the challenges they pose.

One of the main problems is that the benefits of globalization are distributed extremely unevenly. Economically developed countries reap the greatest benefits. In developing countries, globalization often has negative consequences: the destruction of traditional ways of life, reduced competitiveness of local production, rising unemployment, and increased social inequality.

In addition, globalization contributes to the loss of national sovereignty. Decision-making in key areas of the economy and finance increasingly depends on international organizations and transnational corporations, which leads to a reduction in states' control over their own economies (OECD, 2025).

The growing interdependence of different countries' economies increases the risk of the spread of crises. If an economic crisis occurs in one country, it can easily spread to others through financial, trade, and other ties, threatening the emergence of global crises (Pasternak-Taranushenko, 1994).

Another problem is increased competition. Due to globalization, small and medium-sized enterprises are forced to compete with transnational corporations that have significantly greater resources. This often leads to local businesses being forced out of the market. Globalization also contributes to cultural unification and the displacement of traditional cultures, languages, and customs, which in the long term can lead to a loss of national identity. Thus, despite its advantages, globalization also poses serious threats. In this regard, there is a need to develop effective mechanisms for regulating and adapting economies to new global conditions. Economic globalization is most often understood as a rapid increase in the flow of goods, investments, loans, information, exchanges of people and ideas, as well as the expansion of their geographical distribution. The global economy has become more prone to economic crises and deep recessions that spread suddenly from one country to another (Manual on education in the field of human rights with the participation of youth, 2025).

Political scandals arising from the illegal use of foreign capital in our country or the opening of secret accounts and businesses in offshore zones by officials, which is currently taking place in our state, and ill-considered foreign borrowing policies are indicators of the absence of a “secure” economic system in the country (Koval, 2024).

According to experts, the most negative threats to economic security at the regional and national levels are currently:

- significant differentiation in income levels among the population;
- deterioration in the structure of nutrition due to reduced consumption of protein products;
- an increase in the number of poor people whose income has fallen below the subsistence level as a result of inflation.

The consequences of these threats, which are most significant for economic security, are a decline in birth rates and an increase in mortality, the gradual depletion of the nation's gene pool due to the deterioration of material living conditions, and an ineffective healthcare system. We also cannot fail to note that the hostilities that began in 2014 significantly worsened the situation, and finally, Russia's full-scale invasion of Ukraine on February 24, 2022, had a serious impact on our gene pool (Sukhorukov & Ladyuk, 2007).

Today, Ukraine faces a number of problems that threaten its economic security. These include the worsening economic crisis amid armed aggression by the Russian Federation, rising corruption, declining living standards and rising unemployment, the shadow economy, a sharp decline in real GDP, and the loss of the country's investment attractiveness.

Economic security, manifesting itself in other areas of national security, penetrating them and interacting with them, accumulates their influence, while remaining the foundation (basis) of national security.

Economic intelligence, defined as a system of information networks that searches for, processes, and disseminates information necessary for the national economy and its entities, plays a key role in ensuring economic security. In addition, economic intelligence is designed to play a key role in ensuring Ukraine's financial security from external threats.

The financial component of economic security lies in the ability of its bodies to ensure the stability of the country's economic development, while neutralizing the impact of global crises and shadow structures on the economic and political systems. The financial component can be ensured by various instruments, including a range of measures to prevent capital flight abroad, attract foreign capital, and prevent and combat crimes and offences in the field of financial offences (Svystun & Levkova, 2017).

Economic security and the stability of the financial component can be measured by a whole group of indicators, such as:

- budget deficit;
- inflation rate;
- stability of the national currency;

- dynamics of external and internal debt, etc.

The processes of globalization, which have affected all areas of the world economy, have a significant impact on the economic security of individual states. On the one hand, globalization creates new opportunities for development – expansion of markets, inflow of investments, and dissemination of innovative technologies. At the same time, it creates a number of external threats that can weaken the national economy, undermine its competitiveness, and make it more dependent on external factors.

One of the main reasons for these threats is the rapid development of the transnationalization of economic ties and the internationalization of the global economy. In the context of open national markets, countries become more vulnerable to global fluctuations, crises, and external shocks. Economic activity increasingly goes beyond national jurisdictions, making it difficult to control financial flows and the movement of capital and goods (Shemaeva, 2009).

The second important reason is the growing autonomy of large players in the transnational economy–transnational corporations (TNCs). They have significant financial, technological, and information resources, which allows them to influence the economic policies of states and shape global trade and investment trends. As a result, national governments often find themselves dependent on the interests of global business, which may conflict with strategic economic security objectives.

Another factor is the high degree of mobility and interconnection of financial markets, reinforced by the development of modern information and communication technologies. Global financial flows move at an extraordinary speed, which increases the risks for national currency systems.

Therefore, in the context of globalization, external threats to economic security are caused not only by the expansion of global economic ties, but also by the deepening dependence of national economies on global processes. Therefore, to ensure Ukraine's stability and competitiveness, it is necessary to develop an effective system for monitoring external risks, diversify economic ties, and develop strategies for adapting to dynamic changes in the global market (Shkarlet, 2007).

In the current conditions of global instability, the issue of strengthening Ukraine's economic security is becoming particularly relevant. External challenges, such as geopolitical tensions, financial dependence, and technological backwardness, require a comprehensive approach to building a sustainable national economy. An effective economic security system must be based on a balanced combination of internal and external protection

https://doi.org/10.36690/PUBADM

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

mechanisms. Its improvement is only possible through a combination of state regulation, institutional stability, and support for national producers.

It is advisable to develop ways to improve Ukraine's *economic security system:*

1. *Regulation* of foreign participation in the national economy. Setting limits on foreign participation in the capital of domestic enterprises is an important prerequisite for preserving economic sovereignty. Sectoral restrictions or prohibitions on foreign investors' participation in strategic areas–such as energy, transport, and defense–minimize the risks of losing control over critical resources. At the same time, it is necessary to implement investment screening mechanisms to identify potential threats in a timely manner.

2. *Protection of the domestic market and competitive environment*. Strengthening economic security requires creating conditions for fair competition and preventing monopolization. It is necessary to apply antitrust measures to companies that distort market conditions. State support for national businesses, especially small and medium-sized enterprises, which form the basis of the country's economic independence, plays an important role.

3. *Technological and production independence*. Strengthening the technological potential of the state should be a priority of economic policy. An important condition is the introduction of requirements for the localisation of production and the promotion of the use of local resources and components. At the same time, innovative infrastructure should be developed – science parks, technoparks, start-up incubators – which will contribute to the technological renewal of the economy.

4. *Control of financial flows and borrowing*. An effective economic security system requires transparent control over the attraction and use of foreign funds. It is necessary to introduce effective mechanisms for monitoring external borrowing, ensure transparency of information on public debt, and improve the efficiency of financial resource management. It is also important to stimulate domestic sources of investment as an alternative to external loans.

5. *Institutional and regulatory support*. Improving the legislative framework in the field of economic security is the basis for effective public administration. Coordination is needed between the authorities responsible for monitoring and responding to economic threats. It is important to develop a comprehensive National Economic Security Strategy that combines long-term development goals with current protection measures (WTO, 2025).

Therefore, improving Ukraine's economic security system requires a systematic and multi-level approach. It should include effective regulation of foreign capital, strengthening the domestic market, developing technological independence, and controlling financial flows. The institutional capacity of the state plays an important role in ensuring coordination between all economic policy actors. The implementation of the proposed measures will contribute to the formation of a sustainable, competitive, and independent economy capable of withstanding global challenges.

Let us analyze regional economic security, because in general terms, the goal of regional economic security is to achieve (maintain) a certain state of the economy by ensuring favorable conditions and factors. At the same time, the level of development of a country's economy may be high, but in times of crisis, the state of the economy deteriorates. In reality, the regional economy cannot function exclusively in an autonomous mode, because there are always “external” supplies, financial flows, and even external markets. However, due to current realities, including the need for import substitution, one of the tasks of regional economic security is to reduce the dependence of the regional economy on external and internal threats of a decline in key socio-economic indicators of regional development (Table 3.15).

3. External threats of globalization and directions for strengthening Ukraine’s economic security. Threats to economic security can lead to imbalances in the activities of economic entities at any level, from individual enterprises to the entire national economy. They manifest themselves in the form of financial instability, loss of competitiveness, inefficient use of resources, and a decline in the standard of living of the population. Economic security has become a strategic goal at the national level, since social, political, military, technological, food, and other components of national security directly depend on the stability of the economic sphere. Ensuring stable economic growth, improving the well-being of citizens, and sustainable development of the state are the foundation of its economic stability and prosperity (Shcherbyna, 2006).

Threats to the economic security of the state vary in nature and impact. They can be both internal (ineffective state policy, corruption, shadow economy, low level of innovation) and external (economic pressure from other countries, fluctuations in world markets, financial crises, armed conflicts). The correct classification and assessment of these threats plays a key role in the process of strategic management and the formation of an effective economic security system.

Table 3.15. The essential and structural characteristics of the national security system are divided into types of security according to the nature of threats and dangers

Type of security	Nature of threat sources	Brief description
Internal security	Internal (endogenous) threats – political instability, corruption, crime, social tension, economic inequality	Provides protection for the state against threats arising within the country and aims to preserve political, social, and economic stability.
External security	External (exogenous) threats – military aggression, external economic pressure, sanctions, interference in internal affairs, information attacks	Aimed at protecting state sovereignty, territorial integrity, and national interests from the influence of other states or international actors
Political security	Political factors of both domestic and foreign origin	Guarantees the stability of the political system, the effectiveness of public administration, the legitimacy of power, and the prevention of usurpation.
Economic security	Internal and external economic threats – crises, inflation, debt dependency, energy vulnerability	Ensures the stability and independence of the national economy, its ability to self-develop and protect against destructive influences
Social security	Socio-demographic and humanitarian threats – unemployment, poverty, migration, decline in quality of life	Focused on maintaining social stability, justice, public welfare, and social cohesion
Military security	External military threats – aggression, armed conflicts, terrorism	Ensures the protection of the state from military aggression, maintains defense capabilities, and develops the Armed Forces.
Ecological security security	Technogenic, natural, and anthropogenic threats	Aimed at preventing environmental disasters, preserving the natural environment, and ensuring sustainable development
Information security	Internal and external information threats – cyberattacks, disinformation, propaganda	Provides protection for the information space, state data, public awareness, and critical infrastructure

Source: compiled based on data from (Sidenko, 2012; Shemaeva, 2009; Shkarlet, 2007; Shlemko & Binko, 1997; Shnipko, 2006)

Many threats are intensifying under the influence of globalization processes that have been developing over the past decades and encompass all spheres of the global economy. Globalization is an evolutionary trend in the development of society that contributes to the formation of a single global economic space. At the same time, this phenomenon is controversial: along with expanding economic opportunities, it creates new risks and challenges for national security (Yuskiv, 2009). The positive effects of globalization are evident in the development of international relations, the intensification of import and export processes, the expansion of investment flows, and the strengthening of cultural and scientific ties between countries. However, the downside of this process is the growing dependence of national economies on external markets, the instability of the global financial system, the influence of transnational corporations, and the intensification of socio-economic inequality. In addition, globalization contributes to the spread of crises through the rapid transmission of negative economic impulses between countries.

Thus, summarizing the main threats to economic security associated with globalization processes, we can conclude that they cover the most important areas of the national economy and directly affect human life. In the context of growing interdependence of world markets, ensuring the economic security of the state requires a systematic approach that combines adaptation to global processes with the protection of strategic national interests. Only under such conditions is it possible to build a stable, competitive economy capable of responding effectively to the challenges of a globalized world.

Conclusions. The study found that in the context of global transformations, the digital revolution, and growing geopolitical instability, the issue of economic security is becoming strategically important. Not only economic stability but also political independence, social stability, and the country's competitiveness in the global arena depend on the level of economic security.

Modern economic security is shaped by the rapid digitalization of management processes, which requires a transition from traditional management methods to innovative models based on the use of digital technologies, analytical platforms, and artificial intelligence. At the same time, digital transformation, in addition to opportunities, also creates new threats – from cyber risks and loss of information sovereignty to technological dependence on external suppliers.

For Ukraine, the issue of economic security is particularly critical, given the consequences of armed aggression, the destruction of industrial infrastructure, demographic losses, and energy vulnerability. Under such conditions, public administration must be reoriented toward the principles of digital transparency, adaptability, and innovation. The use of electronic risk monitoring systems, digital security dashboards, and analytical forecasting tools allows for timely response to crises and minimizes the impact of external threats.

The paper proves that economic security is a multi-component system that includes financial, energy, social, innovation and technological, raw material and resource, food, and foreign economic security. Each of these components forms the basis of national resilience, and their balance determines the overall level of economic protection of the state.

Globalization processes have a dual impact on economic security: they open up new opportunities for development, investment, innovation, and market expansion, but they also increase threats such as financial dependence, technological vulnerability, brain drain, and loss of economic sovereignty. It has been determined that the state's ability to effectively adapt to globalization changes without losing control over strategic sectors of the economy is a key factor in its security.

Particular attention is paid to the role of international institutions – the IMF, the World Bank, the WTO – which shape global rules of economic interaction. Their activities create both additional opportunities for integration and risks of increased external influence on national economic policy. Ukraine's accession to the WTO was an important step towards integration into the world economy, but it requires a balanced combination of market openness with mechanisms for protecting national producers.

International trade, as a key indicator of economic security, is being transformed under the influence of digitalization, regionalization, and environmental trends. The role of e-commerce, intellectual property, and innovative technologies is growing. However, at the same time, the dependence of national economies on external markets is increasing, which can lead to a loss of internal stability in the event of global crises.

Thus, ensuring economic security in the context of globalization involves:

- development of one's own innovation potential and scientific and technological base;
- diversification of energy and trade relations;
- strengthening financial stability and control over capital movements;
- improving cyber and information security mechanisms;
- developing a system of strategic forecasting and analytical risk monitoring.

Summarizing the results of the study, it can be stated that economic security in the 21st century should be considered not only as a state of security of the economic system, but as a dynamic process of adaptation, development and stability of the state in the face of global changes. Effective public administration in this area should be based on a combination of innovative potential, digital technologies and flexible management solutions focused on long-term stability and independence of the national economy.

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. Council of Europe. (2025). *Manual on education in the field of human rights with the participation of youth: Globalization*. Retrieved from: https://www.coe.int/uk/web/compass/globalisation
2. Datskiv, R. M. (2004). Economic security in the global dimension. *Current Economic Problems*, 7(37), 143–153.
3. Duleba, N. V. (2008). Research on the transformation of the concept of "economic security of an enterprise". Retrieved from http://www.economy.nayka.com.ua/?op=1&z=2387
4. Dyba, O., & Osadchy, E. (2014). The impact of globalization on the socio-economic state of Ukraine. *Securities Market in Ukraine*, 7, 19–28.
5. Fedorenko, T., & Zahorodnia, A. (2024). Economic security of the enterprise: Modern challenges and threats. *Intellectualization of Logistics and Supply Chain Management*, 26, 75–79. https://doi.org/10.46783/smart-scm/2024-26-6
6. Fedorenko, T., Dolynskiy, S., & Zahorodnia, A. (2022). An evolutionary approach to the interpretation of the term "economic security of enterprises". *International Journal of Innovative Technologies in Economy*, 4(40), 1–6. https://doi.org/10.31435/rsglobal_ijite/30122022/7926
7. Koval, Ya. (2024). Peculiarities of information and analytical support in decision-making within government bodies. *Public Administration and Law Review*, 3(19), 4–16. https://doi.org/10.36690/2674-5216-2024-3-4-16
8. Koval, Ya., Fedorenko, T., & Zahorodnia, A. (2024). Information and analytical activity in the system of economic security of the enterprise. *Intellectualization of Logistics and Supply Chain Management*, 24, 83–88. https://doi.org/10.46783/smart-scm/2024-24-9
9. Kovalenko, M. A., Nagorodna, I. I., & Radvanska, N. V. (2009). *Economic security of a corporate enterprise*. Kharkiv: Oldi-plus.
10. Kryvovyazyuk, I. V. (2013). *Economic diagnostics*. Kyiv: TsUL.
11. Kutsyk, P. O., Kovtun, O. I., & Bashtyanin, G. I. (2015). *Global economy: Principles of formation, functioning and development*. Lviv: Merts Acad.
12. Laptiev, S., Mazur, I., Koval, Ya., & Laptiev, M. (2024). Business reputation and resilience: Digital skill strategies in a transformative era. In M. Denysenko, L. Khudoliy, & S. Laptiev (Eds.), *Digital skills in a digital society: Requirements and challenges* (pp. 189–209). Estonia: Scientific Center of Innovative Research. https://doi.org/10.36690/DSDS-189-209
13. Levitt, T. (2025). The globalization of markets. *Harvard Business Review*. Retrieved from https://hbr.org/1983/05/the-globalization-of-markets

14. Lukyanenko, D., Poruchnik, A., & Stolyarchuk, Ya. (2010). Global financial imbalances and their economic consequences. *Journal of European Economy*, 9(1), 73–92.
15. MacFarlane, S. N., & Khong, Y. F. (Eds.). (2006). *Human security and the UN: A critical history* (United Nations intellectual history project, illustrated ed.). Bloomington, IN: Indiana University Press.
16. Ministry of Economy of Ukraine. (2013). *Methodology for calculating the level of economic security of Ukraine*. Retrieved from: https://zakon.rada.gov.ua
17. Organization for Economic Cooperation and Development. (2025). *OECD*. Retrieved from: http://www.oecd.org
18. Pasternak-Taranushenko, G. A. (1994). *Economic security of the state*. Kyiv: Institute of State Administration and Self-Government at the Ministry of Finance of Ukraine.
19. Pihariiev, Yu., & Kosteniuk, N. (2021). Digitalization of public administration as a factor of Ukraine's digital transformation. *Aktualni problemy derzhavnoho upravlinnia*, 2(83), 92–96. https://doi.org/10.35432/1993-8330appa2832021237257
20. Reznik, N. P., Zahorodnia, A. S., & Chornenka, L. M. (2021). Analysis of the logistics component of the economic security system of enterprises. *International Journal of Innovative Technologies in Economy*, 4(36), 109–113.
21. Robertson, R. (1992). *Globalization: Social theory and global culture*. London: Sage.
22. Shcherbyna, V. M. (2006). Information security of economic security of enterprises and institutions. *Current Problems of Economy*, 10(64), 220–225.
23. Shemaeva, L. G. (2009). *Ensuring the economic security of an enterprise based on the management of strategic interaction with external entities*. Kyiv: National Security and Defense Council of Ukraine, National Institute of International Security Problems.
24. Shkarlet, S. M. (2007). Evolution of the category "security" in the scientific and economic environment. *Formation of Market Relations*, 6, 7–12.
25. Shlemko, V. T., & Binko, I. F. (1997). *Economic security of Ukraine: Essence and directions of provision*. Kyiv: NISD.
26. Shnipko, O. S. (2006). Types and factors of security of hierarchical economic systems: Theoretical and methodological aspect. *Current Problems of Economy*, 5(59), 78–85.
27. Sidenko, V. R. (2012). Modification of the world economy under the influence of the latest factors of the global transformation crisis. *Economy of Ukraine*, 5, 18–31.
28. Sukhorukov, A. I., & Ladyuk, O. D. (2007). *Financial security of the state: A textbook*. Kyiv: Center for Educational Literature.
29. Svystun, L. A., & Levkova, R. M. (2017). Improving the cost management system of an enterprise in an unstable economy. *Economy and Region*, 4, 57–62.
30. Syrotin, V. D. (2023). Features of digitalization in the field of public administration. *Problemy suchasnykh transformatsii. Seriia: Pravo, publichne upravlinnia ta administruvannia*, 9. https://doi.org/10.54929/2786-5746-2023-9-02-06
31. Varnalii, Z. S. (Ed.). (2009). *Economic security: A textbook*. Kyiv: Knowledge.

32. Vlasyuk, O. S. (2008). *Theory and practice of economic security in the system of economic science*. Kyiv: National Institute of International Security Problems under the National Security and Defense Council of Ukraine.
33. Vorobyov, V. I. (2011). Methodological foundations of building a comprehensive system of economic security of an enterprise. *Scientific Notes*, 1(19), 38–44.
34. World Trade Organization. (n.d.). *WTO*. Retrieved from http://www.wto.org
35. Yuskiv, B. M. (2009). *Globalization and labor migration in Europe*. [Monograph].
36. Zahorodnia, A. (2024). International organizations as a tool for the development of the world economy. *Herald of Khmelnytskyi National University. Economic Sciences*, 336(6), 567–572. https://doi.org/10.31891/2307-5740-2024-336-84
37. Zahorodnia, A. (2025). The evolution and impact of the North American Free Trade Agreement (NAFTA) on the economic development of participating countries. *Herald of Khmelnytskyi National University. Economic Sciences*, 342(3[1]), 298–305. https://doi.org/10.31891/2307-5740-2025-342-3(1)-42
38. Zahorodnia, A. S., & Sharma, M. (2024). International experience in business process management: Relations between Ukraine and the Republic of India. *Intellectualization of Logistics and Supply Chain Management*, 28, 71–77. https://doi.org/10.46783/smart-scm/2024-28-6
39. Zakharov, O. I. (2015). The mechanism of interaction between government and business in the system of economic security. *Collection of Scientific Works of Cherkasy State Technological University. Economic Sciences*, 33(3), 151.
40. Zakharov, O. I. (2016). Globalization and its impact on economic security. *Scientific Notes of the University "KROK"*, 43, 4–13.

Section 3.3. Public Governance of Energy Policy: Evidence from the Visegrád Group Countries

Dmytro Tkach[1]

[1]Ph.D. in Economics, Research Fellow, Center for Innovations and Technological Development, State Institution "Dobrov Institute for Scientific and Technological Potential and Science History Studies of the NAS of Ukraine", Kyiv, Ukraine, ORCID: https://orcid.org/0009-0009-1401-3324

Citation:
Tkach, D. (2025). Public Governance of Energy Policy: Evidence from the Visegrád Group Countries. In O. Akimov (Ed.), *Public Administration 4.0: Leveraging Digital Tools for Effective Governance*. 262 p. (pp. 206-240). Scientific Center of Innovative Research. https://doi.org/10.36690/PUBADM-206-240

Abstract. *The study examines the public governance of energy transformation in the Visegrád Group countries in the context of European climate neutrality goals and post-2022 energy security shocks, focusing on how state institutions reconcile decarbonization commitments with dependence on fossil fuels and Russian energy resources. The objective is to analyse the role of the state in designing and implementing energy transitions in Poland, Czechia, Slovakia, and Hungary, to identify convergent and divergent governance models, and to outline implications for regional cooperation and broader European integration in the energy sector. Methodologically, the study applies a comparative case study design that combines analysis of EU strategic frameworks (European Green Deal, REPowerEU) with document analysis of national energy and climate plans, sectoral legislation, and large-scale infrastructure projects, complemented by an interpretive reading of theoretical approaches to European integration and energy policy. The main results show that energy transformation in the V4 is highly uneven, reflecting different starting structures, resource endowments, and political preferences. Poland prioritizes large-scale offshore wind and gradual coal phase-out with emerging CCUS, Slovakia builds its strategy around an expanded nuclear fleet with moderate RES growth, Hungary pursues a pragmatic mix of nuclear expansion and rapid solar development while maintaining deep ties to Russian energy, and Czechia accelerates coal phase-out through nuclear investment and a controlled scaling-up of renewables. Across all cases, nuclear energy appears as a long-term stabilizing pillar, while integration into EU electricity and gas markets, regional interconnections, and financial instruments of the European Investment Bank support the transition but do not remove national asymmetries. The conclusions highlight the centrality of the state as a strategic planner, regulator, investor, and mediator of social impacts, as well as the need to balance climate objectives with security and affordability. Directions for further research include a deeper assessment of distributional and regional justice in coal-dependent territories, the interaction between CBAM and industrial competitiveness in V4 economies, and the potential transfer of governance lessons to Ukraine's post-war energy transformation.*

Keywords: *energy transformation; Visegrad Group; renewable energy sources; decarbonization; energy security; coal dependence; nuclear energy; European Green Deal; climate policy; energy transition; V4; energy cooperation; sustainable development.*

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

1. The state as an organizer of energy transformation in the Visegrad Four under EU climate goals and post-2022 energy security pressures. The Visegrad Four (Poland, the Czech Republic, Slovakia, and Hungary) entered the 2020s at the intersection of three policy imperatives that mutually constrain state decision making (European Commission, 2019). First, EU climate governance requires a credible pathway toward climate neutrality by 2050, supported by binding intermediate targets and sectoral instruments (European Commission, 2019). Second, Russia's full scale invasion of Ukraine in 2022 exposed structural vulnerabilities created by fossil fuel import dependence and accelerated the securitization of energy policy, especially in gas and oil supply chains (OSW Centre for Eastern Studies, 2022; Reuters, 2022, April 27). Third, the transformation is politically feasible only if it is socially managed, particularly in coal dependent regions and in systems where affordability is central to legitimacy (OECD, 2021). In this context, the state is not merely a regulator but an organizer that coordinates planning, investment, infrastructure, and distributional mitigation across multiple levels of governance (European Commission, 2019). This role is reinforced by the EU's multi level policy architecture, where national strategies must align with European targets while remaining responsive to domestic constraints (Bache, 2008; Dunn, 2012).

EU framework conditions that structure national choices in V4. The European Green Deal, presented in 2019, established the overarching political and regulatory direction for EU decarbonization, including climate neutrality by 2050 and a reorientation of investment and industrial policy (European Commission, 2019). The legal and policy environment has since been reinforced through subsequent packages and sectoral rules, with renewable energy targets serving as a key constraint for national energy mixes (European Commission, 2023). Under the updated Renewable Energy Directive adopted in 2023, the EU set a 2030 target of at least 42.5% renewables in gross final energy consumption, with an indicative ambition to reach 45%, which directly shapes V4 planning, permitting, and grid integration priorities (European Commission, 2023). After 2022, the EU added an explicit security and affordability logic through REPowerEU, which frames accelerated deployment of renewables, energy efficiency, and infrastructure as tools for reducing dependence on imported fossil fuels (European Investment Bank, 2023). This reframing matters for V4 because it legitimizes faster and more interventionist state action, including public financing, expedited permitting, and infrastructure upgrades.

A crucial element of state capacity in this framework is access to long

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

term finance for grids and clean generation (European Investment Bank, 2023). The European Investment Bank positioned its REPowerEU+ commitment as a major channel for mobilizing capital, increasing its support target to €45 billion until 2027, intended to catalyze much larger volumes of investment (European Investment Bank, 2023). For V4 governments, this creates both an opportunity and an obligation: domestic planning must be sufficiently coherent and bankable to absorb European financing, while administrative systems must handle procurement, permitting, and implementation at scale (European Investment Bank, 2023).

The post-2022 security shock and the reconfiguration of regional politics. The gas crisis triggered by Russia's use of supply leverage made energy security immediately operational, not only as a strategic narrative but as an acute governance problem (OSW Centre for Eastern Studies, 2022; Reuters, 2022, April 27). Russia's Gazprom halted gas supplies to Poland and Bulgaria in April 2022 amid a payments dispute, signaling that supply interruptions could occur rapidly and with political intent (OSW Centre for Eastern Studies, 2022; Reuters, 2022, April 27). This experience pushed governments to accelerate diversification, expand storage, and invest in interconnectors and alternative routes (Visegrad Group, 2010). It also strengthened the EU level logic of phasing out Russian fossil fuel imports, culminating in a Commission roadmap published in May 2025 and follow up proposals that envisage ending Russian oil imports by the end of 2027 and phasing out Russian natural gas imports on a defined timeline (European Commission, 2025; European Parliament, 2025).

At the same time, security pressures contributed to political fragmentation within the V4, particularly regarding Russia policy and the governance of solidarity mechanisms (Fisher, 2024). Analytical assessments increasingly described the group as functioning like a "V2+2", with Warsaw and Prague more consistently aligned with a pro Ukraine stance, while Bratislava and Budapest adopted more ambiguous or obstructionist positions in EU level bargaining (Fisher, 2024). This divergence matters for energy governance because joint regional initiatives depend on trust, coordinated investment, and shared risk assessments, all of which weaken when geopolitical preferences diverge (Fisher, 2024).

Poland. Poland's state strategy is anchored in long term planning instruments that define a transformation pathway while explicitly linking decarbonization with security and industrial modernization (Ministerstwo Klimatu i Środowiska, 2021). The government adopted the Energy Policy of Poland until 2040 (EPP2040) in February 2021, framing the transition as a managed process combining new capacity, infrastructure, and regulatory

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

reform (Ministerstwo Klimatu i Środowiska, 2021). In investment terms, European Parliament analysis of Poland’s climate and energy planning highlights very large required outlays, including an estimate of PLN 792 billion for implementation needs in the 2026 to 2030 period within the broader national planning context (European Parliament, 2024). The 2022 supply cut episode reinforced Poland’s prioritization of supply resilience, adding urgency to diversification measures and reducing tolerance for strategic dependence (OSW Centre for Eastern Studies, 2022; Reuters, 2022, April 27).

A distinctive element of Poland’s state enabled pathway is the pursuit of small modular reactors alongside broader nuclear planning (U.S. Department of State, 2023, September 7). U.S. backed programs such as Project Phoenix and the NEXT initiative were designed to support coal to SMR conversion pathways in Europe, explicitly connecting climate goals with local employment and security rationales (U.S. Department of State, 2023, September 7). Poland’s Orlen Synthos Green Energy has been identified among Project Phoenix participants, and related reporting notes support for feasibility work connected to SMR deployment (Orlen Synthos Green Energy, 2023; U.S. Department of State, 2023, September 7). In parallel, ORLEN and Synthos have publicly communicated steps toward Poland’s first BWRX-300 SMR project, indicating that state strategy, corporate execution, and transatlantic technology access are being combined in a single investment logic (ORLEN, 2025; Reuters, 2025, August 28).

Slovakia. Slovakia’s transformation model relies heavily on nuclear generation as the backbone of low carbon electricity supply and as a stabilizer for the wider system (International Atomic Energy Agency, 2025; Slovenské elektrárne, n.d.). The completion and commissioning progress of Mochovce Unit 3 has been a central milestone, with reporting indicating successful commissioning steps in 2023 and formal integration into the operator’s nuclear fleet (World Nuclear News, 2023, October 17). Complementary technical information from the operator emphasizes the scale and system role of Mochovce 3 and 4, reinforcing the interpretation of nuclear completion as a state level strategic asset rather than a purely corporate project (Slovenské elektrárne, n.d.). International nuclear databases and country profiles similarly document the operational timeline and the broader prominence of nuclear power in Slovakia’s electricity mix (International Atomic Energy Agency, 2025; Slovakia Energy Profile, 2025).

At the same time, Slovakia has faced acute exposure to uncertainty around gas transit arrangements, especially as the Russia Ukraine transit agreement approached expiry at the end of 2024, making alternative sourcing a practical necessity (Reuters, 2024, November 13). In response, Slovakia's main gas buyer SPP signed a short term pilot contract to purchase natural gas from Azerbaijan in late 2024, explicitly linking the move to preparation for possible changes in Russian supply routes via Ukraine (Reuters, 2024, November 13). This illustrates a typical state organizing function in hybrid energy systems: while electricity decarbonization may be nuclear centered, gas security still requires targeted diversification, diplomatic engagement, and contractual experimentation to manage transition risk (Reuters, 2024, November 13).

Czech Republic. The Czech Republic combines a historically coal intensive power sector with a strong national preference for nuclear energy as a strategic pillar of system stability (Ember, 2020; OECD, 2021). Independent analysis of the Czech power mix during the crisis years underscores the continuing weight of coal in electricity generation, including estimates around the low forties percent in 2022, which frames decarbonization as both technically and politically demanding (Ember, 2020). International institutional assessments similarly stress that coal remains central but that the strategic issue is the timing and governance of exit rather than whether an exit will occur (OECD, 2021). In this context, the state's organizing role is expressed through long horizon nuclear planning, investment coordination, and the management of social and regional impacts, while also scaling renewables within grid and permitting constraints (OECD, 2021; World Nuclear News, 2025, June 5).

Grid modernization becomes a decisive governance lever because it determines the absorptive capacity for renewables and the resilience of the system under stress (European Investment Bank, 2024). The European Investment Bank has supported Czech electricity infrastructure modernization, including a €400 million financing arrangement connected to distribution upgrades, aligning with national objectives around resilience and integration of new generation (European Investment Bank, 2024). This type of intervention illustrates how state capacity depends on blending domestic planning with EU level financing mechanisms, since the grid is both a technical asset and a political instrument for affordability and reliability (European Investment Bank, 2024).

Hungary. Hungary represents the most contested case in V4 because it has sought to preserve substantial energy ties with Russia while simultaneously expanding low carbon capacity (Reuters, 2025, December 8). Reuters reporting in December 2025 described continued reliance on Russian gas flows via TurkStream, referencing Hungary's 2021 long term contract for 4.5 bcm annually and reporting higher import volumes in 2025, alongside political efforts to ensure route stability (Reuters, 2025, December 8). This indicates a state choice to prioritize continuity and price considerations even when EU level policy is oriented toward accelerated phase out of Russian fossil energy (European Commission, 2025; European Parliament, 2025).

In electricity, Hungary's decarbonization profile is anchored by nuclear output from the Paks plant, which has provided roughly half of domestic electricity generation in recent years according to international profiles and operator linked reporting (International Atomic Energy Agency, 2022; International Trade Administration, 2024). Hungary has also pursued rapid solar deployment, with sectoral reporting indicating large annual additions and a steep rise in cumulative capacity, reflecting a dual track strategy in which nuclear provides baseload stability while solar expands quickly where permitting and economics are favorable (International Trade Administration, 2024). The resulting policy configuration can be described as a state managed portfolio that delivers low carbon electricity growth but remains exposed to geopolitical criticism and systemic risk because fuel import dependence is only partially reduced (European Commission, 2025; Reuters, 2025, December 8).

Cross cutting obstacles and the political economy of implementation. Across the V4, progress in renewable deployment and emissions reduction has been uneven because the binding constraint is frequently not ambition but implementation capacity (European Commission, 2023). Permitting speed, grid access, storage, and balancing resources determine how quickly renewables can scale, while social acceptance and distributional fairness determine how stable policy can remain (European Investment Bank, 2023). The crisis years amplified the affordability dimension, leading households and firms to adopt decentralized solutions where feasible, which reshaped the relationship between the state and citizens (Mazač et al., 2024; Żuk, 2025). In several V4 settings, rapid growth in prosumer activity has functioned as a form of self protection against price volatility and uncertainty, effectively shifting part of the transformation burden to households and small firms (Mazač et al., 2024; Żuk, 2025). This bottom up dynamic can strengthen resilience but can also expose policy inconsistencies if tariff design, net metering, or subsidy regimes change abruptly (Żuk, 2025).

Another structural obstacle is the sequencing problem between coal exit and replacement capacity (OECD, 2021). Where coal remains a large share of generation, the state must coordinate multiple timelines: decommissioning, labor market transition, new firm investment, and infrastructure readiness (OECD, 2021). The Czech experience illustrates how coal dependence creates a narrow corridor for policy, since rapid exit without replacement and grid readiness risks reliability, while delayed exit risks EU compliance costs and stranded assets (Ember, 2020; OECD, 2021). Consequently, "just transition" is not an additional policy layer but a core state function that conditions feasibility (OECD, 2021).

Table 3.16. Comparative characteristics of the energy strategies of the V4 countries

Parameter	Poland	Czechia	Slovakia	Hungary
Main Strategy	Energy Policy to 2040 (EPP2040)	Balancing between nuclear and RES	Nuclear strategy with RES supplement	Dependence on Russia + nuclear energy
Position regarding Ukraine (2024)	Biggest defender, 4.7% GDP on defense	Active support for sanctions and military aid	Ambiguous position after Fico's return	Most pro-Russian position
Dependence on Russian gas (2020)	50%	55%	68%	61%
Dependence on Russian energy carriers (2024)	Disconnected since April 2022	Reduced	Diversifying	90% gas, 65% oil
Nuclear Energy	Development of new + SMR, participation in Phoenix Initiative	Strategic priority, expansion of fleet + SMR	Basis of decarbonization, new reactors 2023-2024	20% of energy balance, modernization
Share of low-carbon generation Target share of RES by 2030	In development	In development	>85% (including RES)	In development
Target share of RES by 2030	According to EU plans	According to EU plans	19.2%	-
Development of solar energy	Investments 792 billion zlotys in RES projects	400 million euros from EIB for ČEZ	New nuclear blocks	Modernization of nuclear infrastructure
Energy status	Importer	Importer	Net exporter from 2024	Importer

Source: (European Investment Bank, 2022)

Regional cooperation: infrastructure solidarity and lessons from earlier crises. V4 cooperation on energy security gained salience after the 2009 gas crisis, when supply disruptions highlighted the need for regional flexibility (Visegrad Group, 2010). The Declaration of the Budapest V4+ Energy Security Summit of February 2010 framed cooperation around infrastructure, interconnectivity, and solidarity, providing a political basis for measures such as reverse flows and enhanced storage (Visegrad Group, 2010). These instruments later became important for Central European resilience and for Ukraine's ability to reduce direct dependence on Russian gas imports, since reverse flow capacity and regional market access expanded the set of feasible supply options (Maksymak, 2018). This history demonstrates that state organizing capacity can be reinforced through regional coordination, but only if political trust and strategic priorities remain sufficiently aligned (Visegrad Group, 2010; Fisher, 2024).

The evidence across the four cases supports a general conclusion: in V4, energy transformation is state organized because the transition requires simultaneous coordination of long term planning, regulatory alignment, investment mobilization, and security management (European Commission, 2019; OECD, 2021). EU level targets and instruments define the boundary conditions, especially renewable energy obligations and the post 2022 security oriented REPowerEU logic (European Commission, 2023; European Investment Bank, 2023). The security shock of 2022 accelerated diversification and legitimized more interventionist policy tools, while the EU's later phase out agenda formalized the direction of travel for gas and oil dependence (European Commission, 2025; OSW Centre for Eastern Studies, 2022; Reuters, 2022, April 27). However, divergent geopolitical positions within V4 have reduced collective coherence, limiting the political capacity for unified regional leadership, even when infrastructure cooperation remains technically beneficial (Fisher, 2024; Visegrad Group, 2010).

A realistic strategic interpretation is that V4 states will increasingly pursue hybrid transition portfolios, combining nuclear expansion or life extension, rapid solar and wind deployment where feasible, and aggressive grid modernization, while using targeted diversification contracts to manage residual gas dependence during the transition period (European Investment Bank, 2024; International Atomic Energy Agency, 2022; International Atomic Energy Agency, 2025). Hungary's continued Russian gas reliance and Slovakia's pilot diversification toward Azerbaijani gas illustrate two different approaches to managing the same vulnerability, with distinct implications for EU solidarity and domestic affordability (Reuters, 2024, November 13; Reuters, 2025, December 8). Ultimately, the success of V4 energy transformation will depend on whether states can deliver implementation capacity at scale, protect legitimacy through just transition instruments, and align security imperatives with EU climate commitments in a way that remains institutionally stable over multiple electoral cycles (European Commission, 2023; OECD, 2021).

2. Theoretical foundations of European integration in energy. The EU Strategy for Energy System Integration (2020) conceptualizes integration as a systemic redesign of how energy is produced, moved, and consumed across sectors, with the explicit purpose of reducing emissions and resource use while maintaining security of supply (European Commission, 2020). It formulates three organizing principles. The first is circularity, understood as prioritizing energy efficiency and the reuse of energy streams, including waste heat and sector coupling solutions that reduce primary energy demand (European Commission, 2020). The second is electrification of end use consumption, which links decarbonization to the rapid expansion of clean power and to the modernization of networks so that electricity can substitute fossil fuels in transport, buildings, and parts of industry (European Commission, 2020). The third is the use of renewable and low carbon fuels, including hydrogen and sustainable biogases, where direct electrification is not technically feasible or cost effective, which repositions fuel markets as complementary to, rather than substitutes for, electrified systems (European Commission, 2020). In theoretical terms, the 2020 Strategy should be read as a policy attempt to align internal market integration with the European Green Deal's climate neutrality horizon, so that competition, infrastructure investment, and decarbonization become mutually reinforcing rather than sequential goals (European Commission, 2019; European Commission, 2020).

A second foundational layer concerns the internal energy market logic, especially the long running effort to dismantle vertically integrated market structures and replace them with regulated competition. The EU's market building agenda rests on unbundling, meaning the separation of supply and generation from transmission network operation to prevent discrimination in grid access and to promote competitive outcomes (European Commission, n.d.). This idea is institutionalized in the governance of the internal energy market through regulatory oversight, network access rules, and coordination among national regulators and system operators (European Commission, n.d.). The Energy Union framework further adds a strategic narrative that integrates energy security, solidarity, market completion, energy efficiency, decarbonization, and research and innovation into a single policy architecture, thereby widening the integration rationale beyond price competition to include resilience and long term transformation capacity (European Parliament, 2015; European Commission, 2015). For Central and Eastern Europe, this framework translates into practical requirements to comply with ENTSO E standards and cross border operational rules, and to participate in coordinated grid operation and market coupling mechanisms that enable cross border balancing and investment planning (ENTSO E, 2022; European Commission, 2018). In this respect, synchronization should be interpreted not simply as a technical event but as an institutional condition

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

that binds national energy systems into a shared operational and regulatory space, as illustrated by the emergency synchronization of Ukraine and Moldova with the Continental European system in 2022, which also redefined the geopolitical meaning of grid integration for the region (ENTSO E, 2022).

Neofunctionalism provides a classical explanation for why energy has repeatedly become a driver of deeper European integration. Haas argued that integration tends to generate spillover, meaning that cooperation in one sector creates functional pressures for cooperation in adjacent sectors, as institutions, markets, and interest groups adapt to new interdependencies (Haas, 1958). In energy, spillover is visible when cross border electricity trade requires common network codes, which then stimulates cooperation on balancing, adequacy, and investment planning, which in turn pushes toward stronger supranational coordination to manage systemic risks and externalities (European Commission, 2020; ENTSO E, 2022). The Energy Union and the Energy System Integration Strategy can therefore be understood as attempts to formalize spillover dynamics into deliberate governance design, especially by linking electrification and hydrogen deployment to infrastructure and market rules that must operate across borders (European Commission, 2015; European Commission, 2020). However, neofunctionalism alone is insufficient for explaining variation in outcomes, because energy is a domain where sovereignty concerns remain particularly salient and where national governments retain powerful tools over the choice of energy sources and system structure (Treaty on the Functioning of the European Union, 2012).

New intergovernmentalism is helpful in explaining why integration in energy often advances through coordination and joint problem solving rather than through straightforward delegation to supranational institutions. Bickerton, Hodson, and Puetter describe a post Maastricht pattern in which member states intensify cooperation and create governance arrangements, yet remain cautious about transferring core powers, relying instead on intergovernmental bargaining and consensus seeking formats (Bickerton et al., 2015). In energy, this pattern emerges because the costs of transition are unevenly distributed, security risks are nationally differentiated, and governments face strong domestic constraints from incumbents, regions, and voters. As a result, integration frequently proceeds through negotiated packages that allow flexibility, derogations, and differentiated implementation, even while common targets and market rules expand. The legal structure of Article 194 TFEU reflects this duality, because it codifies EU energy objectives in a spirit of solidarity and internal market functioning, but also preserves member states' authority over their energy mix and the general structure of supply, which anchors sovereignty within the constitutional framework of integration (Treaty on the Functioning of the European Union, 2012; EUR Lex, 2012).

Multi level governance complements these accounts by shifting attention from treaty level bargaining to the implementation arena, where supranational, national, regional, and local actors jointly shape outcomes. In energy, this is visible in the interaction of EU institutions that set targets and rules, national regulators and ministries that transpose and enforce them, system operators that implement operational standards, and subnational governments and energy communities that influence permitting, acceptance, and distributed generation (Bache, 2008; European Commission, n.d.). The energy transition amplifies this logic because decarbonization is increasingly implemented through projects with local footprints, such as wind and solar deployment, grid expansion, district heating modernization, and hydrogen infrastructure, all of which face place based constraints and distributional contestation. At the normative level, the emphasis on solidarity and environmental integration in Article 194 can be interpreted as providing legal support for distributive justice claims, since it embeds social and environmental considerations into the policy objectives that guide interpretation and design (Treaty on the Functioning of the European Union, 2012; Kaschny, 2023). Consequently, multi level governance is not a descriptive add on but a core explanatory lens for why formally shared EU goals produce uneven national trajectories.

The specificity of the V4 can be framed through Europeanization, understood as the domestic adaptation to EU objectives, rules, and policy styles, filtered through national political economy and energy system legacies. Empirical research on V4 implementation of EU energy goals indicates differentiated progress across Energy Union dimensions, with stronger convergence in decarbonization related metrics and greater divergence in infrastructure and final energy consumption patterns, reflecting both structural conditions and domestic policy choices (Wach, 2021). This differentiation is reinforced by internal heterogeneity in preferences and voting behavior on climate and energy files, where governments may align on some dossiers but diverge on others depending on industrial structure, security assessments, and fiscal capacity (Wach, 2021). From a theoretical standpoint, this suggests that the V4 cannot be modeled as a unitary actor within EU energy integration; instead, it represents a cluster of partially shared constraints with distinct national strategies. Therefore, the energy integration of V4 is best explained through a synthetic approach that combines neofunctionalist mechanisms of interdependence, new intergovernmentalist dynamics of sovereignty sensitive bargaining, and multi level governance patterns of implementation, especially under the compounded pressures of decarbonization and post 2022 security recalibration (European Commission, 2019; European Commission, 2020; Bickerton et al., 2015; Wach, 2021).

Table 3.17 systematizes the main theoretical lenses used to explain European integration in the energy sector and clarifies how each approach interprets the drivers, institutional mechanisms, and policy outcomes of integration.

Table 3.17. Theoretical approaches to European integration in the energy sector

Theoretical Approach	Main Provisions	Mechanisms of Integration	Application in Energy	Specifics for V4 Countries
Neofunctionalism (Ernst Haas)	Integration in one sector creates pressure for integration in adjacent sectors.	"Spillover" effects. Gradual transfer of powers to supranational bodies.	From ECSC to the energy market. Synchronization with ENTSO-E. Decarbonization by 2050.	The highest level of integration in decarbonization. Gradual adaptation to the goals of the "Green Deal".
New Intergovernmentalism	States retain sovereignty, preferring cooperation without the delegation of powers.	Intergovernmental agreements. Retention of national control. Limited transfer of powers.	Energy security as a national priority. Control over energy resources.	Particular jealousy regarding energy sovereignty. The largest variations in energy infrastructure.
Multilevel Governance	Interaction between different levels of government through a complex system of interdependent administrative levels.	Supranational level. National level. Regional level. Local level.	Coordination of energy policy. Participation of various actors. Vertical and horizontal integration.	Significant heterogeneity in voting in the EP. Different economic interests. Foreign policy positi
Theoretical Approach	Main Provisions	Mechanisms of Integration	Application in Energy	Specifics for V4 Countries

Source: (Borysova, O., & Rudnik, D., 2024)

The table 3.17 provides an analytical bridge between general theories of integration and the differentiated realities of the Visegrad countries.

The comparison indicates that no single theory fully captures the complexity of EU energy integration, because the sector simultaneously exhibits spillover driven deepening, intergovernmental constraint, and multi level implementation. Neofunctionalism best explains why technical interdependence and market coupling generate pressures for further harmonization, which is particularly visible in network coordination and climate target alignment. New intergovernmentalism clarifies why member states continue to defend sovereignty in energy security and energy mix decisions, producing differentiated commitments and uneven infrastructure convergence. Multilevel governance, in turn, accounts for the practical reality that EU goals are realized through layered interactions among supranational rules, national regulators, regional authorities, and local actors, which makes implementation contingent on administrative capacity and political acceptance. For the V4, the table 2 suggests that convergence is strongest where EU rules align with strategic national interests, such as decarbonization supported by nuclear or grid modernization, and weakest where integration implies perceived losses of control or asymmetric costs. As a result, a synthetic framework that combines these approaches is most suitable for analyzing V4 energy integration across time, policy domains, and crisis contexts.

3. Models of transformation in CEE countries: Poland's offshore wind scale-up, grid integration, and industrial decarbonization instruments. Models of transformation in CEE countries. Offshore wind energy in the Baltic Sea. The Baltic Power project is the flagship of offshore energy. It is a joint project between PKN ORLEN (Poland) and Northland Power (Canada) with a capacity of up to 1.2 GW, which will become Poland's first offshore wind farm (Chancellery of the Prime Minister, 2025; Baltic Power, 2025). After launch in 2026, Baltic Power will generate 4 TWh of electricity annually, covering 3% of Poland's electricity needs and providing for over 1.5 million households (Chancellery of the Prime Minister, 2025). Technical specifications. 76 Vestas V236-15.0 MW turbines with blades 115 meters long and a total height of over 260 meters (Chancellery of the Prime Minister, 2025; OffshoreWIND.biz, 2025; Vestas, 2022). Located 23 km from the Polish coast at the level of Choczewo and Leba, with an area of approximately 130 square kilometers (Chancellery of the Prime Minister, 2025). The project will help reduce CO2 emissions by approximately 2.8 million tons per year (Chancellery of the Prime Minister, 2025).

Large-scale ambitions for offshore wind. Poland is developing 19 offshore wind projects with a total capacity of 12 GW (BalticWind.eu, 2025; Reuters, 2024). The Polish Wind Energy Association estimates Poland's total offshore wind potential at 33 GW, which will make Poland a leader in offshore wind energy in the Baltic Sea (Polish Wind Energy Association, 2022; Reuters, 2025). Baltica 2 with a capacity of 1.5 GW supported by the EIB in the amount of €400 million (European Investment Bank, 2025a). Baltica 3 (1,050 MW, planned launch 2030), MFW Baltica II and III (720-1,200 MW each, 2027) (Ørsted, 2025; PGE Baltica, 2025). Modernization of coal energy with CCS. Poland is the largest producer of hard coal in the EU and the second largest in Europe after Russia, making coal a strategically important asset (European Commission, 2023). According to the analysis, in the 2030s, most coal-fired power plants will be decommissioned, and part of the gas generating capacities will be equipped with carbon capture technologies, with 4 GW equipped with CCS technologies (Clean Air Task Force, 2024).

Regulatory changes. In October 2023, Poland adopted regulatory acts that simplify the regulation of previously inactive CCUS (carbon capture, utilization, and storage) technologies (CMS, 2024; Szurlej et al., 2024). Prior to this, carbon capture and storage was only allowed as a demonstration project, which made it impossible to use the installation on an industrial scale (CMS, 2024; Szurlej et al., 2024). Technical implementation of CCS. Analysis of the efficiency of CCS technology for a 600 MW power plant showed positive modeling results (NPV amounted to 147 million euros) (Kępińska et al., 2024). The strategy envisages the implementation of gas power plants equipped with carbon capture capabilities to provide dispatchable capacities to complement weather-dependent wind energy (Clean Air Task Force, 2024).

Synchronization with ENTSO-E. LitPol Link is an electrical connection between Poland and Lithuania with a capacity of 500 MW, which has been operating in synchronous mode since 2025, connecting the Baltic energy systems to the Continental European Synchronous Area (ENTSO-E, 2025; Ministry of Energy of the Republic of Lithuania, n.d.; Wikipedia contributors, 2025a). The modernized LitPol Link near Alytus is now capable of operating in synchronous mode with the Continental European Synchronous Area (Ministry of Energy of the Republic of Lithuania, n.d.; Wikipedia contributors, 2025a). Technical details. It consists of a 53-kilometer double 330 kV line from Kruonis to Alytus, a 1000 MW back-to-back station in Alytus, and a 106-kilometer 400 kV line to the Lithuania-Poland border (Ministry of Energy of the Republic of Lithuania, n.d.; Wikipedia contributors, 2025a). The investment cost was €580 million: Lithuania paid €150 million, Poland €430 million, with EU funding of €213 million for Poland and €35 million for Lithuania (Litgrid, 2015).

SwePol Link, connection with Sweden, is a 254-kilometer monopolar underwater HVDC cable between the Stärnö peninsula near Karlshamn

(Sweden) and Bruskowo Wielkie near Słupsk (Poland), which can transmit up to 600 MW at a voltage of 450 kV. The line was opened in 2000 (Wikipedia contributors, 2025b). Utilization efficiency. In 2020, SwePol had an available technical capacity of 87%, of which 3.8 TWh (72% of technical capacity) was transmitted from Sweden to Poland (ENTSO-E, 2021). Since July 2017, LitPol Link has been used for energy trading between Lithuania and Sweden through the creation of a virtual trading zone, allowing energy to be transmitted to Sweden via Poland (BiznesAlert, 2017).

Table 3.18 consolidates the key energy projects that operationalize Poland's transition model by linking large scale renewable deployment, system flexibility solutions, and cross border infrastructure integration within a single investment portfolio.

Table 3.18. Key Energy Projects in Poland

Project Type	Project Name	Capacity	Launch Date	Technical Characteristics	Financing/Partners
Offshore wind energy	Baltic Power	1.2 GW	2026	76 Vestas V236-15.0 MW turbines. 115m blades, 260m height. 23 km from the coast. 130 km² area.	PKN ORLEN (Poland) + Northland Power (Canada)
(Offshore wind - Total potential)	19 projects	12-33 GW potential	By 2030	Leadership in the Baltic Sea.	Various investors
CCS technologies	Gas power plants with CCS	4 GW	2030s	CO_2 capture. Dispatchable capacity.	Public and private
Electrical interconnections	LitPol Link	500 MW	2025 (synchronization)	NPV €147 million (for 600 MW). 53 km 330 kV line. 1000 MW station in Alytus. 106 km 400 kV line.	€580 million (CC €248 million)
(Electrical interconnections)	SwePol Link	600 MW	2000 (operational)	254 km submarine HVDC cable, 450 kV voltage. 87% availability (2020).	Poland-Sweden

Source: (Baltic Power Offshore Wind Farm, 2026)

Table 3.18 synthesizes Poland's energy transition as a coordinated portfolio in which offshore wind operates as the flagship decarbonization

https://doi.org/10.36690/PUBADM

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

pathway, while interconnections and CCS ready dispatchable generation support adequacy, balancing, and system resilience under variable renewables. By comparing capacity, timing, technical characteristics, and project partners, the table clarifies the sequencing logic that requires grid and market integration to progress in parallel with new generation assets. It also demonstrates the multi actor nature of implementation, combining state enabled frameworks with corporate partnerships and cross border coordination. Overall, the table shows that Poland's transition depends on coherent alignment of permitting, financing, and grid readiness across complementary project types rather than on any single technology solution.

CBAM challenge for industry. The Carbon Border Adjustment Mechanism (CBAM) is an EU tool to set a fair price on carbon emitted during the production of carbon-intensive goods imported into the EU (European Commission, 2023; European Commission, n.d.-a). CBAM will apply in full mode from 2026, with a transitional period from 2023-2025 (European Commission, 2023; European Commission, 2023/956). Goods under regulation. The CBAM Regulation covers imports of cement, iron and steel, aluminum, fertilizers, electricity, and hydrogen for emissions of carbon dioxide, nitrous oxide, and perfluorocarbons (European Commission, 2023; European Commission, 2023/956). By 2030, the scope of CBAM is expected to expand to all product groups covered by the EU ETS (European Commission, 2023/956). Impact on Polish industry. The application of this regulation will significantly affect the profitability of business operations and investment decisions of companies subject to it (European Commission, 2023; Reuters, 2025). Companies that consume products within the scope of the EU ETS (e.g., manufacturing) may face significant additional costs from existing suppliers if CBAM is implemented (European Commission, 2023).

Transitional period and fines. Transitional phase: fines up to €50 per ton of CO2 (European Commission, 2023; German Emissions Trading Authority, 2025). During the transitional period, importers of goods subject to CBAM will have to report quarterly on embedded greenhouse gas emissions in their imports, without surrendering CBAM certificates (European Commission, 2023; European Commission, 2023/956). Economic prospects. Poland faces an investment deficit in the energy transition, with the Ministry of Climate and Environment estimating costs at 800 billion zlotys by 2030 (KUKE, 2024; Strategic Energy Europe, 2025). Over the lifetime of Baltic Power, Polish companies and contractors will account for approximately 20% of total investments (WindEurope, 2025).

Table 3.19 outlines the key regulatory changes and economic instruments that structure Poland's energy transition, linking each mechanism to its scope, timeline, and measurable impacts on investment, industry, and the energy balance.

Table 3.19. Regulatory changes and economic impact of the energy transformation

Regulation Area	Mechanism Name	Term of Action	Scope	Economic Impact	Impact on Poland	Regulation Area
CCUS Technologies	Simplification of regulation	October 2023	Industrial use of CO2	Transition from demonstration to industrial projects	Possibility of scaling up CCS	CCUS Technologies
Carbon Border Adjustment Mechanism (CBAM)	CBAM (transitional period)	2023-2025	Cement. Iron and steel. Aluminum. Fertilizers. Electricity. Hydrogen	Fines up to €50/ton of CO2	Quarterly reporting without certificates	Carbon Border Adjustment Mechanism (CBAM)
Investment Needs	Energy transition	By 2030	Entire energy system	800 billion zlotys	Investment deficit	Investment Needs
Localization of production	Baltic Power	Project life cycle	Offshore wind energy	20% of total investment	Development of Polish companies and contractors	Localization of production
Energy Balance	Baltic Power (impact)	From 2026	National energy system	4 TWh/year. 3% of Poland's needs. 1.5 million households	CO2 reduction by 2.8 million tons/year	Energy Balance
Coal Industry	Phased closure	2030s	Most coal-fired power plants	Need to replace generation	The largest coal producer in the EU	Coal Industry

Source: (BalticWind.eu, 2025)

Overall, the table shows that Poland’s transition is shaped by enabling regulation for CCUS, compliance pressures from CBAM, and large financing needs, while flagship projects like Baltic Power combine emissions reduction with industrial localization effects.

4. Formation of Slovakia's National Energy Strategy. Slovakia’s national energy strategy is characterized by a deliberate prioritization of nuclear power combined with a gradual, policy managed expansion of renewable energy sources (Government of the Slovak Republic, 2019; International Energy Agency [IEA], 2025). This approach is formalized through the National Energy and Climate Plan (NECP), adopted by the Slovak government in December 2019 and submitted to the European Commission in the same period, which sets the 2030 trajectory while aligning with the EU's longer-term climate neutrality objective for 2050 (Government of the Slovak Republic, 2019; European Commission, 2019; IEA, 2025). Within this framework, the state positions electricity-sector decarbonization as a cornerstone of national competitiveness, industrial stability, and social affordability, rather than as a narrow environmental target (IEA, 2025).

The policy logic also reflects Slovakia's structural conditions: a small open economy with limited domestic fossil resources, an inherited nuclear base, and a grid that benefits from stable baseload generation (IEA, 2025; International Atomic Energy Agency [IAEA], 2024). In practice, this produces a dual mandate for public authorities: maintain high system reliability through nuclear assets while creating regulatory and investment conditions that allow renewables to scale without undermining security of supply (Government of the Slovak Republic, 2019; IEA, 2025). The result is not a simple "nuclear versus renewables" choice, but a sequencing strategy in which nuclear anchors the transition and renewables are expanded where they are economically and administratively feasible (IEA, 2025). This sequencing has become more salient since 2022, as security considerations reshaped European energy priorities and increased the value of predictable domestic generation (European Commission, 2022; IEA, 2025).

A distinctive feature of Slovakia's energy mix is the exceptionally large role of nuclear power in electricity generation, commonly reported as above 60% in recent assessments, which places the country among the most nuclear-reliant systems in the European Union (IAEA, 2024; IEA, 2025). Slovakia operates five reactors across two sites, Bohunice and Mochovce, and the national strategy treats these assets as the primary instrument for decarbonization and long-term price stability (IAEA, 2024; IEA, 2025). The commissioning of Mochovce Unit 3, a 471/472 MW unit that entered commercial operation in 2023 after a prolonged, stop-and-go construction history, is central to this trajectory because it expands low-carbon output without depending on weather-sensitive resources (World Nuclear News, 2023; IAEA, 2024). In parallel, Mochovce Unit 4 is in late-stage completion, with regulatory and operator reporting pointing to commissioning during 2025, which would further strengthen the system's export capability and reserve margins (Slovenské elektrárne, 2025; World Nuclear News, 2025). Policy documents and independent analyses link these additions to a strategic objective: restoring and consolidating Slovakia's role as a net exporter of electricity, a status that was weakened after older nuclear units were shut down under EU accession-related commitments (IEA, 2025; OECD, 2024). In this sense, nuclear development is not only a climate instrument but also an industrial policy tool designed to support electrification, attract investment, and reduce exposure to volatile fuel markets (IEA, 2025).

Beyond completing existing units, the state has signaled intent to expand large-scale nuclear capacity at Bohunice, including a new unit around 1.2 GW that would represent one of the largest infrastructure investments in Slovakia’s modern history (Reuters, 2024). Reuters reporting indicates that the government has considered and advanced preparations for such a project, while explicitly excluding Russia’s Rosatom from procurement, which illustrates how geopolitical constraints shape technology choices even in a nuclear-centered system (Reuters, 2024). The institutional and ownership model under discussion emphasizes state control and strategic partnership selection, with references to potential cooperation with suppliers from the United States, France, and South Korea (Reuters, 2024). This governance design matters because nuclear expansion requires long planning horizons, credible financing structures, and stable regulatory commitments across electoral cycles (IAEA, 2024; OECD, 2024). It also reflects a broader regional pattern in Central and Eastern Europe, where nuclear build programs are increasingly framed as sovereignty-enhancing investments under the combined pressure of decarbonization and security imperatives (OECD, 2024; Reuters, 2024).

In parallel, Slovakia has pursued an innovation track through small modular reactors (SMRs), treating them as a potential bridge between decarbonization goals and the socio-economic challenge of coal region transformation (U.S. Department of State, 2023; Duke University, 2024). In 2024, Project Phoenix-related feasibility work involved preliminary site visits and assessments that included both nuclear locations and former coal-related sites, consistent with the program’s coal-to-SMR conversion logic (U.S. Department of State, 2023). Slovakia also received a USD 5 million grant under the US NEXT initiative to support site selection and preparatory work for SMR deployment, indicating an effort to translate feasibility assessments into an investable pipeline of projects (Duke University, 2024). The strategic rationale is twofold: SMRs could provide dispatchable low-carbon power with smaller unit sizes suitable for industrial nodes, and they could offer a structured pathway for replacing coal-based capacity while preserving local employment and grid stability (U.S. Department of State, 2023; Duke University, 2024). At the same time, the SMR track remains contingent on licensing timelines, supply chain readiness, and cost competitiveness relative to alternative flexibility options such as storage, demand response, and enhanced interconnection (IAEA, 2024). For that reason, Slovakia's SMR policy is best interpreted as a hedging instrument within a broader nuclear portfolio rather than as a near-term substitute for large units (Duke University, 2024; IEA, 2025).

Renewable energy policy in Slovakia is designed as a complementary pillar with moderate targets that reflect both administrative constraints and the inherited strength of low-carbon nuclear and hydro generation (Government of the Slovak Republic, 2019; IEA, 2025). The NECP framework sets a renewable share target for 2030 and outlines a diversified portfolio, typically emphasizing hydropower and solar photovoltaics while maintaining roles for biomass and biogas, and assigning a comparatively limited role to wind due to social, permitting, and geographic factors (Government of the Slovak Republic, 2019; Blue Europe, 2024). Empirical overviews note that wind capacity has remained very small, with only a few installations and limited change over long periods, whereas solar has expanded more dynamically in recent years (Blue Europe, 2024; IEA, 2025). Biomass and biogas remain significant in the renewable mix, which aligns with the country's forestry and agricultural structure, but raises governance questions about sustainability criteria, competing land uses, and the long-term availability of feedstock under stricter EU climate accounting (Blue Europe, 2024; European Commission, 2023). Geothermal resources are repeatedly identified as underutilized relative to technical potential, largely because network expansion and heat infrastructure investment are needed to convert subsurface heat into scalable decarbonization outcomes for buildings and district heating (Blue Europe, 2024). Consequently, renewable policy is less about headline shares and more about targeted modernization: grid reinforcement, streamlined permitting, and deployment in sectors where renewables reduce gas dependence most effectively, especially heating and distributed generation (IEA, 2025; European Commission, 2023).

Energy security considerations introduce the most complex tensions in Slovakia's strategy, because the country's gas and oil supply chains have remained more Russia-linked than those of many EU peers (IEA, 2025; Reuters, 2024). Slovakia's main gas supplier SPP has a long-term contract with Gazprom valid until 2034, and reporting after the end of transit through Ukraine highlights a continued reliance on Russian-origin gas delivered through alternative routes, including flows associated with TurkStream and regional intermediation (SPP, 2023; Reuters, 2024). Comparative assessments show that Hungary and Slovakia reduced Russian pipeline gas imports far less than the EU average after 2022, with dependence indicators

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

increasing by 2024 even as the rest of the EU reduced imports substantially (European Commission, 2024; Eurostat, 2024). This security dilemma is not purely technical: it is explicitly politicized in national discourse (Euronews, 2025; Deutsche Welle, 2024). Prime Minister Robert Fico has criticized EU proposals to end Russian gas imports by 2027, describing the approach in stark economic terms and insisting on guarantees that Slovakia will not be disadvantaged by rapid restrictions (Euronews, 2025). The transit dimension intensifies these issues because Slovakia historically benefitted from its position as a corridor for east-west gas flows, yet volumes have fallen sharply since 2022 and the end of transit through Ukraine from 1 January 2025 forced a reconfiguration of import logistics and bargaining leverage (European Commission, 2025; Reuters, 2024). These developments increase the strategic value of domestic low-carbon electricity and, simultaneously, raise the economic premium on diversification options in gas, including new contractual routes and regional solidarity mechanisms (European Commission, 2025; IEA, 2025).

A critical, often underappreciated security layer concerns the nuclear fuel cycle and maintenance dependence (IAEA, 2024; IEA, 2025). Slovakia's reactors are of the VVER-440 type, historically supplied by Russia's TVEL, and multiple analyses underline that the fuel and parts ecosystem constitutes a vulnerability even when electricity generation itself is domestic and low carbon (IAEA, 2024; OECD, 2024). Since 2023, Slovakia has taken concrete steps toward diversification through fuel-related agreements with Westinghouse and later with Framatome, aimed at licensing and supplying alternative fuel assemblies for VVER-440 reactors, with deliveries expected to begin after regulatory approvals and transition periods (Westinghouse, 2023; Framatome, 2024; OECD, 2024). This diversification trajectory is strategically important because it reduces single-supplier risk and aligns Slovakia with broader EU efforts to develop non-Russian nuclear fuel supply chains (European Commission, 2024; OECD, 2024). However, the transition is technically and institutionally demanding: it requires compatibility testing, licensing, and supply assurance over decades, which means that risk reduction is gradual rather than immediate (IAEA, 2024). In this context, nuclear expansion and nuclear fuel diversification are tightly coupled components of the same state strategy, because new build decisions are difficult to separate from long-term fuel sovereignty and geopolitical resilience (OECD, 2024; Reuters, 2024).

From an economic and infrastructure perspective, Slovakia's strategy relies on life-extension and modernization decisions to bridge the period between current assets and future capacity additions (IEA, 2025; OECD, 2024). Long-lived nuclear assets require systematic upgrades and regulatory oversight to ensure safety, reliability, and performance, and national planning documents and sector assessments repeatedly emphasize the role of maintenance, refurbishment, and grid readiness in preserving system stability during transition (Government of the Slovak Republic, 2019; IEA, 2025). At the same time, the strategy must manage the integration of distributed generation and the electrification of demand, which increases the importance of networks, flexibility resources, and cross-border cooperation (European Commission, 2020; IEA, 2025). This is particularly relevant in a system where low-carbon generation is already high, since the marginal decarbonization gains increasingly depend on replacing fossil fuels in heating, transport, and industry rather than only changing the electricity mix (European Commission, 2020; IEA, 2025). The policy implication is that Slovakia's state-led strategy must coordinate investments across generation, grids, and end-use sectors, while maintaining affordability and limiting distributional impacts that could undermine public support (OECD, 2024).

Overall, the formation of Slovakia's national energy strategy illustrates the complex trade-offs faced by a small EU member state seeking to reconcile climate commitments with security vulnerabilities and economic constraints (IEA, 2025; OECD, 2024). The nuclear-centered model provides Slovakia with a strong platform for electricity-sector decarbonization and potential export capacity, while SMR initiatives and renewable expansion serve as complementary pathways to broaden flexibility and regional resilience (IAEA, 2024; Duke University, 2024; Government of the Slovak Republic, 2019). Yet the persistence of Russian-linked gas and oil exposure, combined with fuel-cycle dependence in the nuclear sector, creates strategic risks that require sustained diversification policies and credible international partnerships (European Commission, 2025; OECD, 2024; Reuters, 2024). The success of the strategy will therefore depend less on a single technology choice and more on the state's capacity to execute a coordinated portfolio: completing and financing nuclear projects, accelerating viable renewables, modernizing infrastructure, and reducing external dependence through both market instruments and diplomatic leverage (IEA, 2025; OECD, 2024). In that sense, Slovakia's case demonstrates that energy transition governance in Central and Eastern Europe is inseparable from security governance, and that national strategies must be evaluated as integrated systems rather than as isolated sectoral plans (European Commission, 2020; OECD, 2024; IEA, 2025).

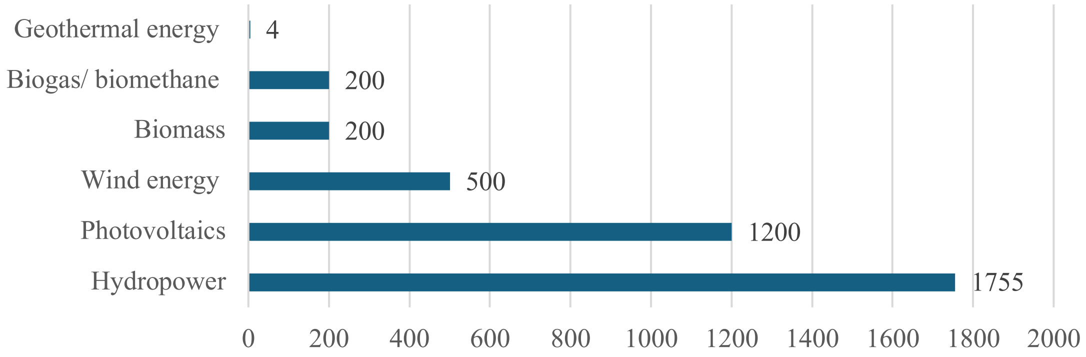

Figure 3.3. Target installed capacities of renewable energy sources in Slovakia by 2030 (MW)

Source: (Tuzhanskyi, 2022)

Table 3.20 summarizes the structure of Slovakia's energy sector by comparing current capacities with planned targets and deadlines across nuclear, renewable, and traditional generation. It highlights the strategic dominance of nuclear power and the complementary, slower scaling of renewables within the 2030 planning horizon.

Table 3.20. Structure of Slovakia's energy sector

Sector	Object/Technology	Current Capacity	Planned Capacity/Goals	Implementation Deadline	Development Status
Nuclear Energy	Total nuclear capacity	2,308 MW net	>3.5 GW	By 2031-2035	>60% of energy balance
Renewable Sources	Hydropower	Existing base	1,755 MW	2030	14.4% of generation (2019)
	Photovoltaics	840 MW (2023)	1,200 MW	2030	Successful development
	Wind Energy	3 MW	500 MW	2030	Regulatory challenges
	Biomass	Potential 11,200 GWh/year	200 MW	2030	Dominates in RES
	Biogas/biomethane	Developing	200 MW	2030	Promising sector
	Geothermal energy	280 MW (thermal), 145 GWh/year	4 MW + expansion	By 2030	2.6% of potential
	Total RES goal	8.9% (2019)	19.2%	2030	Below EU average (32%)
Traditional Energy	Thermal power plants	21% of generation (2019)	Gradual reduction	By 2030-2050	Baseload generation
Total Capacity	All sources	7,728 MW (2019)	Increase to >10 GW	2030-2035	Infrastructure modernization

Source: (International Energy Agency, 2024)

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

Overall, the table 3.20 shows that Slovakia's transition model is built on expanding and maintaining nuclear capacity while raising renewables toward the 2030 target, with the main constraints concentrated in wind permitting, geothermal scaling, and system-wide infrastructure modernization.

5. Hungary - pragmatic energy policy. Hungary represents one of the clearest cases of pragmatic energy policymaking in Central and Eastern Europe, combining compliance with EU climate objectives with a strong preference for policy instruments that protect affordability and supply security. Hungary's strategic framework is anchored in the National Energy Strategy 2030, with an outlook to 2040, which articulates a "clean, smart and affordable" vision and is operationalized through measures in the National Energy and Climate Plan and related long term strategies (OECD, 2023; European Commission, 2023). In parallel, Hungary has codified a climate neutrality objective for 2050 and has framed decarbonization primarily through electrification, nuclear baseload continuity, targeted renewable deployment, and energy efficiency improvements (IEA, 2022a; IEA, 2022b). This approach aligns with EU level decarbonization goals while preserving a national preference for controllable capacity and centralized planning in system critical segments, particularly nuclear power and gas infrastructure (European Commission, 2023; IEA, 2022a).

Table 3.21 summarizes the core targets and quantitative indicators embedded in Hungary's National Energy Strategy, linking the 2030 pathway to the 2050 climate neutrality horizon through renewables, emissions reduction, efficiency, nuclear share, and energy dependency.

Table 3.21. Main goals and indicators of Hungary's National Energy Strategy until 2030

Indicator	Base year (2020)	2030 Target	2050 Target
Share of renewable energy sources (%)	12.6%	21%	85%
Reduction of CO_2 emissions (% from 1990 level)	-32%	-40%	-85%
Energy efficiency (consumption reduction)	-	23%	50%
Share of nuclear energy (%)	48%	52%	55%
Energy dependency (%)	58%	45%	20%

Source: (Enerdata, 2024; International Energy Agency, 2022)

Overall, the table 3.21 shows a strategy that combines rising renewables and efficiency gains with a sustained nuclear backbone, while explicitly treating lower energy dependency as a central performance indicator of long-term energy security.

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

The result is a policy model in which climate ambition is mediated by energy security calculations and by a political economy that prioritizes stable consumer prices and predictable industrial energy inputs (IEA, 2022a).

A defining feature of Hungary's pragmatism is the persistence of Russian-linked supply chains in fossil fuels and nuclear fuel, even after the strategic shock of Russia's full-scale invasion of Ukraine. The International Energy Agency identifies Hungary's high reliance on Russia for gas, oil, and nuclear fuel as a near-term vulnerability and recommends accelerated diversification and demand-side measures to reduce exposure (IEA, 2022a; IEA, 2022b). The government's response has often emphasized continuity of supply and domestic stabilization rather than rapid disengagement from Russian sources, which differentiates Hungary from many EU peers that pursued more abrupt import restructuring after 2022 (European Commission, 2023; Reuters, 2025-12-10). This posture became explicit in July 2022, when Hungary declared an energy emergency and announced steps focused on strengthening domestic output and securing additional supply, including higher domestic gas production, expanded coal extraction, and measures related to the Mátra lignite complex, rather than a policy pivot away from Russian imports (Euronews, 2022). The logic of this response is consistent with a security-first framing, where diversification is pursued selectively and incrementally, and where the government maintains maximum discretion over the speed and sequencing of structural change (IEA, 2022a).

Nuclear energy constitutes the backbone of Hungary's strategy and the main instrument through which the country reconciles decarbonization with reliability. The Paks Nuclear Power Plant provides around 2,000 MW of capacity and is central to Hungary's electricity system, with lifetime extension policies designed to preserve firm low-carbon generation through the 2030s (World Nuclear Association, n.d.; Reuters, 2024-07-27). Hungary's expansion strategy is institutionalized in the Paks II project, which adds two 1.2 GW units awarded to Russia's Rosatom in 2014 and supported by a Russian state loan covering the majority of the project's estimated EUR 12.5 billion cost (Reuters, 2024-05-29; Reuters, 2024-11-20). Regulatory milestones have advanced in recent years, including the Hungarian Atomic Energy Authority's issuance of a construction license in August 2022, which is a foundational legal step for project implementation (Hungarian Atomic Energy Authority, 2022). Subsequent reporting indicates continued progress in the licensing and safety documentation pathway, alongside recurring delays and contract adjustments reflecting cost pressures and the broader sanctions environment (Reuters, 2024-11-20; NucNet, 2024-12-05). In late 2025, the United States issued a general license clarifying that

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

certain transactions related to the Russian-backed project could proceed under specified conditions, underscoring how geopolitical constraints increasingly shape project finance and supply-chain risk management in nuclear megaprojects (Reuters, 2025-11-21).

Renewable energy policy in Hungary is best characterized as selective acceleration, with strong performance in solar photovoltaics but prolonged stagnation in wind. Table 3.22 presents the historical structure of Hungary's electricity production and the planned 2030 mix, allowing comparison of how nuclear, gas, coal, and renewables are expected to evolve under the current transition model.

Table 3.22. Structure of electricity production in Hungary

Energy Source	2015	2020	2023	Planned for 2030
Nuclear energy (%)	52.7	47.8	46.2	52.0
Natural gas (%)	19.4	20.1	21.5	15.0
Coal (%)	21.1	14.2	12.8	5.0
Solar energy (%)	1.2	7.8	12.5	18.0
Wind energy (%)	0.6	2.1	2.8	6.0
Hydropower (%)	2.1	2.2	2.1	2.0
Biomass (%)	2.9	5.8	2.1	2.0

Source: (Enerdata, 2024)

Overall, the table indicates that Hungary's planned transition relies on maintaining or increasing nuclear share, reducing coal, moderating gas, and scaling solar more strongly than wind, which is consistent with the country's selective renewable deployment approach.

By 2021, renewables accounted for 19.2% of Hungary's electricity production, and solar became the leading renewable source, generating 3,793 GWh and reaching a 10.6% share of total electricity output, supported by rapid capacity additions (International Trade Administration, 2024). Official Hungarian energy briefings also document substantial solar expansion through 2022, reflecting an investment and permitting environment that has favored PV as the most scalable renewable option in the short term (Hungarian Energy and Public Utility Regulatory Authority, 2023). In contrast, wind power development has been constrained by restrictive siting rules introduced in 2016, including a de facto exclusion zone requiring turbines to be located far from populated areas, which has inhibited new projects and kept installed wind capacity largely unchanged for years (Euronews, 2016; Energiaklub, 2023). This asymmetry between PV growth and wind stagnation illustrates a pragmatic balancing of land-use politics, local acceptance, and perceived system controllability, even though the IEA

https://doi.org/10.36690/PUBADM

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

explicitly highlights Hungary's underused wind and geothermal potential as an important diversification and decarbonization opportunity (IEA, 2022b; IEA, 2022a). Accordingly, Hungary's renewable pathway is not a uniform expansion across technologies but a pattern of concentrated support where deployment is politically feasible and economically predictable (International Trade Administration, 2024).

Energy security in Hungary remains strongly connected to oil and gas import architecture, with policy choices shaped by the country's landlocked geography and legacy infrastructure. EU sanctions adopted in 2022 imposed major restrictions on Russian oil imports while providing derogations for certain landlocked member states supplied via pipeline routes, which preserved short-term continuity for countries including Hungary (Reuters, 2022-05-31). This framework reduced immediate disruption risks but also created structural incentives to delay deeper refinery adaptation and supply diversification, since pipeline flows could continue under exemptions while alternatives required capital-intensive upgrades and new contractual arrangements (European Commission, 2023; Reuters, 2022-05-31). On the gas side, Hungary has continued substantial Russian imports, including volumes routed via TurkStream, while simultaneously pursuing limited diversification through LNG-linked options in the wider region (Reuters, 2025-12-08). The Krk LNG terminal in Croatia represents one of the most relevant non-Russian access points for Central Europe, with initial capacity designed at 2.6 bcm per year and subsequent steps to raise effective regasification capacity, enabling additional flexibility for regional traders and utilities (European Commission, 2021; MET Group, 2021). While such infrastructure broadens the menu of supply options, the overall balance of Hungary's gas system has remained heavily influenced by Russian-origin volumes, which the IEA identifies as a critical exposure that should be reduced through both supply diversification and structural demand reduction (IEA, 2022a).

The political economy of energy transformation in Hungary is closely tied to the strategic role of national champions and the state's preference for controllable transition pathways. MOL Group, with meaningful state participation, remains a key actor in implementing diversification and investment priorities, including in solar where the company has publicly reported acquisitions and portfolio expansion consistent with its renewable strategy (MOL Group, 2024). This corporate-state linkage supports a transition model in which large incumbents mediate the pace of change through asset conversion, targeted renewable investments, and refinery and infrastructure adaptation, rather than through rapid disruption of the existing fossil value chain (IEA, 2022a). At the same time, Hungary's approach has generated tensions within the EU when national energy choices intersect with collective policy objectives, particularly on Russia-related measures. A clear example is the 2023 Bulgarian transit levy on Russian gas, which prompted diplomatic conflict involving Hungary and drew scrutiny from EU institutions, illustrating how transit, taxation, and sanction coordination can become politically salient instruments of energy governance (AP News, 2023-10-20; Radio Free Europe/Radio Liberty, 2023-10-18). In this environment, Hungary has repeatedly framed affordable supply as a sovereignty issue, reinforcing the broader pattern of pragmatic resistance to policy changes perceived as increasing domestic costs or reducing national control (IEA, 2022a; European Commission, 2023).

Coal policy completes the picture of gradualism and sequencing in Hungary's transition. While Hungary has communicated coal phase-out intentions in different timeframes across policy cycles, external tracking and policy documents indicate that timelines have been revised in response to replacement capacity uncertainty, particularly around the future configuration of the Mátra complex and associated gas and grid investments (IEA, 2022c; Beyond Fossil Fuels, 2024). This illustrates a consistent principle in Hungary's strategy: coal exit is pursued insofar as stable replacement capacity, often gas or nuclear-linked system stability measures, can be credibly secured without jeopardizing affordability and security of supply (IEA, 2022a). Overall, Hungary's pragmatic energy strategy is best understood as a managed transition that privileges firm low-carbon generation (nuclear), accelerates renewables where deployment is least politically costly (solar), and maintains supply relationships that minimize near-term price and security risks, even when these relationships generate political controversy within the EU (IEA, 2022a; International Trade Administration, 2024). The medium-term success of this model will depend on whether Hungary can reduce Russia-linked vulnerabilities in gas, oil, and nuclear fuel, while meeting tightening EU decarbonization and security requirements that are increasingly oriented toward a full phase-out of Russian gas imports by 2027 (IEA, 2022a; Reuters, 2025-12-10).

6. Czech Republic. National Energy and Climate Plan (NECP). On December 18, 2024, the Czech government approved an updated National Energy and Climate Plan (NECP), which defines the trajectory of the energy sector to 2030 with a strategic outlook to 2050 and explicitly links decarbonization to energy security and affordability (Ministry of Industry and Trade of the Czech Republic, 2024). The updated plan formalizes a long-term structural shift away from coal and towards a dual pillar model based

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

on nuclear generation as a stable low-carbon backbone and renewables as the main source of incremental capacity growth (Ministry of Industry and Trade of the Czech Republic, 2024; World Nuclear News, 2025). In quantitative terms, the NECP anticipates nuclear power reaching around 44% of electricity generation by 2030 and increasing to approximately 68% by 2040 as new units come online (Ministry of Industry and Trade of the Czech Republic, 2024; World Nuclear News, 2025). In parallel, the plan expects the share of renewables in gross final energy consumption to exceed 30% by 2030 and foresees renewables' share in electricity generation rising from 16.5% in 2023 to 28% by 2030 (Ministry of Industry and Trade of the Czech Republic, 2024). This design reflects an attempt to reconcile three constraints that are especially salient in Czech conditions: high exposure to the coal legacy, the need for system reliability in an increasingly electrified economy, and the EU-level decarbonization timetable that makes postponement costly in regulatory and investment terms (World Nuclear News, 2025).

Table 3.22 summarizes the expected evolution of the Czech electricity mix by focusing on the planned increase in the nuclear share and linking it to the parallel expansion of renewables and the transitional stabilizing role of gas across the 2023–2050 horizon.

Table 3.22. Current and future energy balance of the Czech Republic regarding the share of nuclear energy in electricity production

Year	Share of nuclear energy in electricity production	Comments on projects and development	Total RES share and the role of gas
2023	about 40%	6 reactors are in operation at the Temelín and Dukovany NPPs	RES share is about 16.5%, gas serves as a transition fuel
2030	target of 44%	Launch of two new reactors at Dukovany (2400 MW) by 2030	RES will increase to 28%, gas ensures system stability
2040	ambitious goal — 68%	The introduction of new units and small modular reactors is planned	RES share will grow to 46%, gas will begin to decline
2050	planned increase from the current 33% to 50%	Extension of Temelín's operational life, expansion of small reactors	RES to 46% and more, gas will be gradually replaced

Source: (UNN.ua, 2024)

Overall, the table indicates a transition pathway in which nuclear expansion is treated as the main driver of firm low-carbon capacity, while renewables rise steadily and gas functions as a temporary balancing fuel that declines as new nuclear and flexibility resources are deployed.

Nuclear power is positioned as the core instrument for maintaining security of supply while accelerating emissions reductions. The Czech Republic operates two nuclear plants, Dukovany and Temelín, which together account for roughly 40% of domestic electricity generation in the early 2020s, making nuclear the single most important low-carbon source in the national mix (Ministry of Industry and Trade of the Czech Republic, 2024; World Nuclear News, 2025). A central modernization and expansion step is the Dukovany new-build program, for which the Czech government selected Korea Hydro & Nuclear Power (KHNP) as the preferred bidder in 2024, with the project framed as a multi-unit option that may later extend beyond the first two reactors (Associated Press, 2025). The updated plan describes nuclear expansion as a key enabling condition for coal exit and for stabilizing electricity prices under tighter EU carbon constraints, because firm low-carbon generation reduces the need to rely on fossil-based balancing during periods of low renewable output (World Nuclear News, 2025). Importantly, nuclear expansion is also treated as an industrial policy instrument, since the scale and duration of nuclear projects creates stable demand for domestic engineering, construction, and high-value supply chains when governance and procurement frameworks are aligned with national capabilities (Associated Press, 2025).

Coal phase-out is the second major axis of the updated NECP and is formulated as a fixed political commitment rather than an aspirational scenario. The Czech government has committed to ending coal use in the energy sector by 2033, replacing a previously later timetable and signaling a tighter national interpretation of decarbonization urgency (Ministry of Industry and Trade of the Czech Republic, 2024; NucNet, 2025). This is consequential because coal remained a large contributor to Czech electricity generation in the early 2020s, at about 43% in 2022, which implies that the transition requires not only new capacity but also grid reinforcement, flexible resources, and predictable permitting for renewables and replacement heat sources (Carbon Tracker, 2022). Analytical modeling indicates that an accelerated coal exit by 2030 is technically feasible under ambitious but realistic assumptions, primarily through rapid additions of onshore wind and solar that would reach around 4 GW and 10 GW respectively by 2030, provided that planning and connection constraints are actively managed (Ember, 2020). However, the feasibility of such an acceleration depends on political acceptance of faster infrastructure buildout and on balancing decarbonization with social and regional impacts in coal-dependent districts, which often become the binding constraint rather than pure technology availability (Ember, 2020).

Renewable energy development in Czech strategy is therefore shaped by both target setting and implementation bottlenecks, especially permitting, grid capacity, and local acceptance. Official targets require a substantial increase in installed solar and wind capacity by 2030, and national oversight reporting emphasizes that achieving the government-approved 2030 renewable share will require approximately 10.1 GWp of photovoltaic capacity and about 1.5 GW of wind capacity connected to the grid (Supreme Audit Office of the Czech Republic, 2025). The policy emphasis on distributed solar reflects the relative ease of deployment compared to large wind projects, but it also increases the need for network modernization and flexibility solutions to maintain stability during peak generation hours (Supreme Audit Office of the Czech Republic, 2025). In this context, biogas and biomethane projects are increasingly framed as both circular-economy infrastructure and a security asset, because they convert municipal and agricultural waste streams into dispatchable energy and heat. Illustrative initiatives include wastewater-based biogas projects designed to process thousands of tons of biodegradable waste annually and supply heat and electricity locally, strengthening resilience while reducing methane emissions from unmanaged waste (World Bio Market Insights, 2024).

Energy security considerations after 2022 reinforced the Czech preference for diversification and for reducing exposure to Russian supply disruptions, particularly in oil. The Czech government announced that the country became fully independent from Russian oil supplies, enabled by increased capacity and use of the TAL and IKL pipeline routes from the west, which structurally reduces a long-standing vulnerability associated with the Druzhba pipeline (Government of the Czech Republic, 2025; Reuters, 2025). This shift is consistent with a broader state strategy of resilience through route diversification and regional market integration, where physical infrastructure decisions are treated as security policy instruments as much as economic assets (Government of the Czech Republic, 2025). For gas, diversification has included contracting and market-based sourcing via European hubs, alongside efforts by major actors to broaden supply options. For example, ČEZ reported extended cooperation with Algeria's Sonatrach, describing supplies that can cover roughly 2% of Czech annual gas consumption and that provide an additional route in case of shortages (ČEZ, 2025). Such measures do not eliminate gas-related risks, but they reduce dependence concentration and complement the longer-term NECP logic that assumes electrification and low-carbon generation will gradually reduce the strategic weight of gas in the system (Ministry of Industry and Trade of the Czech Republic, 2024).

Overall, the updated Czech NECP represents a coherent, state-led transition model that relies on nuclear expansion for firm low-carbon capacity, a fixed coal exit date as a governance commitment, and accelerated renewable deployment supported by grid and flexibility investments (Ministry of Industry and Trade of the Czech Republic, 2024; World Nuclear News, 2025). Its internal consistency is strongest where targets, timelines, and financing instruments are aligned, particularly in the nuclear roadmap and the formal coal phase-out objective (NucNet, 2025). Its primary implementation risks arise in the renewable deployment pipeline, where permitting and network constraints can translate formal targets into delayed delivery, increasing reliance on gas and imports during the transition decade (Supreme Audit Office of the Czech Republic, 2025; Ember, 2020). The Czech case therefore illustrates an energy transition pathway in which the state acts as a strategic coordinator of long-horizon infrastructure, combining security and climate rationales while continuously managing the trade-offs between speed, affordability, and political feasibility (Ministry of Industry and Trade of the Czech Republic, 2024).

Conclusion. The comparative evidence from Poland, the Czech Republic, Slovakia, and Hungary indicates that energy transformation in the Visegrád Group is structurally state-organized because governments must coordinate long-term planning, regulatory alignment, investment mobilization, and energy security management under EU climate targets and post-2022 supply shocks. The analysis confirms that national pathways remain uneven due to differences in initial energy mixes, domestic resource endowments, institutional capacity, and political preferences, which explains why common EU objectives generate divergent national implementation patterns. Across the four cases, nuclear energy functions as a key stabilizing pillar for electricity-sector decarbonization, while renewables expand at different speeds depending on permitting constraints, grid readiness, and affordability pressures affecting households and industry. Market integration and cross-border interconnections support resilience and can accelerate modernization, yet they do not eliminate national asymmetries or the distributional tensions that shape public acceptance of transition policies. A central governance implication is that credibility depends not only on adopting strategies but on building implementation capacity at scale, including network modernization, stable investment frameworks, and socially managed coal-exit policies that protect legitimacy in affected regions. Finally, geopolitical divergence inside the V4 weakens collective coherence and reduces the scope for unified regional leadership, even when technical cooperation in infrastructure remains economically rational.

Overall, the study supports the conclusion that V4 countries will increasingly rely on hybrid transition portfolios that combine nuclear expansion or life extension, accelerated solar and wind where feasible, and selective diversification contracts to manage residual fossil dependence during the transition period. The primary policy challenge is therefore not selecting a single "best" technology, but sustaining a coherent sequencing logic that aligns decarbonization, security, and affordability across multiple electoral cycles and investment horizons. This requires states to operate simultaneously as strategic planners, regulators, financiers, and mediators of distributional impacts, since the feasibility of the transition depends on how costs and benefits are allocated across territories and social groups. The analysis also implies a forward research agenda focused on the practical outcomes of just transition instruments in coal-dependent regions, the competitiveness effects of carbon-border measures for energy-intensive industries, and the conditions under which governance lessons from the V4 experience can be transferred to post-war reconstruction and integration processes in neighboring countries.

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

Conflict of interest. The author 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 author 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 author 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. AABE Economics. (2023). *Energy economy of Hungary and Austria in the face of energy challenges*. https://aab-economics.kmf.uz.ua/aabe/article/view/72
2. Atlantic Council. (2019). *Hungary's energy landscape: MOL Group's strategic role and renewable energy expansion*. https://www.atlanticcouncil.org/blogs/energysource/hungarys-energy-landscape-mol-groups-strategic-role/
3. Bache, I. (2012). *Multi-level governance in the European Union*. https://www.researchgate.net/publication/288802300_Multi-Level_Governance_in_the_European_Union
4. Blue Europe. (2024). *A brief outlook of renewable energy in Slovakia: Trend and potential*. https://www.blue-europe.eu/analysis-en/short-analysis/a-brief-outlook-of-renewable-energy-in-slovakia-trend-and-potential/

5. Borysova, O., & Rudnik, D. (2024). Theoretical foundations and models of European integration. *Scientific and Theoretical Almanac Grani, 27*(5), 105–112. https://doi.org/10.15421/172498
6. Carbon capture and storage (CCS). (2025). https://www.futurecoal.org/sustainable-coal/carbon-capture-and-storage/
7. Christin, S., & Stefanini, S. (2018, November 20). Hungary wants end to coal power by 2030. *Climate Home News*. https://www.climatechangenews.com/2018/11/20/hungary-wants-end-coal-power-2030
8. Country nuclear power profiles 2022 edition: Czech Republic. (2022). https://www-pub.iaea.org/MTCD/publications/PDF/cnpp2022/countryprofiles/CzechRepublic/CzechRepublic.htm
9. Czech Republic advances biogas production to enhance energy independence. (2024). *World Bio Market Insights*. https://worldbiomarketinsights.com/czech-republic-advances-biogas-production-to-enhance-energy-independence/
10. Czech Republic energy mix and decarbonisation pressures: Balancing between nuclear and renewables. (2025). *CzechTrade Offices*. https://www.czechtradeoffices.com/se/news/czech-government-updates-national-energy-plan-boosting-nuclear-and-renewables
11. Dunn, T. M. (2012, November 28). Neo-functionalism and the European Union. *E-International Relations*. https://www.e-ir.info/2012/11/28/neo-functionalism-and-the-european-union/
12. Electricity link LitPol Link. (2023). https://enmin.lrv.lt/en/strategic-projects/electricity-sector/electricity-link-litpol-link/
13. European Investment Bank. (2025). *Financing the modernization of the Czech energy infrastructure: Support to ČEZ*. https://www.eib.org
14. European Investment Bank (EIB) REPowerEU funding programs: 45 billion EUR allocation (2022–2024). (2024). https://bankwatch.org/eib
15. European Union Strategy for Energy System Integration. (2022). https://greentransform.org.ua/strategiya-yevropejskogo-soyuzu-z-integratsiyi-energetychnoyi-systemy/
16. Europeanization processes of the EU energy policy in Visegrad countries in the years 2005–2018. (2021). https://www.mdpi.com/1996-1073/14/7/1802
17. Global Energy Prize. (2024). *Hungary's Paks II NPP receives approval for pouring of first concrete*.
18. Hungary and Slovakia have alternatives to oil and gas from the Russian Federation, but they only increase their dependence, experts. (2025, May 15). https://www.slovoidilo.ua/2025/05/15/novyna/polityka/uhorshhyna-ta-slovachchyna-mayut-alternatyvy-nafti-hazu-rf-vony-lyshe-zbilshuyut-svoyu-zalezhnist-eksperty
19. Hungary and Slovakia resist EU's energy security plan. (2025, June 16). *Euronews*. https://www.euronews.com/my-europe/2025/06/16/hungary-and-slovakia-resist-eus-energy-security-plan
20. Hungary: Energy market overview: Nuclear and renewables. (2024). https://www.trade.gov/market-intelligence/hungary-energy-market-overview-nuclear-and-renewables

21. International Trade Administration. (2024). *Hungary: Energy*. https://www.trade.gov/country-commercial-guides/hungary-energy
22. Maksymak, H. (2018). Як далі будувати співпрацю України з Вишеградською групою? [How to further build Ukraine's cooperation with the Visegrad Group?]. *Perspektyva*. http://prismua.org/%D1%8F%D0%BA-%D0%B7-%D0%B2/
23. Stephen, G. (2004). Multi-level Governance and the European Union', in Ian Bache, and Matthew Flinders (eds), *Multi-level Governance*, https://doi.org/10.1093/0199259259.003.0007
24. Nuclear Expediting the Energy Transition (NEXT) One Stop Shop for Small Modular Reactor (SMR) Support Program. (2024). https://researchfunding.duke.edu/nuclear-expediting-energy-transition-next-one-stop-shop-small-modular-reactor-smr-support-program
25. Poland enacts regulations to accelerate development of carbon dioxide capture, utilisation and storage technology (CCUS). (2024). https://cms-lawnow.com/en/ealerts/2024/02/poland-enacts-regulations-to-accelerate-development-of-carbon-dioxide-capture-utilisation-and-storage-technology-ccus?utm_source=chatgpt.com
26. Renewable energy in Czech Republic. (2024). https://cms.law/en/int/expert-guides/cms-expert-guide-to-renewable-energy/czech-republic
27. Rosslowe, C. (2020). *Coal-free Czechia 2030*. https://ember-energy.org/latest-insights/coal-free-czechia-2030/
28. European Environment Agency. (2025). *Slovakia* (Europe environment 2025 country profile). https://www.eea.europa.eu/en/europe-environment-2025/countries/slovakia
29. Slovakia: Gas conflict with Ukraine as a delaying maneuver. (2025). *Deutsche Welle*. https://www.dw.com/uk/slovaccina-gazovij-konflikt-z-ukrainou-ak-okozamiluvalnij-manevr/a-71209938
30. Slovakia to end renewable subsidies by 2026. (2025). *Euractiv*. https://www.euractiv.com/section/eet/news/slovakia-to-end-renewable-subsidies-by-2026/
31. The Czech Republic announced the date for the complete abandonment of coal and the transition to nuclear energy. (2025). https://unn.ua/news/chekhiia-oholosyla-datu-povnoi-vidmovy-vid-vuhillia-ta-perekhid-na-atomnu-enerhetyku
32. Wolf Theiss. (2023). *Winds of change: Positive outlook for Hungary's wind energy regulations*. https://www.wolftheiss.com/insights/positive-outlook-for-hungarys-wind-energy-regulations/
33. World Nuclear News. (2025, June 5). KHNP sets out plans for USD18.6bn Czech nuclear project. https://www.world-nuclear-news.org/articles/khnp-sets-out-plans-for-usd186bn-czech-nuclear-project.

Conclusions

Based on the research results presented by the authors in this monograph, the following conclusions can be drawn:

1. Digitalization of public administration is most accurately interpreted as a shift from technology focused automation to governance centered transformation, where digital instruments reshape institutional design, integrated service delivery, and accountability. The section demonstrates that the evolution of digital government can be systematized through successive phases, culminating in value based and resilience oriented models, in which rights protection, inclusion, and institutional trust become explicit performance criteria. The analysis shows that sustainable scaling depends on interoperability, lawful data reuse, and trust infrastructure, because these mechanisms enable cross agency coordination and reduce repetitive administrative requests. The EU pathway is presented as a coordinated model of shared principles and monitoring commitments, while Ukraine's experience illustrates accelerated implementation via unified service ecosystems supported by interoperability infrastructure. A key conclusion is that implementation policy should prioritize co development of legal interoperability, institutional capacity, and data governance rather than equating progress with service digitization counts.

2. International experience becomes practically valuable when it is translated into evidence grounded lessons that link outcomes, mechanisms, and enabling conditions, rather than being reduced to the replication of visible artefacts such as portals or apps. The section concludes that policy transfer is most effective when it transfers governance routines, enforceable authority, and lifecycle capabilities, because these elements determine whether reforms function under real administrative constraints. Adaptation to national context is identified as the decisive stage, since institutional fit determines whether transferred mechanisms can operate lawfully, reliably, and inclusively at scale, and whether reforms avoid symbolic imitation and implementation fatigue. The analysis also highlights procurement as a governance lever that can lock in interoperability, portability, auditability, and accountability across the lifecycle of digital systems. Finally, the section supports an evaluation stance in which digital transformation is judged by completion, administrative burden reduction, equity, trust, and resilience, rather than by the number of digitized services.

3. The study concludes that AI in public administration should be treated as institutional and organizational change, because it transforms the design, delivery, and oversight of services and influences public trust and the

https://doi.org/10.36690/PUBADM

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

legitimacy of decisions. The results indicate that AI can increase efficiency through automation of routine processes, better targeting of services, and predictive analytics that enable more proactive policy design. At the same time, the analysis demonstrates that AI introduces distinct governance risks, including bias, opacity, data insecurity, and digital exclusion, which may undermine public value if left unaddressed. Therefore, AI driven modernization requires explicit governance conditions that secure accountability, transparency, lawful data management, and safeguards for inclusion. The section’s general conclusion is that effectiveness and legitimacy must be advanced together, so that efficiency gains do not come at the cost of rights, trust, or procedural fairness.

4. Risk based digital supervision is concluded to be an institutional capacity building trajectory, not a set of digital artefacts, because durable public value depends on lawful data use, interoperability, accountability, and inclusion. The results show a structural shift from inspection led compliance toward harm oriented supervision, where risk segmentation and analytics enabled triage improve timeliness and consistency but also create obligations related to explainability, auditability, model risk, and due process. Anti fraud governance is positioned as the operational core of the risk approach because it translates abstract risk into observable patterns, measurable indicators, and coordinated inter agency responses supported by reliable identifiers and lawful data reuse. The section further concludes that reform effectiveness depends on a coherent instrument mix combining prevention, compliance support, targeted detection, and proportionate enforcement, with performance management focused on outcomes rather than digitization activity. Administrative burden reduction is therefore treated not as a side effect, but as a design objective that must be balanced with legitimacy and fairness.

5. The study concludes that digitalization of accounting and reporting functions as a public governance tool that influences the quality of financial information and the resilience of the economy, especially under conditions of martial law and accelerated reforms. The analysis identifies a new digital architecture of accounting shaped by platforms and systems such as Diia, BAS ERP, electronic document management, fintech solutions, and Inline XBRL, which together improve timeliness, transparency, and accessibility of reporting data. At the same time, the results show that these gains coexist with risks related to cybersecurity threats, human capital constraints, and regulatory instability, which can weaken governance capacity if safeguards lag behind scaling. A further conclusion is that integration into the European digital space requires alignment not only of technologies, but also of

institutional rules, data governance standards, and oversight routines. Overall, the section supports a dual logic of modernization, where efficiency and transparency benefits must be matched by security, competence development, and stable regulatory steering.

6. The study concludes that the quality of digital reporting should be evaluated through an integrated framework distinguishing technical, semantic, and pragmatic dimensions, and linking them to regulatory architectures and oversight tools. The results show convergence around XBRL and Inline XBRL in digital financial reporting, but also persistent heterogeneity in tagging scope, validation rules, and the institutionalization of data quality mechanisms. Digital reporting is assessed as a double edged phenomenon, since it enables transparency and automated analytics while opening new channels for impression management, greenwashing, semantic opacity, and information overload. The section concludes that effective precautions require a combined toolkit that includes prescriptive taxonomies, automated validation, SupTech based anomaly detection, and digital operational resilience frameworks, with attention to proportionality for smaller entities and less mature markets. Overall, the central conclusion is that fragmented or weakly enforced regimes can turn digital disclosure into an amplifier of risk rather than a safeguard of transparency and market discipline.

7. The study concludes that Russia's full scale invasion of Ukraine has reshaped the national security agenda of EU countries by demonstrating how high intensity war can cascade into disruptions of governance, markets, energy supply, critical infrastructure, and social stability. In this context, public administration is identified as the institutional core that translates political commitments into coordinated procedures, lawful emergency regimes, and implementable programs capable of sustaining continuity of government and public trust. The analysis therefore supports a governance centered understanding of security, where resilience depends on administrative capacity for coordination, rapid decision implementation, and credible public communication under stress. A further conclusion is that security oriented governance must integrate continuity planning and institutional learning mechanisms, because crisis conditions reveal dependencies and vulnerabilities that routine administration may overlook. Overall, the section positions public administration not as a supporting function, but as a decisive capability that operationalizes security policy into reliable practice.

8. The study concludes that economic security requires an updated public administration approach because globalization and digitalization

https://doi.org/10.36690/PUBADM

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

simultaneously open access to markets, investment, and technology while increasing exposure to external shocks, financial dependence, and technological risks. The results clarify the structure of economic security and emphasize that strengthening it in Ukraine requires targeted governance priorities, including regulation of foreign participation in strategic sectors, support for national producers, and development of technological and production independence. Digital tools and management innovations are treated as enablers of monitoring and policy responsiveness, particularly through improved financial monitoring and institutional strengthening of the economic security system. The analysis also underscores the relevance of international economic institutions in shaping the external environment of national security and risk profiles. Overall, the section supports the conclusion that economic security is achieved through coordinated institutional design, data informed monitoring, and coherent policy instruments aligned with prolonged war conditions and post war recovery demands.

9. The study concludes that energy transformation in the Visegrád Group countries is governed within a tension between European climate neutrality commitments and post 2022 energy security shocks, especially where dependence on fossil fuels and Russian energy resources has shaped national policy constraints. The analysis demonstrates that the state remains a central actor in designing and implementing transitions, since infrastructure choices, regulatory frameworks, and investment coordination require institutional steering beyond market signals alone. A comparative perspective reveals both convergent and divergent governance models across Poland, Czechia, Slovakia, and Hungary, which has implications for regional cooperation and the trajectory of broader European integration in the energy sector. The section also supports a conclusion that energy policy governance must reconcile decarbonization with supply security and affordability, and that these objectives demand evidence based monitoring and adaptive institutional coordination. Overall, public governance capacity is presented as a determinant of whether energy transition becomes a stable development strategy or a sequence of reactive adjustments to shocks.

10. Based on the research results presented by the authors in this monograph, the following conclusions can be drawn. Public Administration 4.0 should be understood as a governance paradigm in which digital tools transform institutional design, integrated service delivery, and accountability, rather than as a narrow program of administrative automation. Sustainable digitalization requires the parallel development of legal and organizational interoperability, reliable data governance, and trust

building mechanisms, with success assessed through inclusion and institutional resilience. International experience is most valuable when translated into lessons that connect outcomes with enabling conditions and when adapted to national capacity, so that reforms become functional governance rather than symbolic imitation. The monograph also shows that procurement discipline, data stewardship, and safeguards are core administrative capacities that determine whether digital government can scale lawfully and reliably. Artificial intelligence can enhance efficiency and policy targeting, but it also increases governance risks related to bias, opacity, data security, and unequal access. Therefore, AI adoption must be governed as institutional change through accountable decision pathways, legality and ethics by design, and auditable oversight routines that protect legitimacy and public trust. Overall, effective digital governance emerges when modernization aligns efficiency with legality, integrity, inclusion, and security, strengthening the state’s capacity to deliver public value under conditions of turbulence and long term transformation.

References

1. AABE Economics. (2023). *Energy economy of Hungary and Austria in the face of energy challenges*. https://aab-economics.kmf.uz.ua/aabe/article/view/72
2. Accountancy Europe. (2021). *Response to the European Commission consultation on strengthening the quality of corporate reporting and its enforcement* [Position paper]. https://accountancyeurope.eu/wp-content/uploads/2022/12/Accountancy_Europe_response_to-_EC_corporate_reporting_quality-enforcement_2021.pdf
3. Alles, M., & Gray, G. L. (2012). The pros and cons of XBRL adoption in Greece. *International Journal of Economics and Business Administration, 1*(1), 91–106. https://ideas.repec.org/a/tei/journl/v1y2012i1p91-106.html
4. Atlantic Council. (2019). *Hungary's energy landscape: MOL Group's strategic role and renewable energy expansion*. https://www.atlanticcouncil.org/blogs/energysource/hungarys-energy-landscape-mol-groups-strategic-role/
5. Bache, I. (2012). *Multi-level governance in the European Union*. https://www.researchgate.net/publication/288802300_Multi-Level_Governance_in_the_European_Union
6. Benko, M. M., & Sopko, V. V. (2011). Bukhgalterskyi oblik u skladi informatsiinoi systemy pidpryiemstva yak obiektu informatsiinykh tekhnolohii [Accounting as part of the information system of the enterprise as an object of information technologies]. *Bukhgalterskyi oblik i audyt*, (3), 117–124. Retrieved from the Vernadsky National Library of Ukraine database. URL: http://www.business-navigator.ks.ua/journals/2011/24_2011/24_2011.pdf#page=115
7. Bielai, S. V., Kobzar, O. F., Yevtushenko, I. V., Korniienko, V. O., & Koba, O. V. (2021). The legal regulation of service and combat activities of the security and defense sector of Ukraine in crisis situations. *Journal of the National Academy of Legal Sciences of Ukraine, 28*(2), 76–85. https://doi.org/10.37635/jnalsu.28(2).2021.76-85
8. Bielai, S., Antonova, L., Hololobov, S., Yevtushenko, I., & Sporyshev, K. (2024). The impact of a practice-oriented paradigm on public administration and national security. *International Journal of Sustainable Development and Planning, 19*(1), 277–288. https://doi.org/10.18280/ijsdp.190126
9. Blue Europe. (2024). *A brief outlook of renewable energy in Slovakia: Trend and potential*. https://www.blue-europe.eu/analysis-en/short-analysis/a-brief-outlook-of-renewable-energy-in-slovakia-trend-and-potential/
10. Bonsón, E., Cortijo, V., & Escobar, T. (2009). Towards the global adoption of XBRL using International Financial Reporting Standards (IFRS). *International Journal of Accounting Information Systems, 10*(1), 46–60. https://doi.org/10.1016/j.accinf.2008.10.002
11. Borblik, K. (2022). *Digitalization of the Ukrainian economy: Global challenges and local dilemmas*. MRU CRIS Repository.

https://cris.mruni.eu/server/api/core/bitstreams/6fe83e53-6c39-4bf7-956c-46f59ccb0942/content

12. Borysova, O., & Rudnik, D. (2024). Theoretical foundations and models of European integration. *Scientific and Theoretical Almanac Grani, 27*(5), 105–112. https://doi.org/10.15421/172498
13. Broeders, D., & Prenio, J. (2018). *Innovative technology in financial supervision (SupTech): The experience of early users* (FSI Insights on policy implementation No. 9). Bank for International Settlements. https://www.bis.org/fsi/publ/insights9.pdf
14. Brookings Institution. (2024). *Ukraine: Digital resilience in a time of war*. Brookings. https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf
15. 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
16. Canadian Management Centre. (2024). *Discover 2024 AI trends*. Retrieved March 22, 2025, from: https://cmcoutperform.com/
17. Carahsoft. (2025). *AI solutions for government: AI in the public sector*. Retrieved March 20, 2025, from: https://www.carahsoft.com
18. Carbon capture and storage (CCS). (2025). https://www.futurecoal.org/sustainable-coal/carbon-capture-and-storage/
19. Christin, S., & Stefanini, S. (2018, November 20). Hungary wants end to coal power by 2030. *Climate Home News*. https://www.climatechangenews.com/2018/11/20/hungary-wants-end-coal-power-2030
20. Committee of Sponsoring Organizations of the Treadway Commission, & Association of Certified Fraud Examiners. (2023). *Fraud risk management guide* (2nd ed.): Executive summary. COSO & ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/fraud-risk-management-guide-executive-summary.ashx
21. Committee of Sponsoring Organizations of the Treadway Commission. (2023). *Fraud risk management guide* (2nd ed.). COSO. https://www.aicpa-cima.com/resources/landing/coso-fraud-risk-management-guide
22. Cordella, A., & Hesse, J. (2015). E-government in the making: An actor-network perspective. *Transforming Government: People, Process and Policy*, 9(1), 104–125. https://doi.org/10.1108/TG-02-2014-0006
23. Council Decision (CFSP) 2022/1968 of 17 October 2022 on a European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine). (2022). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dec/2022/1968/oj
24. Council Decision (CFSP) 2024/890 of 18 March 2024 amending Decision (CFSP) 2021/509 establishing a European Peace Facility. (2024). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024D0890
25. Council Implementing Decision (EU) 2022/382 of 4 March 2022 establishing the existence of a mass influx of displaced persons from Ukraine within the meaning of Article 5 of Directive 2001/55/EC, and having the effect of introducing temporary protection. (2022). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dec_impl/2022/382/oj

26. Council Implementing Decision (EU) 2025/1460 of 15 July 2025 extending temporary protection as introduced by Implementing Decision (EU) 2022/382. (2025). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dec_impl/2025/1460/oj
27. Council of Europe. (2025). *Manual on education in the field of human rights with the participation of youth: Globalization*. Retrieved from: https://www.coe.int/uk/web/compass/globalisation
28. Council of the European Union. (2022, March 21). *A Strategic Compass for Security and Defence*. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-security-and-defence/
29. Council of the European Union. (2022, March 23). *European Peace Facility: Council doubles funding to support the Ukrainian armed forces*. https://www.consilium.europa.eu/en/press/press-releases/2022/03/23/european-peace-facility-council-doubles-funding-to-support-the-ukrainian-armed-forces/
30. Council of the European Union. (2024, June 25). *Temporary protection: Council agrees to extend temporary protection for people fleeing from Ukraine*. https://www.consilium.europa.eu/en/press/press-releases/2024/06/25/temporary-protection-council-agrees-to-extend-temporary-protection-for-people-fleeing-from-ukraine/
31. Council of the European Union. (2024). *Integrated Political Crisis Response (IPCR) arrangements*. https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/
32. Country nuclear power profiles 2022 edition: Czech Republic. (2022). https://www-pub.iaea.org/MTCD/publications/PDF/cnpp2022/countryprofiles/CzechRepublic/CzechRepublic.htm
33. Czech Republic advances biogas production to enhance energy independence. (2024). *World Bio Market Insights*. https://worldbiomarketinsights.com/czech-republic-advances-biogas-production-to-enhance-energy-independence/
34. Czech Republic energy mix and decarbonisation pressures: Balancing between nuclear and renewables. (2025). *CzechTrade Offices*. https://www.czechtradeoffices.com/se/news/czech-government-updates-national-energy-plan-boosting-nuclear-and-renewables
35. Datskiv, R. M. (2004). Economic security in the global dimension. *Current Economic Problems*, 7(37), 143–153.
36. Deloitte. (2024). *Artificial intelligence in finance and accounting: From automation to augmentation* [Report]. Deloitte Insights. https://www2.deloitte.com
37. Dolowitz, D. P., & Marsh, D. (2000). Learning from abroad: The role of policy transfer in contemporary policy-making. *Governance, 13*(1), 5-24. https://doi.org/10.1111/0952-1895.00121
38. Duleba, N. V. (2008). Research on the transformation of the concept of "economic security of an enterprise". Retrieved from http://www.economy.nayka.com.ua/?op=1&z=2387
39. Dumchykov, M., Utkina, M., & Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering, 12*(4), 481–490. https://doi.org/10.18280/ijsse.120409

40. Dunn, T. M. (2012, November 28). Neo-functionalism and the European Union. *E-International Relations*. https://www.e-ir.info/2012/11/28/neo-functionalism-and-the-european-union/
41. Dyba, O., & Osadchy, E. (2014). The impact of globalization on the socio-economic state of Ukraine. *Securities Market in Ukraine*, 7, 19–28.
42. e-Estonia. (2025). *AI Leap programme to bring AI tools to all schools*. Retrieved March 17, 2025, from: https://e-estonia.com/estonia-announces-a-groundbreaking-national-initiative-ai-leap-programme-to-bring-ai-tools-to-all-schools/
43. EFRAG. (2023). *European Sustainability Reporting Standards (ESRS) – Set 1* [Standards]. European Financial Reporting Advisory Group. https://xbrl.efrag.org/e-esrs/esrs-set1-2023.html
44. Electricity link LitPol Link. (2023). https://enmin.lrv.lt/en/strategic-projects/electricity-sector/electricity-link-litpol-link/
45. EU4Digital. (2025). *EGOV4Ukraine*. Retrieved December 9, 2025, from https://eufordigital.eu/discover-eu/egov4ukraine/
46. European Commission, Directorate-General for Taxation and Customs Union. (2023). *Compliance risk management in the digital era* (CRM Guide). https://taxation-customs.ec.europa.eu/system/files/2024-01/2023_CRM_Guide.pdf
47. 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). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016DC0179
48. 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
49. 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
50. 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
51. European Commission. (2022, May 18). *REPowerEU plan* (COM(2022) 230 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0230
52. European Commission. (2022). *Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 as regards corporate sustainability reporting (Corporate Sustainability Reporting Directive)*. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2464/oj
53. European Commission. (2025, June 17). *Commission proposes a roadmap to phase out Russian gas and oil imports by 2027*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1540

54. European Commission. (2025, May 6). *REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu_en
55. European Commission. (2025). *Emergency Response Coordination Centre (ERCC)*. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en
56. European Court of Auditors. (2025). *The Recovery and Resilience Facility's contribution to the digital transition in the EU: Risks to delivering EU ambitions* (Special Report 13/2025). https://www.eca.europa.eu/en/publications/sr-2025-13
57. European Environment Agency. (2025). *Slovakia* (Europe environment 2025 country profile). https://www.eea.europa.eu/en/europe-environment-2025/countries/slovakia
58. European External Action Service. (2022). *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
59. 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
60. European External Action Service. (2025). *Third report on Foreign Information Manipulation and Interference (FIMI) threat*. https://www.eeas.europa.eu/eeas/third-report-foreign-information-manipulation-and-interference-fimi-threat_en
61. European Investment Bank (EIB) REPowerEU funding programs: 45 billion EUR allocation (2022–2024). (2024). https://bankwatch.org/eib
62. European Investment Bank. (2025). *Financing the modernization of the Czech energy infrastructure: Support to ČEZ*. https://www.eib.org
63. 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
64. 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
65. 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
66. 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
67. 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*

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

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

68. 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
69. European Securities and Markets Authority. (2017). *European Single Electronic Format (ESEF) Reporting Manual*(ESMA32-60-254). ESMA. https://www.esma.europa.eu/document/esef-reporting-manual
70. European Securities and Markets Authority. (2025). *ESEF Reporting Manual – Preparation of annual financial reports in ESEF format (Update October 2025)* (ESMA32-60-254 Rev). ESMA. https://www.esma.europa.eu/sites/default/files/library/esma32-60-254_esef_reporting_manual.pdf
71. European Union Strategy for Energy System Integration. (2022). https://greentransform.org.ua/strategiya-yevropejskogo-soyuzu-z-integratsiyi-energetychnoyi-systemy/
72. European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
73. European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557
74. European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj
75. 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). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
76. Europeanization processes of the EU energy policy in Visegrad countries in the years 2005–2018. (2021). https://www.mdpi.com/1996-1073/14/7/1802
77. FASB. (2023). *US GAAP Financial Reporting Taxonomy – 2023 release*. Financial Accounting Standards Board. https://www.fasb.org/page/PageContent?pageId=1.1.10
78. Fedorenko, T., & Zahorodnia, A. (2024). Economic security of the enterprise: Modern challenges and threats. *Intellectualization of Logistics and Supply Chain Management*, 26, 75–79. https://doi.org/10.46783/smart-scm/2024-26-6
79. Fedorenko, T., Dolynskiy, S., & Zahorodnia, A. (2022). An evolutionary approach to the interpretation of the term "economic security of enterprises". *International Journal of Innovative Technologies in Economy*, 4(40), 1–6. https://doi.org/10.31435/rsglobal_ijite/30122022/7926
80. Financial Action Task Force. (2012). *International standards on combating money laundering and the financing of terrorism and proliferation: The FATF*

Recommendations (Updated October 2025). FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.pdf

81. Financial Action Task Force. (2021). *Guidance on risk-based supervision*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Risk-Based-Supervision.pdf.coredownload.pdf
82. Financial Stability Board. (2020). *The use of supervisory and regulatory technology by authorities and regulated institutions: Market developments and financial stability implications*. https://www.fsb.org/uploads/P091020.pdf
83. Fukuyama, F. (2014). *Political order and political decay: From the industrial revolution to the globalization of democracy*. Farrar, Straus and Giroux.
84. Gaozhao, D., Wright, J. E., & Gainey, M. K. (2023). Bureaucrat or artificial intelligence: People's preferences and perceptions of government service. *Public Management Review*, 1–28. https://doi.org/10.1080/14719037.2022.2160488
85. Global Energy Prize. (2024). *Hungary's Paks II NPP receives approval for pouring of first concrete*.
86. Global Reporting Initiative. (2021). *GRI 1: Foundation 2021; GRI 2: General Disclosures 2021; GRI 3: Material Topics 2021 (Universal Standards)*. GRI. https://www.globalreporting.org/standards/standards-development/universal-standards/
87. Government Digital Service. (2025). *Introducing GOV.UK Verify*. Retrieved March 22, 2025, from: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
88. Hinton, G., Osindero, S., & Teh, Y. (2006). A fast learning algorithm for deep belief nets. *Neural Computation*, 18(7), 1527–1554. https://doi.org/10.1162/neco.2006.18.7.1527
89. Hungary and Slovakia have alternatives to oil and gas from the Russian Federation, but they only increase their dependence, experts. (2025, May 15). https://www.slovoidilo.ua/2025/05/15/novyna/polityka/uhorshhyna-ta-slovachchyna-mayut-alternatyvy-nafti-hazu-rf-vony-lyshe-zbilshuyut-svoyu-zalezhnist-eksperty
90. Hungary and Slovakia resist EU's energy security plan. (2025, June 16). *Euronews*. https://www.euronews.com/my-europe/2025/06/16/hungary-and-slovakia-resist-eus-energy-security-plan
91. Hungary: Energy market overview: Nuclear and renewables. (2024). https://www.trade.gov/market-intelligence/hungary-energy-market-overview-nuclear-and-renewables
92. IBM. (2025). *What is NLP (natural language processing)?* Retrieved March 22, 2025, from: https://www.ibm.com/think/topics/natural-language-processing
93. ICAEW. (2024). *How standards can help squash the greenwash*. Institute of Chartered Accountants in England and Wales. https://www.icaew.com/insights/viewpoints-on-the-news/2024/sep-2024/how-standards-can-help-squash-the-greenwash
94. IFRS Foundation. (2020). *IFRS Taxonomy 2020 – Illustrated*. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs-taxonomy/

95. IFRS Foundation. (2023). *IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information; IFRS S2 Climate-related Disclosures*. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs-sustainability-standards
96. Ingram, G., & Vora, P. (2024). *Ukraine: Digital resilience in a time of war* (Working Paper 185). Brookings Institution. URL: https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf
97. International Monetary Fund. (2025). *AI projects in financial supervisory authorities* (IMF Working Paper No. WP/25/199). https://doi.org/10.5089/9798229025263.001
98. International Trade Administration. (2024). *Hungary: Energy*. https://www.trade.gov/country-commercial-guides/hungary-energy
99. Interoperable Europe Portal. (2025). *Governance: Ukraine*. Retrieved December 9, 2025, from https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/governance-ukraine
100. IOSCO. (2021). *Environmental, social and governance (ESG) ratings and data providers: Final report*. International Organization of Securities Commissions. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD690.pdf
101. Ivanova, N. (2024). Digital transformation of Ukraine: Impact on the economy, quality of life and achievement of sustainable development goals. *Economics of Systems Development*, 6(1). https://doi.org/10.32782/2707-8019/2024-1-9
102. 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
103. Key ESG. (2023). *Building a sustainable future: A practical guide to ESG reporting and carbon accounting for infrastructure investors*. KEY ESG. https://www.keyesg.com/article/building-a-sustainable-future-a-practical-guide-to-esg-reporting-and-carbon-accounting-for-infrastructure-investors
104. Koval, Ya. (2024). Peculiarities of information and analytical support in decision-making within government bodies. *Public Administration and Law Review*, 3(19), 4–16. https://doi.org/10.36690/2674-5216-2024-3-4-16
105. Koval, Ya., Fedorenko, T., & Zahorodnia, A. (2024). Information and analytical activity in the system of economic security of the enterprise. *Intellectualization of Logistics and Supply Chain Management*, 24, 83–88. https://doi.org/10.46783/smart-scm/2024-24-9
106. Kovalenko, M. A., Nagorodna, I. I., & Radvanska, N. V. (2009). *Economic security of a corporate enterprise*. Kharkiv: Oldi-plus.
107. Kovalov, B., Karintseva, O., Kharchenko, M., Khymchenko, Y., & Tarasov, V. (2023). Methods of evaluating digitization and digital transformation of business and economy: The experience of OECD and EU countries. *Economics of Systems Development*, 5(1), 18–25. https://doi.org/10.32782/2707-8019/2023-1-3
108. Kryshtanovych, M., Antonova, L., Filippova, V., Dombrovska, S., & Pidlisna, T. (2022). Influence of COVID-19 on the functional device of state governance of economic growth of countries in the context of ensuring security. *International Journal of Safety and Security Engineering, 12*(2), 193–199. https://doi.org/10.18280/ijsse.120207

109. Kryshtanovych, M., Kupchak, V., Voronov, O., Larina, N., & Humeniuk, A. (2023). Formation of social leadership in the system of public safety and security through the use of modern modeling techniques. *International Journal of Safety and Security Engineering, 13*(2), 317–324. https://doi.org/10.18280/ijsse.130213

110. Kryvovyazyuk, I. V. (2013). *Economic diagnostics*. Kyiv: TsUL.

111. 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

112. Kutsyk, P. O., Kovtun, O. I., & Bashtyanin, G. I. (2015). *Global economy: Principles of formation, functioning and development*. Lviv: Merts Acad.

113. Laptiev, S., Mazur, I., Koval, Ya., & Laptiev, M. (2024). Business reputation and resilience: Digital skill strategies in a transformative era. In M. Denysenko, L. Khudoliy, & S. Laptiev (Eds.), *Digital skills in a digital society: Requirements and challenges* (pp. 189–209). Estonia: Scientific Center of Innovative Research. https://doi.org/10.36690/DSDS-189-209

114. Levitt, T. (2025). The globalization of markets. *Harvard Business Review*. Retrieved from https://hbr.org/1983/05/the-globalization-of-markets

115. Lukyanenko, D., Poruchnik, A., & Stolyarchuk, Ya. (2010). Global financial imbalances and their economic consequences. *Journal of European Economy*, 9(1), 73–92.

116. MacFarlane, S. N., & Khong, Y. F. (Eds.). (2006). *Human security and the UN: A critical history* (United Nations intellectual history project, illustrated ed.). Bloomington, IN: Indiana University Press.

117. Maksymak, H. (2018). Як далі будувати співпрацю України з Вишеградською групою? [How to further build Ukraine’s cooperation with the Visegrad Group?]. *Perspektyva*. http://prismua.org/%D1%8F%D0%BA-%D0%B7-%D0%B2/

118. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence (1955). *AI Magazine*, 27(4), 12–14.

119. Ministry of Digital Transformation of Ukraine. (2025). *Diia (GovTech project description)*. Retrieved December 9, 2025, from https://digitalstate.gov.ua/projects/govtech/diia

120. Ministry of Economy of Ukraine. (2013). *Methodology for calculating the level of economic security of Ukraine*. Retrieved from: https://zakon.rada.gov.ua

121. Mizhnarodnyi fond «Vidrodzhennia». (2025). *Doslidzhennia nadannia sotsialnykh posluh: Problemy ta stan sfery sotsialnykh posluh v Ukraini* [Study of the provision of social services: Problems and state of the social services sector in Ukraine]. Retrieved March 19, 2025, from: https://parlament.org.ua/news/problemy-ta-stan-sfery-soczialnyh-poslug-v-ukrayini-lzi-provela-prezentacziyu-doslidzhennya/

122. Newell, A., Shaw, C., & Simon, H. (1959). Report on a general problem-solving program. In *Proceedings of the International Conference on Information Processing* (pp. 256–264).

123. Nuclear Expediting the Energy Transition (NEXT) One Stop Shop for Small Modular Reactor (SMR) Support Program. (2024).

https://researchfunding.duke.edu/nuclear-expediting-energy-transition-next-one-stop-shop-small-modular-reactor-smr-support-program

124. OECD (2024), *Enhancing Resilience by Boosting Digital Business Transformation in Ukraine*, OECD Publishing, Paris, https://doi.org/10.1787/4b13b0bb-en.
125. OECD (2024), *OECD Digital Economy Outlook 2024 (Volume 2): Strengthening Connectivity, Innovation and Trust*, OECD Publishing, Paris, https://doi.org/10.1787/3adf705b-en.
126. OECD Observatory of Public Sector Innovation. (2025). *E-procurement system ProZorro*. Retrieved December 9, 2025, from https://oecd-opsi.org/innovations/eprocurement-system-prozorro
127. OECD. (2011). *Regulatory policy and governance: Supporting economic growth and serving the public interest*. OECD Publishing. https://doi.org/10.1787/9789264116573-en
128. 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
129. OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*.
130. OECD. (2024). *OECD Digital Economy Outlook 2024, Volume 2: Strengthening connectivity, innovation and trust*. OECD Publishing. https://doi.org/10.1787/3adf705b-en
131. 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/
132. Open Data Portal of Ukraine. (2025). *Open data portal*. Retrieved December 9, 2025, from https://data.gov.ua/en
133. Organisation for Economic Co-operation and Development. (2014). *Regulatory enforcement and inspections: OECD best practice principles for regulatory policy*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/11/regulatory-enforcement-and-inspections_9f73c9ea/fc8bbb87-en.pdf
134. Organisation for Economic Co-operation and Development. (2014). *Recommendation of the Council on digital government strategies* (OECD-LEGAL-0406). OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406
135. Organisation for Economic Co-operation and Development. (2018). *OECD regulatory enforcement and inspections toolkit*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/10/oecd-regulatory-enforcement-and-inspections-toolkit_83d60f55/9789264303959-en.pdf
136. Organisation for Economic Co-operation and Development. (2019). *Analytics for integrity: Data-driven approaches for enhancing corruption and fraud risk assessments*. OECD Publishing. https://doi.org/10.1787/b354a27e-en
137. Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on artificial intelligence* (OECD/LEGAL/0449). OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

138. Organisation for Economic Co-operation and Development. (2020). *OECD public integrity handbook*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/05/oecd-public-integrity-handbook_598692a5/ac8ed8e8-en.pdf
139. Organisation for Economic Co-operation and Development. (2021). *Managing and improving tax compliance*. OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/09/managing-and-improving-tax-compliance_4d5f9c4c/12f8f563-en.pdf
140. Organisation for Economic Co-operation and Development. (2022). *Building trust to reinforce democracy*. OECD Publishing. https://www.oecd.org/en/publications/building-trust-to-reinforce-democracy_bb2ff49e-en.html
141. Organisation for Economic Co-operation and Development. (2024a). *OECD Survey on Drivers of Trust in Public Institutions: 2024 results*. OECD Publishing. https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_a6fc7d55-en.html
142. Organisation for Economic Co-operation and Development. (2024b). *Trust in public institutions: Trends and drivers*(OECD Trust Survey data and insights). https://www.oecd.org/en/topics/trust-in-government.html
143. Organisation for Economic Co-operation and Development. (2025). *OECD regulatory policy outlook 2025*. OECD Publishing. https://doi.org/10.1787/56b60e39-en
144. Organisation for Economic Co-operation and Development. (2025). *Tax administration 2025: Comparative information on OECD and other advanced and emerging economies*. OECD Publishing. https://doi.org/10.1787/cc015ce8-en
145. Organization for Economic Cooperation and Development. (2025). *OECD*. Retrieved from: http://www.oecd.org
146. Palamarchuk, A. I. (2024). Sudovyi zakhyst prava na dostup do informatsii pro stan navkolyshnoho seredovyshcha v umovakh voiennoho stanu [Judicial protection of the right to access information on the state of the environment under martial law]. In *Suchasni vyklyky ta aktualni problemy sudovoi systemy v Ukraini* [Contemporary challenges and pressing problems of the judicial system in Ukraine] (p. 466). Chernivtsi, Ukraine. Retrieved March 2, 2025, from: https://web.ccu.gov.ua/library/suchasni-vyklyky-ta-aktualni-problemy-sudovoyi-reformy-v-ukrayini-2024
147. Pasternak-Taranushenko, G. A. (1994). *Economic security of the state*. Kyiv: Institute of State Administration and Self-Government at the Ministry of Finance of Ukraine.
148. Peck, J., & Theodore, N. (2010). Mobilizing policy: Models, methods, and mutations. *Geoforum, 41*(2), 169-174. https://doi.org/10.1016/j.geoforum.2010.01.002
149. Pihariiev, Yu., & Kosteniuk, N. (2021). Digitalization of public administration as a factor of Ukraine’s digital transformation. *Aktualni problemy derzhavnoho upravlinnia*, 2(83), 92–96. https://doi.org/10.35432/1993-8330appa2832021237257
150. Pilko, A. (2014). Evolution of models and perspective directions of development of security studies. In *Economic security in the conditions of globalization of the world*

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

economy: Collective monograph (Vol. 1, pp. 166–177). FOP Drobyazko S. I. https://shorturl.at/0rSs0

151. Pohorelenko, A. (2018). Shtuchnyi intelekt: sutnist, analiz zastosuvannia, perspektyvy rozvytku [Artificial intelligence: Essence, application analysis, development prospects]. *Ekonomichni nauky*, (32), 22–27.
152. Poland enacts regulations to accelerate development of carbon dioxide capture, utilisation and storage technology (CCUS). (2024). https://cms-lawnow.com/en/ealerts/2024/02/poland-enacts-regulations-to-accelerate-development-of-carbon-dioxide-capture-utilisation-and-storage-technology-ccus?utm_source=chatgpt.com
153. Prav, R. (2021). Ways to improve the efficiency of mechanisms for ensuring the national security of Ukraine in the context of European experience. *Scientific Perspectives, 9*(15), 197–206. https://doi.org/10.52058/2708-7530-2021-9(15)-197-206
154. Press Information Bureau. (2024). *India's AI revolution*. Retrieved March 27, 2025, from: https://pib.gov.in/PressReleasePage.aspx?PRID=2108810
155. Pritchett, L., Woolcock, M., & Andrews, M. (2013). Looking like a state: Techniques of persistent failure in state capability for implementation. *Journal of Development Studies, 49*(1), 1–18.
156. Pritchett, L., Woolcock, M., & Andrews, M. (2013). Looking like a state: Techniques of persistent failure in state capability for implementation. *Journal of Development Studies, 49*(1), 1–18.
157. PwC. (2022). *Strengthening the quality of corporate reporting and its enforcement: PwC response to the European Commission consultation* [Submission]. PricewaterhouseCoopers. https://www.pwc.com/gx/en/about/assets/response-corporate-reporting-improving-its-quality-and-enforcement-2022.pdf
158. PwC. (2025). *Strategy in the age of AI*. Retrieved March 12, 2025, from: https://www.pwc.com/us/en/services/ai.html
159. Ranerup, A., & Henriksen, H. Z. (2022). Digital discretion: Unpacking human and technological agency in automated decision making in Sweden's social services. *Social Science Computer Review*, 40(2), 445–461. https://doi.org/10.1177/0894439320980434
160. Renewable energy in Czech Republic. (2024). https://cms.law/en/int/expert-guides/cms-expert-guide-to-renewable-energy/czech-republic
161. Reznik, N. P., Zahorodnia, A. S., & Chornenka, L. M. (2021). Analysis of the logistics component of the economic security system of enterprises. *International Journal of Innovative Technologies in Economy*, 4(36), 109–113.
162. Robertson, R. (1992). *Globalization: Social theory and global culture*. London: Sage.
163. Rose, R. (1991). What is lesson-drawing? *Journal of Public Policy, 11*(1), 3–30.
164. Rosslowe, C. (2020). *Coal-free Czechia 2030*. https://ember-energy.org/latest-insights/coal-free-czechia-2030/
165. Selivanova, N. M., Kalabina, V. O., & Minzhyrian, N. I. (2024). Digitalization of accounting and financial reporting in Ukraine. *Economics: Time Realities*, (4[74]), 89–98. https://doi.org/10.15276/ETR.04.2024.10
166. Serhieiev, V., Voronina, Y., Zolotov, A., Akimova, L., Rovynska, K., & Akimov, O. (2025). Innovative competences within public administration landscape: sustainable

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

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

167.Shcherbyna, V. M. (2006). Information security of economic security of enterprises and institutions. *Current Problems of Economy*, 10(64), 220–225.

168.Shcho take shtuchnyi intelekt: Istoriia, vydy ta skladovi [What is artificial intelligence: History, types and components]. (2025). *GigaCloud*. Retrieved March 19, 2025, from: https://gigacloud.ua/articles/shho-take-shtuchnyj-intelekt-istoriya-vydy-ta-skladovi/

169.Shemaeva, L. G. (2009). *Ensuring the economic security of an enterprise based on the management of strategic interaction with external entities*. Kyiv: National Security and Defense Council of Ukraine, National Institute of International Security Problems.

170.Shevchenko, A. I., & Baranovskyi, S. V. (2023). *Stratehiia rozvytku shtuchnoho intelektu v Ukraini. Rozdil 4. Stan rozvytku sfery shtuchnoho intelektu v Ukraini* [Strategy for the development of artificial intelligence in Ukraine. Section 4. State of development of the artificial intelligence sphere in Ukraine] (p. 66). Kyiv, Ukraine. Retrieved March 10, 2025, from: https://jai.in.ua/archive/2023/ai_mono.pdf

171.Shevchuk, O. (2024). Transformation of the fundamental principles of accounting and control in the system of electronic transactions. *Herald of Economics*, no. 2, Aug. 2024, pp. 131-49, https://doi.org/10.35774/visnyk2024.02.131.

172.Shkarlet, S. M. (2007). Evolution of the category “security” in the scientific and economic environment. *Formation of Market Relations*, 6, 7–12.

173.Shlemko, V. T., & Binko, I. F. (1997). *Economic security of Ukraine: Essence and directions of provision*. Kyiv: NISD.

174.Shnipko, O. S. (2006). Types and factors of security of hierarchical economic systems: Theoretical and methodological aspect. *Current Problems of Economy*, 5(59), 78–85.

175.Sidenko, V. R. (2012). Modification of the world economy under the influence of the latest factors of the global transformation crisis. *Economy of Ukraine*, 5, 18–31.

176.Slovakia to end renewable subsidies by 2026. (2025). *Euractiv*. https://www.euractiv.com/section/eet/news/slovakia-to-end-renewable-subsidies-by-2026/

177.Slovakia: Gas conflict with Ukraine as a delaying maneuver. (2025). *Deutsche Welle*. https://www.dw.com/uk/slovaccina-gazovij-konflikt-z-ukrainou-ak-okozamiluvalnij-manevr/a-71209938

178.Smart Nation and Digital Government Office. (2025). *Smart Nation Singapore initiative*. Retrieved March 22, 2025, from: https://www.smartnation.gov.sg/

179.State Enterprise Diia. (2025). *Open Data Web Portal*. Retrieved December 9, 2025, from https://se.diia.gov.ua/en/opendata

180.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

181.Stephen, G. (2004). Multi-level Governance and the European Union', in Ian Bache, and Matthew Flinders (eds), *Multi-level Governance*, https://doi.org/10.1093/0199259259.003.0007

182. Sukhorukov, A. I., & Ladyuk, O. D. (2007). *Financial security of the state: A textbook*. Kyiv: Center for Educational Literature.
183. Svystun, L. A., & Levkova, R. M. (2017). Improving the cost management system of an enterprise in an unstable economy. *Economy and Region*, 4, 57–62.
184. 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
185. Syrotin, V. D. (2023). Features of digitalization in the field of public administration. *Problemy suchasnykh transformatsii. Seriia: Pravo, publichne upravlinnia ta administruvannia*, 9. https://doi.org/10.54929/2786-5746-2023-9-02-06
186. Sytnyk, H. (2011). Institutional and civilizational paradigm of research of problems and public administration aspects of national security. *Bulletin of the National Academy for Public Administration under the President of Ukraine, 2*, 25–34. https://h7.cl/1g9ws
187. Tenyukh, Z., Pelekh, U., & Khocha, N. (2022). Application of digital technologies in accounting and auditing at enterprises of Ukraine. Scientific Bulletin of Mukachevo State University. Series "Economics", 9(4), 46-55. https://doi.org/10.52566/msu-econ.9(4).2022.46-55
188. The Czech Republic announced the date for the complete abandonment of coal and the transition to nuclear energy. (2025). https://unn.ua/news/chekhiia-oholosyla-datu-povnoi-vidmovy-vid-vuhillia-ta-perekhid-na-atomnu-enerhetyku
189. Toronto Centre. (2018). *SupTech: Leveraging technology for better supervision*. https://stage.torontocentre.org/media/acfupload/SupTech_Leveraging_Technology_for_Better_Supervision_Updated_Link_copy_1.pdf
190. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433–460. https://doi.org/10.1093/mind/LIX.236.433
191. U.S. Securities and Exchange Commission. (2018). *Inline XBRL filing of tagged data* (Release No. 33-10514; 34-83551; IC-33148). U.S. SEC. https://www.sec.gov/rules/final/2018/33-10514.pdf
192. United Nations Department of Economic and Social Affairs. (2024). *United Nations e-government survey 2024: Accelerating digital transformation for sustainable development*. UN DESA. https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf
193. United Nations Department of Economic and Social Affairs. (2024). *Addendum on AI and digital government: An addendum to the 2024 UN e-government survey*. UN DESA. https://desapublications.un.org/sites/default/files/publications/2024-10/Addendum%20on%20AI%20and%20Digital%20Government%20%20E-Government%20Survey%202024.pdf
194. United Nations Development Programme. (2021). *UNDP strategic plan, 2022-2025*. https://strategicplan.undp.org
195. 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

196. Vahanova, L. V., Yurychyna, I. A., & Karpanasiuk, O. S. (2022). Upravlinske rishennia yak forma realizatsii orhanizatsiinoi funktsii derzhavnoho upravlinnia [Managerial decision as a form of implementing the organisational function of public administration]. *Visnyk Khmelnytskoho natsionalnoho universytetu*, (1), 94–98.
197. Valentinetti, D., & Rea, M. A. (2013). XBRL for financial reporting: Evidence on Italian GAAP. *International Journal of Accounting Information Systems, 14*(1), 45–63. https://doi.org/10.1016/j.accinf.2012.09.001
198. Varnalii, Z. S. (Ed.). (2009). *Economic security: A textbook*. Kyiv: Knowledge.
199. Vasyltsiv, T., Mulska, O., Levytska, O., Lupak, R., Semak, B., & Shtets, T. (2024). Factors of the Development of Ukraine's Digital Economy: Identification and Evaluation. *Science and Innovation*, *18*(2), 44–58. https://doi.org/10.15407/scine18.02.044
200. Veale, M., & Brass, I. (2019). Administration by algorithm? Public management meets public sector machine learning. In *Algorithmic regulation* (pp. 1–30). https://doi.org/10.31235/osf.io/mwhnb
201. Verbivska, L., Abramova, M., Gudz, M., Lyfar, V., & Khilukha, O. (2023). Digitalization of the Ukrainian economy during a state of war is a necessity of the time. *Amazonia Investiga*, *12*(68), 184-194. https://doi.org/10.34069/AI/2023.68.08.17
202. Vlasyuk, O. S. (2008). *Theory and practice of economic security in the system of economic science*. Kyiv: National Institute of International Security Problems under the National Security and Defense Council of Ukraine.
203. Vorobyov, V. I. (2011). Methodological foundations of building a comprehensive system of economic security of an enterprise. *Scientific Notes*, 1(19), 38–44.
204. Weizenbaum, J. (1966). ELIZA – A computer program for the study of natural language communication between man and machine. *Communications of the ACM*, 9(1), 36–45. https://doi.org/10.1145/365153.365168
205. Wolf Theiss. (2023). *Winds of change: Positive outlook for Hungary's wind energy regulations*. https://www.wolftheiss.com/insights/positive-outlook-for-hungarys-wind-energy-regulations/
206. World Bank Group. (2019). *Warning signs of fraud and corruption in procurement*. https://documents1.worldbank.org/curated/en/223241573576857116/pdf/Warning-Signs-of-Fraud-and-Corruption-in-Procurement.pdf
207. World Bank. (2018). *From spreadsheets to SupTech: Technology solutions for market conduct supervision* (Discussion note, June 2018). https://documents1.worldbank.org/curated/en/612021529953613035/pdf/127577-REVISED-Suptech-Technology-Solutions-for-Market-Conduct-Supervision.pdf
208. World Bank. (2022). *GovTech maturity index: 2022 update.*
209. World Nuclear News. (2025, June 5). KHNP sets out plans for USD18.6bn Czech nuclear project. https://www.world-nuclear-news.org/articles/khnp-sets-out-plans-for-usd186bn-czech-nuclear-project.
210. World Trade Organization. (n.d.). *WTO*. Retrieved from http://www.wto.org

211. XBRL International. (2024). *About XBRL: Improving business reporting*. XBRL International. https://www.xbrl.org/the-standard/what/an-overview-of-xbrl/
212. XBRL US. (2022). *Data Quality Committee (DQC) rules and guidance*. XBRL US. https://xbrl.us/data-quality/rules-guidance/
213. Yarova, I., Mishenin, Y. Methodology of formation of economic and socio-ecological indicators of economic activity in the context of national security. In Emergence of Public Development: Financial and Legal Aspects: Collective Monograph. Agenda Publishing House, Coventry, United Kingdom. 2019, pp. 373-383.
214. Yemanov, V., Belay, S., & Sporyshev, K. (2022). Information-analytical method of improving the efficiency of technical intelligence of the technical support units of the National Guard of Ukraine. *Collection of Scientific Papers of the National Academy of the National Guard of Ukraine, 1*(39), 104–110. https://doi.org/10.33405/2409-7470/2022/1/39/263376
215. Yuskiv, B. M. (2009). *Globalization and labor migration in Europe*. [Monograph].
216. Zagorsky, V., Rahimov, F., Horbova, N., Zhuk, O., Pershko, L., & Mihus, I. (2023). Socio-economic aspect of territorial organization of power. *Economic Affairs, 68*(3), 1555–1564. https://doi.org/10.46852/0424-2513.3.2023.22
217. Zahorodnia, A. (2024). International organizations as a tool for the development of the world economy. *Herald of Khmelnytskyi National University. Economic Sciences*, 336(6), 567–572. https://doi.org/10.31891/2307-5740-2024-336-84
218. Zahorodnia, A. (2025). The evolution and impact of the North American Free Trade Agreement (NAFTA) on the economic development of participating countries. *Herald of Khmelnytskyi National University. Economic Sciences*, 342(3[1]), 298–305. https://doi.org/10.31891/2307-5740-2025-342-3(1)-42
219. Zahorodnia, A. S., & Sharma, M. (2024). International experience in business process management: Relations between Ukraine and the Republic of India. *Intellectualization of Logistics and Supply Chain Management*, 28, 71–77. https://doi.org/10.46783/smart-scm/2024-28-6
220. Zakharov, O. I. (2015). The mechanism of interaction between government and business in the system of economic security. *Collection of Scientific Works of Cherkasy State Technological University. Economic Sciences*, 33(3), 151.
221. Zakharov, O. I. (2016). Globalization and its impact on economic security. *Scientific Notes of the University "KROK"*, 43, 4–13.
222. Zastosuvannia hlybokoho navchannia v shtuchnomu intelekti [Applications of deep learning in artificial intelligence]. (2025). *Stfalcon Blog*. Retrieved March 21, 2025, from https://stfalcon.com/uk/blog/post/5-fascinating-applications-of-deep-learning
223. Zayats, D., Serohina, N., Bashtannyk, O., Akimova, L., Akimov, O., & Mazalov, A. (2024). Economic aspects of public administration and local government in the context of ensuring national security. *Economic Affairs, 69*(2), 979–988. https://doi.org/10.46852/0424-2513.3.2024.23
224. Zuiderwijk, A., Chen, Y.-C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38, Article 101577. https://doi.org/10.1016/j.giq.2021.101577

Public Administration 4.0: Leveraging Digital Tools for Effective Governance

Monograph

Copyright © 2025, Scientific Center of Innovative Research OÜ
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