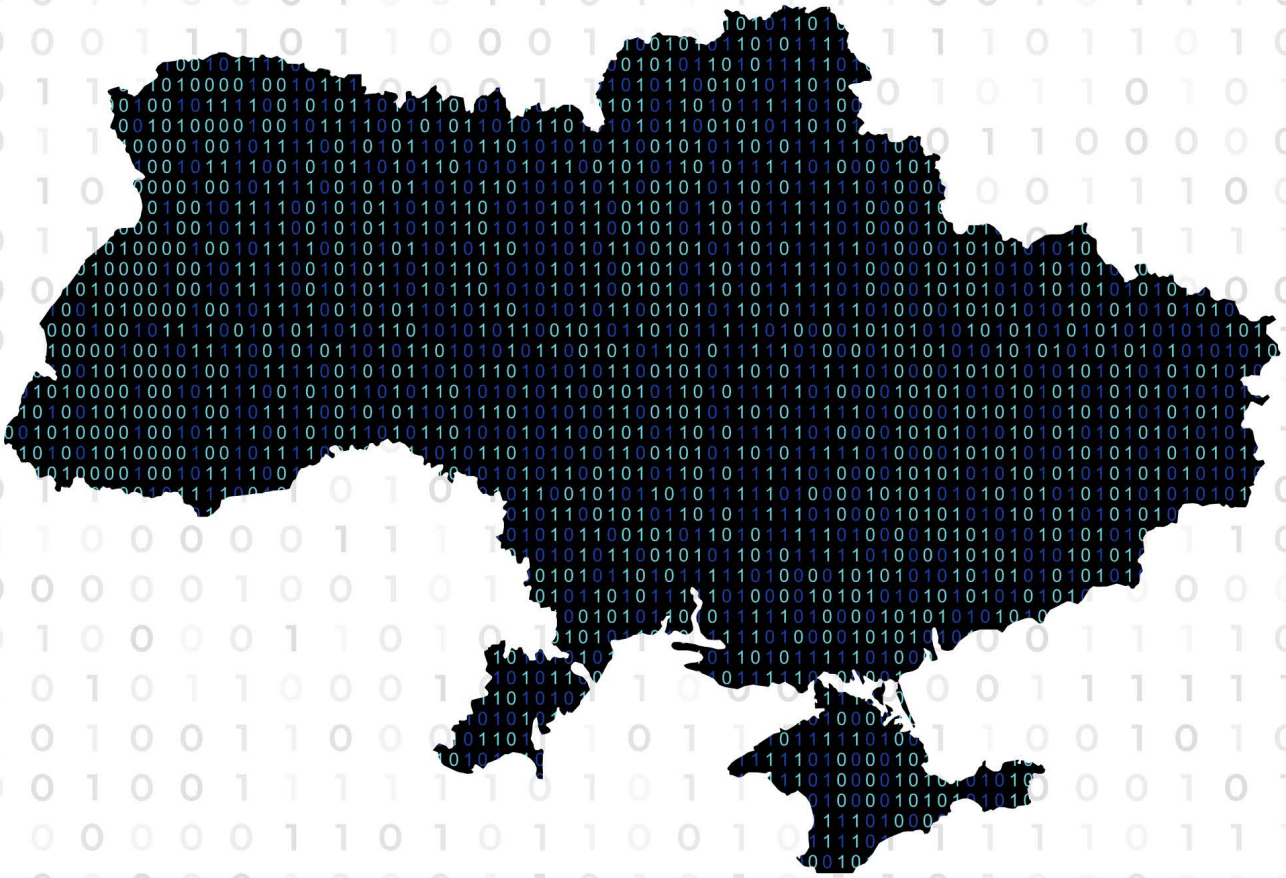
OPERATIONALISING DIGITAL SOVEREIGNTY FOR UKRAINE

Trusted Integration as the Path to Recovery, Security, and Global Digital Cooperation



ECONOMIC
SECURITY COUNCIL
of UKRAINE

aws

OPERATIONALISING DIGITAL SOVEREIGNTY FOR UKRAINE

Trusted Integration as the Path to Recovery, Security, and Global Digital Cooperation

This paper is addressed primarily to the Government of Ukraine and the Parliament (Verkhovna Rada) as decision-makers on digital governance, cloud law, and reconstruction investment. It is also intended to inform Ukraine's international partners — EU institutions, NATO allies, international financial institutions, and donor governments — and the technology sector as they engage with Ukraine's reconstruction framework. Its purpose is practical: to set out the policy choices, legal reforms, and governance mechanisms that would allow Ukraine to use domestic, European, and global digital infrastructure safely and on Ukrainian terms during reconstruction and beyond.

The paper was prepared by the Economic Security Council of Ukraine in cooperation with Amazon Web Services.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Planning regulatory policy amid an existential war is an undertaking without modern precedent. Ukraine's multi-year defence against a larger aggressor stands as one of the most remarkable acts of national will in European history — a struggle that has earned the country an unassailable moral authority to define its own future, also in the digital sphere. At the same time, that future is being secured through an unprecedented web of international partnerships: financial, military, technological, and institutional. The ambition to build genuinely sovereign digital institutions is not only legitimate but necessary. The question this paper addresses is how to achieve that ambition in ways that reinforce the international partnerships and lay the ground for a successful reconstruction.

Digital sovereignty can be defined as the capacity to use domestic, European, and global digital capabilities while retaining enforceable control over data location, data access, encryption keys, security requirements, procurement choices, resilience objectives, portability, exit options, and legal accountability. It is determined not by isolation or the location of servers, but by the ability to make a conscious choice. The path to digital sovereignty lies in rigorous technical safeguards and operational controls. Security and openness are not competing choices: openness to trusted technologies strengthens sovereignty when governed through transparent, risk-based rules.

Cloud and data infrastructure are enabling reconstruction infrastructure — without which recovery delivery, social payments, public administration, procurement, and private-sector continuity are fundamentally weakened. Public cloud, cybersecurity platforms, world-class software, AI-enabled tools, data centres, telecom networks, and service continuity systems are as essential to Ukraine's recovery as the physical rebuilding of roads, energy grids, and housing — and, like those assets, require deliberate governance from day one of reconstruction. They are also essential to sustaining Ukraine's current pace of digital innovation and supporting long-term post-war economic growth. Trusted integration means the framework through which Ukraine governs access to domestic, European, and global digital capabilities under Ukrainian law, aligned with recognised international and European standards. It is a model of governed interdependence: Ukraine retains authority over data classification, access, encryption, procurement, resilience, portability, exit rights, and legal accountability, while preserving access to trusted technologies, competitive markets, and international standards that support interoperability and investment. To help build the policy and regulatory foundation for this effort, ESCU presents the following set of recommendations.

The recommendations are:

1. Adopt trusted integration as the official policy frame for Ukraine’s digital reconstruction, recognising digital sovereignty as the capacity to govern digital interdependence under Ukrainian law and policy choices, while aligning with recognised international and European standards. This means setting clear requirements for data classification, access, encryption, procurement, resilience, portability, accountability, and provider assurance — not replacing international standards with purely domestic alternatives, and not requiring Ukraine to replicate or localise all global digital capabilities domestically.
2. Introduce a unified, risk-based data and workload classification framework linked to cloud eligibility, hosting placement, residency rules, procurement, encryption and key management, provider assurance, portability, exit, backup, and recovery requirements. The framework should be practical, based on confidentiality, integrity, and availability impact, and should avoid over-classification that increases cost, slows recovery, or pushes routine workloads into scarce high-security environments.

3. Enact durable post-martial-law rules for trusted cloud use, cross-border backup, non-classified public-sector workloads, and regulated sectors — so that arrangements made under emergency authorisation have a settled legal basis when martial law ends.
4. Modernise cloud procurement frameworks, contract templates, authorised-resale arrangements, provider-assurance criteria, and standards recognition, building on KMU Resolution №154 (as amended by Resolution №1691, December 2025) as the existing legislative foundation.
5. Treat an open, competitive, and well-governed digital market as a sovereignty instrument: competition reduces lock-in, broadens supplier choice, improves procurement value, and gives public-sector entities (including central and local government bodies, state-owned enterprises, public agencies, and other entities using public funds for digital procurement) and SMEs access to cloud, AI, cybersecurity, and developer tools that would be too costly to build domestically.
6. Ensure that public-sector procurement of digital services operates under transparent, provider-neutral Ukrainian rules based on security performance, resilience, interoperability, portability, and legal accountability with risk-based assessments applied consistently and documented, and with nationality-based restrictions limited to cases where a specific, recorded security determination supports them.
7. Require critical digital service continuity passports specifying institutional owner, dependency map, RTO/RPO targets (Recovery Time Objective and Recovery Point Objective — the maximum tolerable downtime and data-loss window respectively), backup architecture, tested failover arrangements, supplier-risk reviews, and responsible decision-makers — and embed cybersecurity baselines, resilience requirements, supplier-risk assessment, and exit-rights obligations as standard conditions in all digitally significant reconstruction investments from inception, not as retrofit requirements added after architecture decisions are made.
8. Invest in domestic digital capability through Ukrainian, European, and global partnerships: resilient connectivity, data centres where feasible, cloud academies, CISO and CDTO training, SME cloud adoption, data-governance capacity, local integrators, and GovTech startups — supported by voluntary skills-transfer frameworks, certification pathways, university partnerships, local integrator enablement, and SME participation mechanisms that build domestic capability without creating new procurement barriers.

The generation rebuilding Ukraine will expect to use modern, secure, and globally competitive technologies to create better public services, stronger education and healthcare systems, more resilient financial infrastructure, and new digital products for global markets. Digital sovereignty should give them the ability to use those technologies safely under Ukrainian law, aligned with recognised international and European standards — not prevent access to them. Trusted integration converts digital interdependence from a vulnerability into a governance asset: faster reconstruction on safe infrastructure; measurable resilience built into every critical service; data governance capacity — quality, interoperability, open data, and secure analytics — built alongside cloud governance rather than treated as a later phase; EU alignment embedded in procurement rather than retrofitted; and domestic digital capability built through contracts and partnerships rather than protected by barriers that ultimately weaken it.

2. THE POLICY PROBLEM: DIGITAL SOVEREIGNTY IS BEING MISREAD AS ISOLATION

Digital sovereignty can be interpreted in different ways. One reading emphasises physical data localisation and preference for domestic infrastructure as the primary expression of sovereign control. Another focuses on governance capacity — the ability to choose where data resides, control who can access it, set security and compliance requirements, and maintain operational continuity regardless of where infrastructure is located. Both readings reflect genuine national concerns; the question is which approach best serves Ukraine's security, resilience, and reconstruction needs given its specific circumstances.

Ukraine's wartime experience offers relevant evidence for this debate. Domestic infrastructure remains exposed to missile attacks, blackouts, cyberattacks, physical disruption, energy constraints, insurance limitations, and regional concentration risk. At the same time, distributed infrastructure, trusted cloud services, encrypted backups, cross-border recovery, and rapid failover have demonstrably strengthened state continuity and protected critical data. The lesson is not "cloud everywhere." The lesson is that trusted cloud and cross-border resilience can be made available within a governed, classification-led model — one that preserves Ukrainian control over data, workloads, and encryption while expanding the tools available for national resilience.

The second lesson is that mandatory localisation, had it remained in force during the full-scale invasion, would have resulted in the destruction or inaccessibility of critical state data housed in domestic facilities that were struck, disconnected, or rendered inoperable. The workloads that survived did so because they were distributed across trusted international cloud infrastructure. Any future legislative framework that recreates this concentration vulnerability — including a return to blanket data-localisation logic — should be assessed against this documented experience. The practical alternative is a classification-led model that preserves Ukrainian control over data and encryption while deploying infrastructure wherever it delivers the greatest resilience.

RDNA5 (covering February 2022–December 2025, published February 2026) estimates Ukraine's direct damage at USD 195.1 billion, losses at USD 666.7 billion, and recovery and reconstruction needs at USD 587.7 billion over 2026–2035. Within this, the telecom, digital and media sector is assessed at USD 2.5 billion in damage, USD 2.7 billion in losses, and USD 7.1 billion in needs [1]. These figures confirm that digital and telecom resilience is part of Ukraine's reconstruction baseline, not an optional modernisation layer.

Openness delivers the greatest value when paired with clear governance rules. Reliance on any single provider — or on ungoverned procurement arrangements — without clear Ukrainian rules may create concentration, weak accountability, and difficult exit conditions. These risks can be addressed through interoperability, open standards where appropriate, data and model exportability, documented exit plans, migration testing for critical workloads, and procurement rules that preserve customer choice. The objective is not to eliminate all switching costs — which exist in any technology transition — but to prevent artificial technical, contractual, or procedural barriers that make it impractical. Trusted integration therefore means governed interdependence: Ukraine retains control over its data, its access policies, and its ability to move workloads between trusted environments. Sovereignty can be judged by whether Ukraine controls access, classifies data and workloads, manages encryption keys, defines procurement and assurance requirements, understands provider and subprocessor dependencies, verifies compliance through recognised assurance evidence, ensures portability, activates recovery, and maintains critical services under stress.

Cloud risk is usefully understood through the shared responsibility model — a framework in which providers are responsible for security of the cloud (the underlying infrastructure, facilities, hardware, core services, and global operational security) while public-sector entities remain responsible for security in the cloud (classification, access management, configuration, encryption choices, key management, monitoring, lawful use of data, and incident response for their workloads). The responsibility balance differs across service models. A public-sector entity using IaaS (Infrastructure as a Service) retains more direct responsibility for operating systems, applications, and configuration; PaaS (Platform as a Service) shifts more platform responsibility to the provider; SaaS (Software as a Service) shifts more operational responsibility to the provider but still requires the customer to manage identity, access, data governance, retention, and lawful use. Cloud policy can therefore require public-sector entities to understand the service model they are procuring and to document the corresponding security responsibilities — ensuring that sovereignty is operationalised at every layer, not assumed by default.

An open and competitive digital market strengthens sovereignty when it is governed well. Competition reduces lock-in, broadens supplier choice, improves procurement value, supports innovation, encourages investment, and gives Ukrainian SMEs access to cloud, cybersecurity, AI, and digital tools that would otherwise be too expensive to build alone. Some cloud providers now offer sovereign-cloud models — including dedicated sovereign regions operated under local legal frameworks — which could be assessed against Ukrainian legal and technical criteria before procurement. Where such models meet the classification and assurance requirements of the relevant tier, they can serve as a mechanism for combining cloud-scale capability with enhanced jurisdictional control. In a trusted-integration model, openness becomes a sovereignty instrument when combined with security baselines, supplier-risk management, interoperability, exit rights, and Ukrainian legal control.

A classification-led model also helps move beyond binary localisation debates. It allows Ukraine to reserve specialised national or security-authorised environments for genuinely high-risk workloads while enabling lower-risk public-sector systems to use trusted domestic, European, or global cloud where this improves resilience, security, cost, innovation, and service continuity. This is consistent with comparative practice: the UK permits public cloud for official data [2], Finland permits public cloud through lower security classes with encryption and risk decisions [3], Italy permits qualified public cloud for ordinary and critical data while reserving strategic data for nationally controlled infrastructure [11], and Singapore uses a government cloud-access platform to mediate agency use of commercial cloud [5]. By adopting a classification-led approach, Ukraine can chart a pragmatic middle path, safeguarding sovereignty where it matters most while harnessing the full benefits of cloud innovation where the risk profile permits.

Policy implications

A well-designed digital governance framework for Ukraine's reconstruction would:

- classify data and workloads by risk, mapping each tier to permitted hosting environments, encryption and key-management requirements, provider assurance standards, recovery objectives, portability obligations, and exit conditions — replacing blanket localisation rules with architecture chAoices governed by confidentiality, integrity, availability, and mission impact;

- permit trusted cloud[1] and cross-border storage where this approach demonstrably improves resilience, cyber protection, and service continuity, subject to Ukrainian legal control over classification, access, encryption keys, audit logs, and recovery activation;
- treat encryption, key governance, auditability, portability, and exit rights as operational sovereignty instruments, not as contractual add-ons — requiring supplier-risk assessments, tested recovery procedures, and documented exit plans for all critical public-sector workloads;
- reserve specialized national or security-authorized environments for secret, top-secret, defense, intelligence, and other highly sensitive workloads, with placement decisions driven by impact assessment, mission criticality, resilience requirements, and available certified controls rather than by default classification.

[1] For the purposes of this paper, 'trusted' applied to cloud providers, jurisdictions, or integration arrangements refers to providers that meet defined security, resilience, supply-chain, and legal accountability criteria.

3. CLOUD AND DATA INFRASTRUCTURE OPTIONS FOR RECONSTRUCTION

A classification-led cloud and data infrastructure model — matching each dataset, workload, and public function to the appropriate environment based on classification tier, confidentiality, integrity, availability, mission criticality, resilience needs, trusted jurisdiction, and implementation feasibility — provides the most coherent framework for Ukraine's reconstruction choices.[2] Public and routine official workloads may be eligible for trusted public cloud; restricted or high-impact workloads may require qualified cloud (cloud infrastructure certified against defined national or international security standards, such as BSI C5 or EUCS) or hybrid cloud with stronger encryption and recovery controls; the most sensitive classified workloads require specialised national, allied, or security-authorised environments.

Trusted global cloud capacity should remain a central component of Ukraine's broader, classification-led recovery model. It provides scale, cybersecurity capabilities, geographic redundancy, disaster recovery, AI infrastructure, and operational resilience that would be costly and difficult to replicate domestically at comparable scale in the short or medium term. Cloud should not be understood only as compute and storage: modern cloud services include managed databases, cybersecurity tooling, identity services, AI and machine-learning platforms, developer tools, SaaS applications, and backup and recovery. This matters because it can shorten implementation time, reduce upfront capital expenditure, improve security baselines, and give public institutions and SMEs access to capabilities that would be costly or impractical to build locally. The policy question is not only where servers are located but which services Ukraine can safely use to accelerate secure reconstruction.

Cloud and hosting providers may offer different deployment models — including public cloud, qualified cloud, dedicated environments, local zones, on-premises solutions, and jurisdictionally constrained sovereign-cloud arrangements — demonstrating that sovereignty controls and cloud capability are not mutually exclusive. Ukraine's procurement criteria should require trusted providers to demonstrate an equivalent tier structure matched to the classification framework. For high-assurance public-sector workloads, providers should demonstrate that their proposed deployment model and controls meet the requirements of the relevant classification tier. Providers should demonstrate the ability to implement technical controls — including encryption, key management, and access boundary enforcement — that correspond to each classification tier they wish to serve, rather than being required to offer identical infrastructure topology across all tiers.

Domestic infrastructure investment should follow evidence, not precondition. Localisation rules that require providers to build in-country infrastructure as a condition of market access do not automatically lead to infrastructure investments: providers assess addressable demand, energy and grid reliability, physical security, insurance conditions, and regulatory predictability. Where these conditions are favourable, domestic data centres, cloud regions, and local zones can support investment, jobs, latency-sensitive workloads, and ecosystem development — and should be welcomed on that basis. Where conditions are not yet favourable, they are not automatically more sovereign or more resilient than trusted external environments. Ukraine should create predictable, provider-neutral rules permitting secure use of existing trusted regions — including EU regions and

[2] The classification framework is risk-based in methodology — each tier is defined by the confidentiality, integrity, and availability impact of the data or workload — and classification-led in governance: the tier assigned to a workload determines which infrastructure, controls, and procurement rules apply.

sovereign-cloud offerings — while conditions for domestic investment are developed rather than mandated.

Trusted cross-border storage and continuity arrangements can meaningfully strengthen resilience for selected critical backups and recovery functions, particularly while domestic infrastructure remains exposed to kinetic threats, power disruption, and regional instability. The Data Embassy concept reflects an ambition to extend sovereign control beyond national borders, and its further development would benefit from rigorous feasibility assessment against operational benchmarks: application recovery capability, real-time or near-real-time replication, tested failover procedures, RTO/RPO performance, cyber controls, operational staffing, cost sustainability, and clear legal treatment in the host jurisdiction. Where a Data Embassy arrangement meets these benchmarks, it can serve as a continuity option for defined use cases. Where these conditions prove difficult to satisfy at the required scale, trusted distributed cloud backup — offering geographic redundancy, tested recovery, and contractual sovereignty safeguards — may deliver stronger and more flexible resilience for a broader range of critical systems. A framework that accommodates both options, matched to the specific resilience requirements of each system, would position Ukraine to draw on the full range of available tools.

Hybrid, dedicated, or sovereign-cloud arrangements should be considered only where the classification framework and workload impact assessment demonstrate that additional controls are genuinely necessary. The designation "national security" should not justify higher-cost models without a documented classification and risk assessment on record. Over-classification itself is a security risk: budget spent on unnecessarily complex hosting for low-risk workloads is budget unavailable for protecting genuinely sensitive systems. The classification framework should therefore be accompanied by clear worked guidance and periodic review to prevent defensive over-classification becoming the default.

The options below constitute an eligibility framework, not a ranked preference list. Classification and workload-impact assessment determine which model applies. Public cloud, domestic data centres, hybrid cloud, cross-border backup, Data Embassy options, and specialised national environments are tools for different risk categories — not substitutes for one another.

Cloud and data infrastructure portfolio

The six options below are tools for different risk categories. Classification and workload-impact assessment determine which applies; none is a default preference, and none substitutes for the others.

OPTION	STRATEGIC VALUE	MAIN RISKS	POLICY RESPONSE
Trusted global public cloud	Scale, rapid deployment, cybersecurity capabilities, geographic redundancy, AI and analytics, disaster recovery, and advanced services	Jurisdictional exposure, provider concentration, switching costs, and weak exit planning if ungoverned	Classification framework; encryption and key governance; interoperability and exportability; assurance evidence; portability; exit planning; trusted-jurisdiction rules
Domestic data centers / cloud regions / local zones	Investment, jobs, latency reduction, domestic capability, ecosystem development	Physical attack, energy instability, insurance costs, uncertain demand	Evidence-based feasibility assessment; secure locations; backup power; demand aggregation; PPPs; Ukrainian-European-global partnerships

Hybrid or sovereign cloud[3]	Combines global technology capacity with stronger national operational control	Cost, complexity, implementation capacity	Reference architecture; workload classification criteria; operating model design; public-sector skills development
Trusted cross-border storage	Resilience against physical destruction, blackouts, and regional concentration risk	Legal and jurisdictional uncertainty	Trusted-jurisdiction criteria; contractual safeguards; EU and NATO partner arrangements; Ukrainian key control
Data Embassy	High-assurance continuity for selected critical data or functions under intergovernmental agreement	Requires alignment across legal, diplomatic, technical, and operational dimensions; effectiveness depends on meeting stringent recovery and resilience benchmarks	Pursue as a targeted continuity option for defined use cases where intergovernmental agreement and full feasibility validation confirm operational viability; complement with distributed cloud resilience for broader coverage
Specialized national environments	Highest control for defense, secret, and top-secret workloads	Cost, scalability, skills, resilience under sustained attack	Reserve strictly for documented high-sensitivity categories; not the default for unlabelled workloads

Calibrating the classification model

The risk of over-classification is as real as the risk of under-classification. Over-classifying routine public-sector systems raises costs, restricts access to modern cloud and AI tools, slows migration, limits competition, and congests high-assurance environments that must be kept available for genuinely sensitive or mission-critical workloads. Under-classifying exposes sensitive systems to insufficient controls. The classification framework should therefore be supported by clear guidance with worked examples, reviewed periodically as the threat and technology landscape evolves, and anchored by documented management-level risk decisions that record the owner, the justification, and the residual risks accepted.

Working classification tiers and cloud eligibility

PROPOSED TIER	CLOUD ELIGIBILITY	MINIMUM SAFEGUARDS
Public / Open	Trusted public cloud permitted	Basic security baseline, logging, availability controls
Official / Internal	Trusted public cloud permitted, including multi-region or cross-border where lawful	Access control, encryption at rest and in transit, incident notification, provider assurance evidence
Restricted / Official-sensitive	Trusted public cloud, qualified cloud, hybrid cloud, or domestic/cloud mix subject to impact assessment	Strong encryption, key governance, RTO/RPO targets, tested backup, portability requirements, subprocessor transparency
Critical / High-impact	Qualified cloud, hybrid or sovereign cloud, trusted cross-border replication, or controlled domestic environment	Enhanced assurance, documented risk decision, continuity passport, supplier-risk review, exit testing
Classified / National-security restricted	Specialized national, allied, community, or security-authorized environments only	National security authorization, approved cryptography, personnel controls, bespoke recovery and audit regime

[3] 'Sovereign cloud' in this context refers to cloud deployments operated under contractual and technical controls that confine data processing and operations to a defined jurisdiction — including commercially available sovereign-cloud products offered by major providers and nationally operated government cloud environments.

AI as part of the cloud and data governance agenda

As AI services are typically deployed on the same underlying infrastructure as other cloud workloads, the security, resilience, and data-handling risks are the same. AI should therefore be governed within the same classification and procurement framework as other cloud services — not treated as a separate category addressed after infrastructure decisions are made. Advanced public-sector analytics, cyber-defense tooling, fraud detection, service personalization, and semi-automated administrative functions will require scalable infrastructure, strong data governance, secure access controls, auditability, and clear lines of accountability. These requirements map directly onto the classification tiers above: the sensitivity of the data processed, the rights implications of the output, and the mission criticality of the function determine the appropriate hosting environment and assurance level.

Ukraine should build domestic AI capability — through universities, startups, Diia.City (Ukraine's special economic regime for IT and technology companies) companies, and public-sector delivery teams — directing investment toward the layers of the AI value chain where Ukrainian strengths translate most directly into competitiveness. The highest-value opportunity lies not in replicating AI infrastructure or foundation models — efforts that require years of capital-intensive development even for larger economies — but in combining Ukrainian talent, distinctive public-sector use cases, and local integrators with trusted access to global AI and cloud capabilities, governed under Ukrainian law, aligned with recognised international and European standards. This is not a concession of sovereignty; it is how every comparable country with a strong domestic technology sector operates.

AI-enabled public services should embed core dimensions of responsible AI: human oversight wherever the output affects individual rights, entitlements, or enforcement decisions; data protection and purpose-limitation controls matched to the classification of the underlying data; explainability mechanisms proportionate to the stakes of the decision; and clear attribution of public-sector responsibility that cannot be delegated to a model or a provider. These requirements reflect internationally recognised responsible AI principles covering fairness, privacy and security, safety, controllability, robustness, governance, and transparency.

4. LEGISLATIVE AND REGULATORY BARRIERS TO TRUSTED GLOBAL INTEGRATION

Under martial law, Ukrainian public-sector entities have been permitted to migrate data and services to international cloud platforms, activate cross-border backups, and use trusted foreign infrastructure under expedited arrangements that do not require the full legal basis that peacetime rules demand. When martial law ends, that emergency cover lapses — though the timing and legal consequences will vary by data category, institution type, and applicable transitional provisions. Institutions will need settled Ukrainian law to continue existing cloud arrangements, enter new agreements, and maintain cross-border continuity without legal risk; the precise urgency and sequencing will depend on which legal categories and transitional rules apply to each body's specific arrangements. The reforms in this section are therefore not optional modernisation — they are the legal foundation that makes wartime digital resilience durable.

The challenge is not the absence of rules but the need to modernise them so that they support security, resilience, competition, and trusted international cooperation simultaneously. The central bottleneck is the absence of a unified classification-to-cloud eligibility model. Without it, public-sector entities cannot consistently decide which workloads may use trusted public cloud, which require qualified or hybrid environments, which may be replicated abroad for continuity, and which must remain in specialised national or security-authorised environments. Classification should become the legal bridge connecting cloud law, public registers, information protection, cybersecurity, procurement, personal data protection, and critical-infrastructure regulation — replacing the current patchwork of sector-specific rules with a single consistently applied framework. Legislative modernisation should mean better regulation, not deregulation: for sensitive workloads, the question should not be territorial location alone, but whether the chosen architecture provides lawful control, cyber protection, physical survivability, tested recovery, acceptable RTO/RPO targets, and resilience against regional disruption.

Key reform areas

BARRIER	WHY IT MATTERS	REFORM DIRECTION
No classification-to-cloud eligibility model	Public-sector entities cannot consistently decide where data may be hosted, what safeguards apply, or when cloud, hybrid, domestic, cross-border, or specialized environments are allowed	Adopt a unified classification framework that maps each tier to cloud eligibility, residency/trusted-jurisdiction rules, encryption/key management, assurance evidence, RTO/RPO, portability, exit, and audit requirements
Post-martial-law cloud uncertainty	May force inefficient repatriation of suitable workloads or discourage trusted cloud use	Clarify durable rules for trusted cloud, backup, and cross-border continuity
Blanket localisation logic	Can reduce resilience by concentrating infrastructure in physically vulnerable locations	Replace blanket localisation with differentiated localisation based on sensitivity and criticality
Procurement rigidity	Limits access to consumption-based cloud, SaaS, cyber tools, and multi-year services	Create cloud-friendly procurement frameworks, catalogues, and lifecycle-value criteria
Contracting uncertainty	Makes cooperation with global providers difficult or legally risky	Develop model cloud contractual clauses on data ownership, location, security, incident notification, auditability, portability, and exit — designed as baseline templates that can be adapted to different service models (IaaS, PaaS, SaaS), provider size, and workload classification tier, rather than as uniform mandatory terms that would be incompatible with global cloud provider standard agreements.

Weak portability and exit rights	Increases lock-in and reduces strategic control	Mandate exit plans, migration support, portable formats, and periodic exit testing
Supplier-risk gaps	Leaves hidden dependencies unmanaged	Establish supplier-risk, subprocessor disclosure, and trusted provider principles
Personal data reform gap	Weakens EU trust and cross-border data governance	Align with GDPR and Convention 108+[4] logic, including adequacy-pathway preparation; accompany alignment with domestic impact assessments for Ukrainian IT companies, SMEs, and startups, and provide transition guidance so that compliance costs do not disproportionately burden the domestic digital economy. Alignment should be phased to reflect implementation capacity
Limited standards recognition	Creates duplication and uncertainty	Recognize suitable international and EU-compatible standards where appropriate
Sector-specific restrictions	May block secure cloud adoption in regulated sectors	Apply sector-specific but risk-based rules

Building on the existing foundation

KMU Resolution №154 of 11 February 2025, as amended by Resolution №1691 of 17 December 2025, establishes public-sector cloud and data-centre rules covering: (i) provider eligibility requirements based on ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 certification (points 6–7 of the amended Requirements); (ii) a cross-reference to Article 8 of the Cloud Law, which requires incident management, business continuity, monitoring, and compliance with international standards (point 3); (iii) confirmation and registration procedures for the CSPs Register maintained by SSSCIP (points 8–11); and (iv) a model contract template. Effective enforcement requires a designated authority — building on SSSCIP's existing mandate — with the power to audit classification decisions, require corrective action where workloads are misclassified, and publish periodic compliance reports. The classification framework is an accountability mechanism only if adherence to it can be verified.

The main challenge is that Resolution №154 is a secondary regulation linked to the pre-full-scale-invasion Cloud Law (No. 2075-IX, adopted 3 February 2022 — one week before the full-scale invasion). The Cloud Law may require substantive amendment because some registration and compliance requirements appear difficult to reconcile with international cloud operating models. Amendment of Resolution №154 alone may not resolve blockers embedded at the statutory level.

Shared responsibility and provider operating conditions

Cloud governance must be grounded in the shared responsibility model. Providers are responsible for security of the cloud — infrastructure, facilities, hardware, and core platform services. Customers, including public-sector entities remain responsible for security in the cloud — classification, identity and access management, configuration, encryption, key management, monitoring, and incident response. This division shifts by service model: IaaS leaves more operational responsibility with the institution; PaaS and SaaS transfer more platform responsibility to the provider while the institution retains accountability for data governance, access, retention, and lawful use. Public-sector entities should be required to document the service model they are procuring and the corresponding security responsibilities before a contract is signed.

[4] Convention 108+ refers to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (modernised 2018). Ukraine ratified the original Convention in 2010 and signed the modernising Protocol in 2018. Compliance with Convention 108+ supports the pathway toward an EU adequacy decision under Article 45 GDPR.

For international providers and their Ukrainian customers, legal predictability is key. Reform should clarify the authorised-provider and resale model, the role of local partners, applicable governing law and dispute resolution, procurement methodology, pricing structures that recognise cloud computing's consumption-based (pay-as-you-go) delivery model — where customers pay only for resources actually used at publicly published rates — rather than requiring fixed contractual prices incompatible with elastic, on-demand service provisioning, and the rationale for SBU-related security-check requirements, which should be reviewed and, where duplicative of recognised international assurance evidence, narrowed or replaced — where providers can demonstrate independently audited ISO/IEC 27001, 27017, and 27018 compliance, sanctions-screening controls, and other recognised assurance evidence. For workloads involving state secrets, defence, or intelligence functions, national-security review obligations should be defined by law rather than left to case-by-case administrative discretion.

As part of the EU integration process, Ukraine will align with EU frameworks covering data governance, cybersecurity, telecommunications, cloud services, interoperability, and procurement. This alignment can support the adequacy pathway for personal data flows and embed internationally recognised security standards into Ukraine's regulatory framework. It also underscores the need for a supportive and harmonised regulatory framework for emerging technologies. The objective is to ensure that EU law transposition in Ukraine becomes a source of competitive strength and ecosystem resilience. Implementation should be sequenced to reflect Ukraine's current capacity and reconstruction priorities, with transition support and domestic impact assessments accompanying each major alignment step — so that compliance requirements do not disproportionately burden smaller domestic firms and public-sector entities.

The business and technology sector can support this alignment process through skills transfer, co-development of compliance tools, participation in stakeholder consultations, and investment in the domestic institutional capacity — including training for regulatory and procurement staff — that makes implementation feasible rather than nominal. Ukrainian firms, integrators, and SMEs should be active participants in the alignment process, not passive recipients of new compliance obligations.

Democratic accountability and rights-based safeguards

As Ukraine builds its digital reconstruction framework, democratic and rights-based safeguards should be embedded from the start. Trusted integration should strengthen public trust by ensuring that cloud, data, and AI systems are governed through lawful access rules, transparent risk management, data protection, security assurance, and accountable public-sector decision-making. This framing is constructive rather than corrective: it does not assume that existing Ukrainian systems lack safeguards, but recognises that permanent reconstruction frameworks should make those safeguards explicit, auditable, and scalable.

Trust in digital providers should be assessed through a holistic, provider-neutral framework that considers transparent corporate governance, secure development practices, independent assessments, supply-chain and security oversight, operational transparency, respect for the rule of law and data protection, and compliance with relevant international standards such as ISO/IEC 27001. Public-sector accountability should be addressed through lawful-access rules, role-based access control, audit logs, privacy and data-protection impact assessments for high-impact systems, independent security review for systems affecting rights or entitlements, human oversight wherever AI-assisted decisions affect individuals, aggregated transparency reporting that does not expose sensitive technical details, and civil-society consultation for significant new data-processing programmes.

5. RESILIENT BY RECONSTRUCTION

Ukraine's reconstruction represents a generational opportunity to build digital infrastructure that is resilient by design. New projects and infrastructure investments can embed redundancy, geographic distribution, cyber resilience, service continuity, data portability, and accountable recovery from the outset. This can be achieved through complementary tracks — cloud-based digital services built to classification-framework standards from day one; trusted cross-border continuity arrangements with NATO and EU allies for mission-critical workloads; and domestic data centre capacity where economically and operationally viable. The goal is not to choose one track over another — it is to apply consistent continuity, security, and governance standards across all of them, giving Ukraine the flexibility to place workloads where they deliver the greatest resilience and value.

Ukraine's own experience illustrates the risk: data centre concentrations in Kyiv and major eastern cities proved vulnerable to missile strikes and power disruptions in 2022, while workloads distributed across trusted cloud infrastructure maintained continuity. The lesson is not that physical infrastructure is unnecessary, but that concentration — whether domestic or in a single cloud provider — is a vulnerability that governance rules should specifically address. Such wartime measures as blanket localisation, mandatory centralised backup, underground-only data centres, and mandatory double reservation are designed to protect critical data and services under conditions of active military threat and reflect Ukraine's hard-won operational experience. At the same time, permanently codifying emergency measures into peacetime governance involves trade-offs that merit careful consideration. Concentrating data in a limited number of physical locations can itself become a vulnerability; prescriptive infrastructure mandates may inflate costs and limit access to resilient distributed architectures; and applying the highest-assurance requirements uniformly can congest secure environments with workloads that do not require that level of protection. Equally, relaxing these measures too quickly — or without adequate alternatives in place — could expose critical systems during a period of ongoing threat. The challenge is therefore one of calibration: distinguishing between measures justified by the immediate threat environment and durable governance rules suited to the evolving risk landscape. Resilience in the longer term is typically strengthened through geographic and provider diversity, tested failover, clear exit options, and the institutional capacity to migrate between trusted environments — approaches that complement, rather than replace, the protective instincts behind the original emergency measures.

The data localisation trends must be evaluated against this operational history. Provisions that would require repatriation of workloads currently distributed across trusted international infrastructure — or that would prevent future cross-border continuity arrangements for non-classified data — would recreate precisely the concentration vulnerability that emergency legislation was passed to escape in February 2022. The question is not whether Ukraine should maintain protective measures for its most sensitive systems — it should, and this paper's classification framework supports that objective. The question is whether blanket localisation requirements should be applied to workloads that do not require that level of protection, thereby reducing resilience, inflating costs, congesting high-assurance environments, and foreclosing the cloud-based continuity arrangements that preserved state functions during the most intense period of the war.

Digital resilience should be assessed across the full service chain, not only at the cloud or data-centre layer. A public digital service remains operational only if users can access it, telecom networks function, energy backup is available, identity and authentication systems work, registers and APIs remain reachable, cloud or data-centre workloads can be recovered, cybersecurity teams can detect and contain incidents, and suppliers can provide support under disruption. Continuity passports should therefore map dependencies across access networks, transport and core connectivity, cloud and hosting environments, applications, registers, identity services, suppliers, power backup, and

recovery procedures. RTO/RPO targets should be validated through practical failover exercises, not declared as planning assumptions. Telecom resilience — including physical infrastructure hardening, backup power, satellite fallback where applicable, and operator redundancy — is a precondition for cloud-based service continuity and should be addressed as part of the same governance framework.

6. DOMESTIC CAPABILITY, SMES, AND AN OPEN DIGITAL MARKET

Ukraine's domestic digital sector is not a future aspiration — it is a substantial present reality that the governance model must be designed to strengthen.

Domestic digital capability is not an aspiration — it is an already-substantial economic reality. According to Ministry of Digital Transformation data, Diia.City residents paid UAH 34.6bn in taxes in 2025. In March 2026, the Diia.City special economic regime had more than 4,000 resident companies and around 148,000 IT specialists [6]. Ukraine is classified in Group A — Extensive GovTech Maturity — in the World Bank GovTech Maturity Index 2025 [7]. At the same time, the GTMI identifies Digital Citizen Engagement as the weakest component worldwide — average score 0.474 against 0.657 for public service delivery — with open data portals declining in nineteen percent of economies, disproportionately in conflict-affected countries. This gap is directly relevant to reconstruction: trusted integration must strengthen the citizen-facing and transparency layer of digital government, not only backend infrastructure. Ukraine's CNAPs network — the primary offline public service delivery channel reaching citizens across every region — illustrates why connectivity, digital capability, and citizen-facing services must be governed as a single system rather than separate programmes. Inclusive access should be a design criterion for digital reconstruction: services built on cloud infrastructure must remain accessible through offline channels (CNAPs, mobile service points) and must be designed for the full population — including conflict-displaced citizens, communities with limited connectivity, and users requiring accessible design — not only for urban, digitally literate users. Ukrainian IT firms, SaaS providers, cloud integrators, cybersecurity providers, GovTech teams, universities, and SMEs are the sovereign digital capability this governance model exists to strengthen. They should participate as primary delivery partners, not symbolic subcontractors. This is an employment, tax-revenue, skills, investment, and economic-resilience issue as much as a technology one.

The strongest driver of domestic digital capability is a well-governed market with transparent rules, open procurement, and equal conditions for firms of all sizes — not protectionist barriers that limit competition or create administrative burdens. When procurement frameworks are designed for openness and performance-based competition, international technology capacity and local enterprise grow in tandem: domestic firms gain access to global partnerships, skills, and tools, while international providers gain the stable regulatory environment they need to invest and deliver at scale. Open procurement builds domestic capability because it creates genuine competitive pressure — requiring local firms to meet international security and performance standards, gain exposure to global technology stacks, and develop the skills that come from delivery responsibility rather than subcontracting. Protectionist barriers, by contrast, insulate domestic firms from the competitive environment that produces those capabilities.

Where appropriate and proportionate to contract scale, digital reconstruction procurement should create conditions under which Ukrainian cloud integrators, cybersecurity providers, system integrators, startups, and SMEs can compete and grow without restricting access to international technology. This should be achieved through open, transparent, and outcome-based procurement; accessible framework agreements; proportionate assurance requirements; certification support; skills-transfer partnerships; and voluntary cooperation between international providers and Ukrainian firms. The objective is not to impose local-content requirements, but to build a market structure in which international technology capacity is available under Ukrainian law and recognised international standards, while Ukrainian firms progressively build the capability to deliver an expanding range of digital services.

The most durable outcome of digital reconstruction is one in which international technology capacity and domestic delivery capability grow together. Reconstruction engagements offer a unique opportunity to embed this mutual progression by design — through defined roles for Ukrainian cloud integrators, cybersecurity providers, and system integrators; skills-transfer and certification partnerships; local talent development as a measurable deliverable; and transparent SME participation pathways. The objective for Ukraine is a comparable market environment in which international technology operates within Ukraine's regulatory framework, and in which Ukrainian firms progressively move from supporting roles to primary delivery responsibility as capability matures — an outcome that serves the interests of both domestic industry and international partners committed to long-term presence.

What international technology partnerships can deliver

International technology companies bring significant value to Ukraine's digital reconstruction when cooperation is structured around concrete capability-transfer outcomes. Voluntary partnership frameworks — built on mutual benefit rather than prescriptive obligations — have proven effective in comparable contexts and can unlock a range of high-impact contributions. These include: cloud and cybersecurity academies co-developed with Ukrainian universities, building a pipeline of skilled professionals; certification vouchers and training pathways that accelerate readiness among public servants, CDTO and CISO teams, and SMEs; local integrator enablement programmes that progressively build domestic delivery capacity; startup credits, technical mentorship, and incubator access that strengthen Ukraine's GovTech and cybersecurity ecosystem; secure migration support that helps public-sector entities modernise legacy systems faster and more cost-effectively than they could alone; cyber-range exercises that build institutional response capacity through shared expertise; and joint research programmes with Ukrainian universities on AI governance, cloud security, data infrastructure, and digital public services. A cooperative approach that actively engages the domestic SME ecosystem is particularly valuable: it broadens the economic benefits of digital reconstruction beyond Ukraine's largest firms, strengthens the employment and innovation base, and ensures that reconstruction delivers durable, locally-rooted growth.

The precedent is already established

Ukraine has already demonstrated what trusted integration at scale looks like under the most demanding conditions. Following the February 2022 invasion, government ministries migrated critical registers and services to AWS, Microsoft Azure, and Google Cloud within weeks, preserving continuity of pension payments, civil registry access, and core administrative functions. That was not a concession of sovereignty — it was sovereignty in practice: the state retained control over classification, access, and legal accountability while using trusted global infrastructure to remain functional under sustained attack.

The next phase is to transition what was proven under emergency conditions into a durable institutional framework — transparent, predictable, and technology-neutral Ukrainian rules that enable domestic firms, international partners, and public-sector entities alike to invest, plan, and deliver with confidence. The legal and regulatory environment should reward capability and performance, not origin — giving Ukraine the stable foundation it needs to attract sustained investment while building long-term domestic capacity.

7. COMPARATIVE LESSONS: PRACTICAL MECHANISMS FROM PEER COUNTRIES

Comparative experience is useful when it yields transferable mechanisms, not when it produces pressure to copy country models wholesale. The central lesson from every mature digital governance framework is the same: no government with a functioning digital economy makes a binary choice between localisation and cloud. They classify data and workloads, define eligibility by sensitivity, escalate controls proportionately, and reserve nationally controlled environments for a narrowly defined set of genuinely high-risk categories. The variation across countries is in how they implement this logic — the certification machinery, the procurement vehicle, the residency rules, the central authority — not in the underlying principle.

Reference cases and transferable mechanisms

REFERENCE CASE	TRANSFERABLE MECHANISM	RELEVANCE FOR UKRAINE
Estonia	Interoperability architecture and Data Embassy logic	Continuity and interoperability can be combined without centralizing all data in one system
United Kingdom	Cloud procurement, G-Cloud-style frameworks, supplier-risk management	Useful for cloud catalogues, framework agreements, and trusted supplier rules
Singapore	Whole-of-government digital strategy and trusted data governance	Shows the value of combining strategic direction with implementation capacity
Finland / Lithuania	Security of supply, cyber governance, preparedness	Relevant for resilience planning in integrated European systems
Poland	Scaled citizen-facing digital services and EU-aligned public digital government	Relevant for regional digital public-service modernization
Taiwan	Continuity planning under persistent geopolitical and cyber pressure	Relevant for resilience under long-term coercive conditions
Italy	Public-sector cloud classification, trusted cloud, risk-based assurance	Useful for workload classification, trusted environments, and cloud assurance

Four jurisdictions in depth: data residency and certification

Four jurisdictions — the United Kingdom, Finland, Italy, and Singapore — are examined in greater detail because they offer the most directly transferable mechanisms and together span the full range of residency positions that may be relevant for Ukraine's policy design.

The four jurisdictions take markedly different positions on data residency. The UK imposes no location-based restrictions for *official data*, explicitly permitting multi-region and overseas cloud deployment. Finland prefers EU/EEA-based solutions but does not impose an absolute mandate, requiring valid GDPR transfer mechanisms for *personal data*. Italy mandates national infrastructure for *strategic data* through the PSN, while permitting ACN-qualified cloud for lower tiers. Singapore does not impose explicit offshore prohibitions for cloud-eligible data but ensures government control through the GCC operating on major cloud provider regions [5].

The practical implication for Ukraine is that a defensible residency policy does not require a single answer for all data — it requires a tiered answer that matches residency requirements to classification level, as all four jurisdictions do in different ways.

Certification and provider listing frameworks

COUNTRY	PRIMARY ASSESSMENT FRAMEWORK	KEY CERTIFICATIONS REQUIRED	CLOUD PROVIDER LISTING MECHANISM
United Kingdom	14 UK Cloud Security Principles [2]	Cyber Essentials Plus ; G-Cloud self-certification [16]	Digital Marketplace (G-Cloud)
Finland	PiTuKri (52 criteria); Katakri 2020 [9, 3]	ISO 27001; Traficom NCSC-FI approval [10]	Risk-based management decision
Italy	ACN Qualification (QC1–QC3) [11]	ISO 9001, ISO 27001 (with 27017/27018), CSA STAR Level 2 [12]	ACN Qualified Cloud Catalogue
Singapore	IM8 Policy Framework [13]	MTCS SS584:2020 Level 3 (Tier 1/2/3); ISO 27001 [14]	GCC Platform (AWS, Azure, GCP) [15]

What the four frameworks have in common — and what Ukraine could take from them

Despite their structural differences, all four frameworks share four properties. First, controls escalate proportionately with data sensitivity: lower tiers permit commercial public cloud; upper tiers require controlled or nationally authorised environments. Second, each designates a central technical authority responsible for security assessment, certification, and framework governance — the NCSC, Traficom, ACN, and GovTech Agency respectively — providing a single point of accountability that prevents fragmentation across ministries. Third, each framework has become progressively more cloud-permissive over time, not less, as experience has demonstrated that cloud adoption improves resilience, operational efficiency, and security baselines when governed properly. Fourth, none of them treats international certification — ISO 27001, CSA STAR, SOC 2, BSI C5 — as a substitute for government-defined risk requirements, but all of them accept international certification as primary evidence rather than requiring duplicative local assessments.

These examples do not eliminate sovereignty concerns — each country retains nationality-based restrictions, national-security controls, and sector-specific rules that reflect its own threat environment and legal tradition. What they demonstrate is that controls are differentiated by risk tier rather than applied uniformly across all data: the practical lesson is calibration, not convergence.

For Ukraine, the most transferable lesson is not any single country's classification scheme — it is the institutional architecture behind it. Ukraine already has SSSCIP as the designated authority for the CSPs Register under Resolution 154. The priority is to modernise SSSCIP's mandate and processes so they can accommodate international cloud operating models, rather than distributing this function across ministries where it will be applied inconsistently.

8. POLICY RECOMMENDATIONS: A TRUSTED DIGITAL RECONSTRUCTION PACKAGE

The recommendations below translate the analysis in this paper into a practical package of legal reforms, governance decisions, infrastructure investments, and institutional actions. They are not a new institutional architecture — the objective is to make existing policy, procurement, cybersecurity, cloud, telecom, data-protection, and EU-alignment instruments work together coherently under wartime and recovery conditions. The matrix is organised in five groups: foundational decisions that unlock everything else; infrastructure and access; contracts, procurement, and legal reform; resilience and continuity; and capability, market development, and international cooperation. Recommendations in the first group are prerequisites for the rest; those in subsequent groups can advance in parallel once the foundational decisions are made.

Group 1 — Foundational decisions

These three recommendations are prerequisites. Without them, decisions on hosting, procurement, contracts, resilience, and partnerships cannot be made consistently or enforced.

AREA	RECOMMENDATION	EXPECTED OUTCOME	POTENTIAL LEAD OR PARTNER
Strategic framing	Adopt trusted integration as the official policy frame for Ukraine's digital reconstruction — in law, government strategy, and international dialogue — distinguishing it explicitly from both blanket localisation and unmanaged dependency	Coherent policy direction for Parliament, Government, international partners, investors, and the Ukrainian technology sector; ends the false localisation-versus-cloud binary	Parliament, Government
Data and workload classification	Introduce a unified, risk-based classification framework with three-five tiers based on confidentiality, integrity, and availability impact — as set out in the illustrative model in Section 3 — linked directly to cloud eligibility, hosting placement, encryption and key-management requirements, provider assurance standards, RTO/RPO targets (Recovery Time Objective and Recovery Point Objective), portability obligations, and exit conditions; use consistent terminology across all relevant laws; avoid over-classification	Consistent, enforceable decisions on cloud use, hosting, localisation, security controls, and continuity across all public-sector entities	Parliament, Government, central technical authority, public service owners
Reconstruction model	Adopt a classification-led cloud eligibility model mapping each tier to permitted infrastructure options: trusted public cloud, qualified cloud, hybrid or sovereign cloud, trusted cross-border backup, controlled domestic environments, or specialized national and security-authorized environments	Hosting, localisation, backup, resilience, and procurement decisions driven by risk and workload impact rather than blanket rules or political preference	Government, IFIs, donors, technology partners

Group 2 — Infrastructure and access

These recommendations determine what infrastructure Ukraine uses and on what terms. Domestic investment decisions should follow the classification model and feasibility evidence, not precede them.

AREA	RECOMMENDATION	EXPECTED OUTCOME	POTENTIAL LEAD OR PARTNER
Trusted public cloud	Maintain access to trusted domestic, European, and global cloud providers under provider-neutral Ukrainian rules based on technical safeguards, resilience, interoperability, security assurance, customer control over classification and keys, portability, and legal accountability	Faster and safer modernisation; access to best-available technologies; stronger cybersecurity capability; lower fixed infrastructure burden; broader innovation options for public-sector entities	Government, trusted providers, donors
Domestic infrastructure[5]	Decisions regarding domestic cloud infrastructure — whether data centres, regions, or local zones — should follow market-led principles, assessed against latency requirements, demand signals, energy and physical security conditions, insurance availability, workforce readiness, and commercial sustainability. Such infrastructure should be welcomed as a value-add where commercially justified.	Evidence-based investment decisions; avoid committing public funds to infrastructure that duplicates trusted external capacity without resilience benefit	Government, IFIs, investors, cloud providers, telecom operators
Cross-border resilience and continuity	Develop a trusted cross-border backup, replication, and recovery policy for selected continuity functions, covering real-time or near-real-time replication and active-active or active-passive failover where justified by classification and service criticality; treat distributed trusted cloud backup across EU jurisdictions as the preferred continuity model for eligible workloads where classification and legal conditions permit	Protection against physical destruction, blackouts, and regional concentration risk; no premature commitment to a single continuity model	Government, EU and NATO partner states, cloud providers

Group 3 — Contracts, procurement, and legal reform

These recommendations create the legal and commercial conditions under which trusted integration operates. They are largely executive and regulatory actions that do not require primary legislation for initial implementation.

AREA	RECOMMENDATION	EXPECTED OUTCOME	POTENTIAL LEAD OR PARTNER
Procurement	Create cloud-compatible procurement frameworks, service catalogues, and evaluation guidance covering consumption-based pricing, SaaS, multi-year service agreements, and lifecycle-value criteria	Faster, safer, more competitive acquisition of cloud and digital services; reduced reliance on bespoke contracts	Ministry of Economy, Prozorro, Ministry of Digital Transformation
Contracts	Develop non-binding model guidance for public-sector cloud contracting, structured by service model (IaaS, PaaS, SaaS) and classification tier, identifying key topics that should be addressed in contracts, including data ownership, hosting location, security obligations, incident notification (without prescribing specific contractual language in legislation); recognise BSI C5, ISO/IEC standards, SOC reports.	Reduced legal friction; stronger and more consistent safeguards; improved market access for Ukrainian public-sector entities and for international providers operating under Ukrainian rules	Government, legal experts, technology providers

[5] Domestic infrastructure decisions should distinguish three categories, each with different governance and financing logic: (1) commercially viable infrastructure, where market-led principles and PPP models apply; (2) public-interest resilience infrastructure (e.g., backup data centres providing continuity during blackouts or kinetic events), which may require public financing where commercial viability is insufficient; and (3) security-authorised environments for classified workloads, which require national security governance and dedicated financing outside standard procurement frameworks.

Portability and exit	Require that procurement evaluation criteria for public-sector workloads above the public/open tier include assessment of provider-offered exit mechanisms, data export capabilities, and documented service portability features; publish government guidance identifying key risk areas and evaluation factors related to exit planning, data retrieval periods, and format accessibility that contracting authorities should consider during provider selection	Reduced lock-in; preserved public-sector ability to migrate, recover, or change providers without data loss or service disruption	Public service owners, procurement authorities, providers

Group 4 — Resilience and continuity

These recommendations convert resilience from a policy aspiration into a measurable, accountable operational standard.

AREA	RECOMMENDATION	EXPECTED OUTCOME	POTENTIAL LEAD OR PARTNER
Critical service resilience	Require continuity passports for critical public digital services, specifying institutional owner, dependency map, RTO/RPO targets, backup architecture, tested failover arrangements, supplier-risk review, and escalation procedure; mandate periodic testing and aggregated public reporting — with detailed technical architecture, failover procedures, and supplier dependencies protected from disclosure — so that accountability is maintained without creating a targeting map for adversaries	Accountable, tested service continuity; resilience failures identified before they become crises	Government, SSSCIP, CERT-UA, register owners
Secure-by-design reconstruction	Embed cybersecurity baselines, resilience requirements, supplier-risk assessment, and exit-rights obligations as standard conditions in all digitally significant reconstruction investments from inception, not as retrofit requirements	New infrastructure does not reproduce pre-war vulnerabilities; resilience is costed and designed in rather than added later	Government, IFIs, donors, public service owners

Group 5 — Capability, market development, and international cooperation

These recommendations build the domestic digital economy and institutional capacity that make trusted integration sustainable beyond the reconstruction period. Several recommendations in this package — particularly cloud academies, CISO training, cyber ranges, SME digitalization support, and continuity passport development — are suited to IFI and donor co-financing. SME cloud adoption is a sovereignty issue as much as a productivity one. A digital economy in which large firms can use advanced cloud, AI, and cybersecurity tools while SMEs lack the skills, financing, certification, and procurement access to adopt them creates an uneven resilience base. Wider SME adoption of secure cloud, cyber hygiene, accounting, CRM, e-commerce, and data analytics tools also expands Ukraine's tax base, strengthens local supply-chain resilience, and reduces the gap between the export-oriented IT sector and the broader economy.

Ukraine could position these recommendations within the EU4Digital programme, World Bank digital reconstruction financing, and USAID digital governance support frameworks, developing a coordinated financing architecture that avoids fragmented project-by-project implementation.

AREA	RECOMMENDATION	EXPECTED OUTCOME	POTENTIAL LEAD OR PARTNER
Domestic digital capability	Evaluate physical infrastructure investments jointly with human-capability investments: resilient connectivity, cloud academies, university partnerships, cyber ranges, CISO and CDTO training, data-governance teams, and local integrator capacity; encourage skills-transfer frameworks, certification pathways, university partnerships, and local integrator enablement in significant international technology partnerships	Local value creation, skills transfer, and progressive reduction of dependency on external delivery capacity	Government, Diia.City, universities, private sector
SME digitalization	Support SME cloud adoption, cyber resilience, and digital productivity through opening procurement ~~participation requirements~~, subsidised certification, and access to cloud and AI tools under Ukrainian governance rules	Broader economic recovery; employment and productivity growth beyond the large-firm IT sector	Government, donors, IFIs, business associations
EU alignment	Align legal and regulatory reforms with EU data, cybersecurity, telecom, procurement, and digital governance frameworks; sequence implementation to reflect capacity and compliance costs; accompany alignment with domestic impact assessments and SME transition guidance	Stronger institutional trust with EU partners; adequacy-pathway progress; competitive access to European digital markets	Government, EU institutions, ENISA-aligned partners
Coalition-building	Launch a secure digital recovery coalition — government, EU and NATO partners, IFIs, donors, international technology companies, and the Ukrainian IT sector — coordinating implementation of the classification framework, procurement reform, resilience standards, domestic capability-building, and financing	Coordinated implementation; aligned financing and investment dialogue; shared accountability for delivery milestones	Government, EU, NATO partners, IFIs, donors, technology companies, Ukrainian IT sector

9. SEQUENCING

The six priorities below are ordered by dependency, not by importance. Priorities 1 through 3 are foundational: they create the governance rules on which all later decisions — hosting, procurement, contracts, resilience standards, capability investment — depend. Priorities 4 through 6 can begin scoping and preparation in parallel with Priorities 1 through 3, but their full implementation requires the foundational architecture to be in place. The parallel workstreams at the end of this section should start in year one regardless: coalition-building, SME support, AI governance, and sector-specific reforms do not need the classification framework to begin and delaying them creates coordination costs that compound later. The aim throughout is to avoid two failure modes: over-centralised institutional redesign that absorbs administrative capacity without producing usable tools; and fragmented project-by-project digital procurement that locks in commitments before governance rules exist.

While timelines depend on legislative capacity and the trajectory of the conflict, an indicative horizon would be: Priorities 1–2 (classification framework and procurement reform) in the first 12–18 months; Priority 3 (assurance criteria) in months 12–24; Priorities 4–6 (continuity passports, personal data alignment, capability investment) in parallel over 24–36 months, with parallel workstreams beginning in month one.

PRIORITY 1: RISK-BASED DATA AND WORKLOAD CLASSIFICATION

Classification is the single most important foundational enabler. Every subsequent decision — cloud eligibility, hosting placement, trusted-jurisdiction rules, encryption and key management, provider assurance standards, procurement requirements, RTO/RPO targets, backup architecture, cross-border replication, Data Embassy feasibility, portability obligations, and exit conditions — flows from the classification tier assigned to each dataset or workload. Without a unified framework, these decisions are made inconsistently across public-sector entities, creating legal exposure, procurement fragmentation, and resilience gaps that accumulate silently.

The five-tier model set out in Section 3 — distinguishing: Public / Open; Official / Internal; Official-sensitive / Restricted; Critical / High-impact; Secret / Top secret / defense-intelligence restricted — provides the practical working framework, grounded in confidentiality, integrity, and availability impact. A successful classification framework avoids over-classification — which congests high-assurance environments, raises costs, and restricts access to modern cloud and AI tools — uses consistent terminology across all relevant laws, and include worked guidance for public-sector entities on classifying mixed datasets and interconnected services. For sensitive and critical workloads, every classification decision should be accompanied by a documented management-level risk record covering: classification level; business and security owners; hosting model and permitted jurisdictions; encryption and key-management approach; provider assurance evidence; RTO/RPO targets; backup, failover, and replication arrangements; portability and exit plan; residual risks accepted; and the named official accountable for that acceptance. Classification without this record is a label, not an accountability mechanism.

To be operationally actionable rather than a policy document alone, the classification framework should be published in machine-readable format —enabling enforcement through cloud governance tools, resource tagging, policy guardrails, and automated compliance checks —in addition to the standard regulatory text.

PRIORITY 2: CLOUD PROCUREMENT REFORM AND STANDARD CONTRACTUAL SAFEGUARDS

Once classification principles are agreed, procurement guidance and evaluation frameworks should be updated to embed them. Cloud agreements should address the following topics as a baseline: shared responsibility allocation by service model; data ownership and customer control over location; incident notification and SLA obligations; subcontractor and processor transparency; portability requirements; exit procedures and post-termination data access; and acceptable assurance evidence. These topics should be addressed through contracting guidelines, not through prescribed contractual language in legislation. For public cloud, cybersecurity compliance assurance should be evidenced by independent third-party audit reports and recognised certifications, e.g. ISO 27001, SOC2 Type II reports. Data export and deletion obligations should reflect the cloud self-service model: customers must retain the tools, APIs, and documentation needed to retrieve or delete their data without requiring provider intervention.

Contracting guidelines should be structured around the cloud service provider's shared responsibility model, which defines the boundary between provider and customer obligations by service type — and should require contracting authorities to document, for each service procured, which party bears responsibility for which security obligations.

Personal data alignment with GDPR and Convention 108+ is a parallel workstream that must begin in this phase, even though formal adoption requires parliamentary passage. GDPR-compatible data rules determine which workloads qualify for transfer to EU-region cloud infrastructure and which provider agreements are legally available — which means procurement frameworks designed without GDPR alignment may need to be renegotiated once alignment is achieved. Contracting guidelines and procurement evaluation frameworks developed under Priority 2 should be designed to accommodate GDPR-aligned obligations from the outset. The ministries responsible for cloud procurement and those responsible for data protection legislation should be coordinating from day one of implementation.

PRIORITY 3: TRUSTED-PROVIDER ASSURANCE CRITERIA

A transparent, risk-based assurance framework for providers serving defined categories of public-sector workloads will be needed as Ukraine's classification model matures. The mechanism can function as an open qualification process — not a closed whitelist — focused on security controls, resilience, jurisdictional transparency, supply-chain transparency and sanctions compliance, secure development practices, subcontractor disclosure, incident response capability, component provenance, and business continuity. It should not operate as a blanket nationality-based exclusion except where Ukrainian law or a documented security assessment specifically requires it.

Technology supply-chain risk should be addressed explicitly within the assurance framework. Ukraine may find it useful to align its high-risk vendor determination process with the methodologies applied by EU and NATO member states for critical infrastructure procurement — including the approaches reflected in EU cybersecurity certification schemes, NIS2 supply-chain security requirements, and bilateral security assessments with partner states. Active consultation with EU and NATO partners on components, software, and providers posing supply-chain risk to critical infrastructure would reinforce Ukraine's integration trajectory and is consistent with its EU accession path. This process should be institutionalised within the assurance framework and applied systematically, rather than left to ad hoc procurement decisions made differently across public-sector entities.

A transparent, risk-based assurance framework for providers serving public-sector workloads will be needed as Ukraine's classification model matures. Such a framework should function as an open qualification process — not a closed whitelist — enabling any provider that meets the defined criteria to participate.

Provider qualification should be based primarily on internationally recognised third-party attestations and certifications — including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II, BSI C5 — rather than bespoke national compliance regimes that duplicate what independent auditors already verify. These certifications represent global cybersecurity best practices — covering areas such as access control, encryption, vulnerability management, incident response, business continuity, and secure development — and are maintained through continuous independent auditing cycles. This approach reduces compliance friction, avoids creating barriers to market entry, and ensures that assurance criteria reflect proven, continuously verified security controls rather than point-in-time assessments. International certifications are primary assurance evidence, not automatic authorisation. For workloads at Official-sensitive / Restricted tier and above, contracting authorities retain the right — and the responsibility — to apply additional risk-based verification where the workload's sensitivity, jurisdictional considerations, or supply-chain profile warrants it. The framework should specify which tiers require certification-plus-additional-review and which tiers can rely on certification alone.

Priority 4: Critical service continuity passports and failover testing

A practical starting point could be identifying a first tranche of critical public digital services whose disruption would cause the highest impact — whether on citizens, government operations, social payments, public finance, registers, identity services, or economic continuity. For each such service, a "continuity passport" concept could capture: institutional owner; key technical and supplier dependencies; RTO and RPO targets; backup architecture; tested failover arrangements; testing schedule; escalation procedure; and the officials responsible for each decision in the recovery chain.

The value of continuity passports lies in what they reveal. A service that cannot be restored after disruption is not sovereign regardless of where it is hosted. The passport approach converts resilience from a policy commitment into measurable, auditable implementation evidence — making the dependency map, not just the RTO figure, the unit of accountability.

Priority 5: Personal data alignment and standards recognition

Alignment with GDPR and Convention 108+ would support trusted cross-border data exchange, EU integration, adequacy-pathway progress, and the legal basis for recognising European and international assurance evidence in Ukrainian procurement. Given the legislative timeline involved —drafting, stakeholder consultation, and compatibility mapping with existing Ukrainian security, cloud, procurement, and information-protection law —there may be value in beginning preparatory work in parallel with Priorities 1 and 2, even though formal adoption requires parliamentary passage and will naturally take longer. The sequencing placement as fifth reflects not a lower level of urgency, but the reality that completion depends on a legislative timeline that cannot be compressed by executive action alone. Early preparation is precisely what would prevent the frameworks developed under Priorities 2 and 3 from needing to be renegotiated once alignment is achieved.

Priority 6: Domestic digital capability investment

Domestic digital infrastructure investment — data centres, cloud regions, local zones, resilient connectivity — should be guided by evidence of demand, energy resilience, physical security, insurance conditions, skills availability, and commercial viability, and should not be treated as a symbolic commitment to digital sovereignty. The more consequential investment is in the human and institutional capacity needed to govern and use trusted integration effectively: cloud academies co-developed with universities; certification pathways for public servants and SMEs; CISO and CDTO training programmes; cyber ranges; secure migration support; and local integrator enablement. Ukraine's emerging CISO Campus model — treating cybersecurity leadership as a professional ecosystem with competency standards, shared operational expertise, and a community spanning state institutions and critical infrastructure operators — illustrates the right level of ambition. Physical assets without this institutional layer are infrastructure without sovereign operation.

Data governance should be treated as part of Ukraine's sovereignty infrastructure alongside cloud governance. The next stage of Ukraine's Group A GovTech capability is not more service digitisation — it is data-driven governance and the foundations of a data economy: clear rules for data quality, interoperability, access rights, open data, non-sensitive public-sector data reuse, privacy protection, and secure analytics. The CNAPs experience is instructive here: digital transformation delivers durable value when it reaches the citizen's practical interaction with the state — through offline access points, inclusive services, and resilient local delivery — not only when it modernises backend systems. Cloud governance and data governance should be designed as a single framework: data protected where sensitive, opened or shared where lawful and useful, reused to improve public services, SME innovation, and private-sector productivity.

Parallel workstreams: coalition-building, SME support, AI governance, and sector-specific reforms

These four workstreams should begin in year one as dialogue, scoping, and pilot activities. They do not require the classification framework to be complete before starting, but their full operationalisation should be linked to the foundational governance architecture as it develops.

A secure digital recovery coalition — bringing together government, EU and NATO partners, IFIs, donors, international technology companies, Ukrainian IT firms, telecom operators, cybersecurity institutions, universities, and civil society — should coordinate around concrete outputs: the classification framework, cloud procurement tools, continuity passports, resilience indicators, trusted-provider assurance criteria, and domestic capability-building programmes. A coalition organised around declarations rather than deliverables will not sustain the coordination it needs.

SME digitalization and Ukrainian IT-sector participation should begin early, primarily through open, transparent, and outcome-based procurement design rather than additional mandatory contractual obligations. AI governance should proceed in parallel with cloud governance, applying the same classification-based approach to AI-enabled services and the same procurement and assurance standards to AI providers. Sector-specific regulatory reforms — in financial services, health, energy, and public administration — should begin as scoping workstreams that identify where sector rules conflict with or duplicate the unified classification framework and propose rationalisation before the conflicts become embedded in procurement contracts.

This sequencing keeps Ukraine moving with donors, technology partners, and domestic firms while ensuring that implementation programmes do not lock in commitments before the governance rules they depend on are in place.

10. CONCLUSION

Ukraine's own digital transformation story — from Diia to resilient wartime e-governance — demonstrates that access to diverse international technologies and partnerships has strengthened, rather than diminished, the country's ability to serve its citizens and defend its interests. These achievements were possible because Ukraine chose a path of trusted integration: engaging openly with global innovation while retaining governance authority, legal accountability, and operational control.

This does not diminish the importance of security, resilience, or national control. Genuine sovereignty demands robust cybersecurity, transparent data governance, strong local technical capacity, and the institutional ability to make independent decisions even under pressure. These are the true measures of digital independence — and they are best achieved through a competitive, diverse technology ecosystem governed under Ukrainian law aligned with recognised international and European standards.

How Ukraine defines digital sovereignty will shape the country's digital trajectory for a generation. The wartime approach — enabling Ukrainian institutions to access trusted, globally scaled cloud infrastructure — has strengthened national resilience and operational continuity. Ukrainian institutions, citizens, and businesses are already operating on cloud-based services deployed under emergency authorisations. As Ukraine develops its permanent regulatory framework, the central question is whether these proven arrangements will be confirmed on durable, predictable terms — providing the regulatory certainty that international technology partners and investors need to plan long-term commitments to Ukraine's digital future, while enabling Ukrainian firms to play an expanding role in delivery.

No external actor — whether a government, institution, or technology provider — can or should dictate how Ukraine defines its digital sovereignty. What the international community can do is respect and support Ukraine's right to chart that course freely. The trusted-integration framework described in this paper seeks to contribute to that effort: offering a practical architecture for classification, procurement, resilience, provider assurance, portability, exit rights, and capability-building that puts Ukrainian institutions in control of the decisions that matter — data classification, access, encryption, accountability, and recovery — while giving Ukraine's citizens, firms, and public services access to the best available technologies on terms that are safe, lawful, and under Ukrainian institutional control.

Cloud services, cybersecurity solutions, and AI capabilities are strategic reconstruction assets. The generation rebuilding Ukraine will use them to create better public services, stronger education and health systems, more resilient financial infrastructure, and new digital products for global markets. Trusted integration is the practical form of that sovereignty: governed access to domestic, European, and global digital capabilities under Ukrainian law, aligned with recognised international and European standards, with Ukraine retaining control over classification, access, encryption, procurement, resilience, portability, exit rights, provider assurance, and legal accountability. That is digital sovereignty in practice — and it is achievable.

REFERENCES

1. RDNA5, World Bank / Government of Ukraine / European Commission / UN, February 2026, Table 1. URL: https://www.undp.org/ukraine/publications/ukraine-fifth-rapid-damage-and-needs-assessment-rdna5-february-2022-december-2025
2. Guidance Implementing the Cloud Security Principles. URL: https://www.gov.uk/government/publications/implementing-the-cloud-security-principles/implementing-the-cloud-security-principles
3. Criteria for Assessing the Information Security of Cloud Services (PiTuKri). URL: https://kyberturvallisuuskeskus.fi/en/publications/criteria-assessing-information-security-cloud-services-pitukri
4. Italy Information Technology National Strategic Hub Cloud Services. URL: https://www.trade.gov/market-intelligence/italy-information-technology-national-strategic-hub-cloud-services
5. Government on Commercial Cloud. URL: https://www.developer.tech.gov.sg/products/categories/infrastructure-and-hosting/gcc/overview
6. Ministry of Digital Transformation of Ukraine, “У Дія.City уже понад 4 тисячі резидентів і 148 тисяч IT-фахівців”, 26 March 2026. URL: https://thedigital.gov.ua/news/business/u-diiacity-uze-ponad-4-000-rezydentiv-i-148-000-tysiach-it-fakhivtsiv
7. World Bank, GovTech Maturity Index 2025: Tracking Public Sector Digital Transformation Worldwide, Prosperity Insight Series, 2025, Table 1. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099032625154535455
8. United Kingdom Government-Cloud (G-Cloud). URL: https://learn.microsoft.com/en-us/compliance/regulatory/offering-g-cloud-uk
9. Accredited information security inspection bodies. URL: https://www.kyberturvallisuuskeskus.fi/en/our-services/assessment-accreditation-and-guidance/accredited-information-security-inspection-bodies
10. Cryptography solutions approved by Traficom's NCSA-FI. URL: https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa/cryptography-solutions-approved-traficoms-ncsa-fi
11. Italy’s Cloud Strategy. URL: https://www.acn.gov.it/portale/en/strategia-cloud-italia
12. Compliance in Italy: Navigating the New Cloud Italy Strategy. URL: https://cloudsecurityalliance.org/blog/2023/03/30/compliance-in-italy-navigating-the-new-cloud-italy-strategy/
13. Policy. URL: https://docs.developer.tech.gov.sg/docs?category=Policy
14. Compliance and Certification. URL: https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/it-standards-and-frameworks/compliance-and-certification
15. Doubling down on cloud to deliver better government services. URL: https://www.tech.gov.sg/technews/doubling-down-on-cloud-to-deliver-better-government-services/
16. Government Commercial Agency, "G-Cloud 11 goes live with 4,200 suppliers", 2 July 2019. URL: https://www.gca.gov.uk/news/g-cloud-11-goes-live-with-4200-suppliers.

About ESCU

The Economic Security Council of Ukraine (ESCU) is an independent organisation established in 2021 in Kyiv to counter external and internal threats to the national security of Ukraine and its partner countries.

Website: www.escu.ua

Facebook: www.fb.com/escofukraine

Author

Dr. Andrii Paziuk, Professor in European and International Law, Special Advisor to the EPLO Office in Ukraine, specialises in the legal governance of cloud infrastructure, data sovereignty, and public-sector digital accountability.