# Information Security and Long-Term Digital Preservation in Public Governance: Regulatory Alignment, Archival Integrity, and Technology Choices

**Volodymyr Marchenko**[1]

[1]*Doctor of Science (Law), Professor, Professor of the Department of Law Enforcement, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-1921-3041*

***Citation:***
Marchenko, V. (2025). Information Security and Long-Term Digital Preservation in Public Governance: Regulatory Alignment, Archival Integrity, and Technology Choices. *Public Administration and Law Review*, (4(24), 68–77. https://doi.org/10.36690/2674-5216-2025-4-68-77

***Received: November 21, 2025***
***Approved: December 29, 2025***
***Published: December 31, 2025***



***Abstract.*** *Digital transformation has turned information into a strategic resource of public governance, where administrative legitimacy and service continuity depend on secure electronic document management and resilient state information infrastructures. The central challenge is not only operational uptime, but also the legal validity, integrity, and evidentiary sustainability of electronic records across their lifecycle. The file emphasises that information security in public administration must be treated as a multidimensional governance phenomenon that integrates legal regulation, institutional arrangements, organisational procedures, technical safeguards, and the human factor. The objective is to substantiate a governance framework that strengthens information security and long-term digital preservation of official e-documents by aligning legal requirements with standards-based controls and technology architecture choices. The study uses integrated qualitative analysis combining formal-legal systematisation of e-document circulation requirements with comparative mapping to international standards and EU-aligned instruments. It also applies threat-informed reasoning to connect governance prescriptions with dominant incident patterns, and criteria-based evaluation of preservation architectures focused on evidentiary integrity, interoperability, and long-horizon validation. The results identify a comprehensive threat set for public e-document ecosystems, including theft, interception, modification, unauthorised use, disruption, destruction, concealment of socially significant information, and unlawful handling of personal data. These risks arise from mixed failure modes, such as external intrusion, insider misuse, governance gaps, and weak coordination, so effective protection requires combined procedural and technical controls, especially identity and access management, cryptography, monitoring, and documented custody rules. The file further shows that long-term preservation is a distinct capability problem because evidentiary value must survive cryptographic change and tool turnover; blockchain can support registry integrity, yet it is unsuitable as a long-horizon archival substrate beyond ten years due to legal and technical risks. Public-sector record protection should be implemented as a unified security and preservation governance system grounded in auditable procedures and interoperable repositories. Future work should test models for renewing long-term validation, evaluate interoperability performance of repository architectures, and assess hybrid designs linking registry event integrity to archival preservation with reproducible verification.*

***Keywords:*** *public governance; electronic documents; information security governance; digital preservation; evidentiary integrity; access control; custody rules; cryptographic change; interoperability; resilience planning; archival repositories; blockchain registries.*

***JEL Classification****: K11, K12, K24, L86, O33, O34, O38*

***Formulas: 0; fig.: 0; table: 4; bibl.: 14***

**Introduction.** Digital transformation has elevated information to a strategic resource of public governance, where administrative capacity increasingly depends on the reliability of electronic document management systems and state information infrastructures. In this context, the core problem is not only the operational continuity of e-government services, but also the legal validity and evidentiary resilience of electronic records across their life cycle. The attached text frames information security as a multidimensional phenomenon that integrates legal regulation, institutional arrangements, organizational practices, technical controls, and human factors, rather than a purely technical discipline.

This framing is especially relevant for jurisdictions undergoing regulatory modernization and European integration, where fragmentation of rules and limited interoperability can undermine integrity guarantees and citizen trust.

At the same time, international experience demonstrates that the scale and intensity of cyber threats make "business as usual" approaches to recordkeeping increasingly risky for public institutions. For example, EU public administration was reported as the most targeted sector in ENISA's sectorial threat landscape for 2024, with a substantial portion of incidents linked to denial-of-service patterns that disrupt public service delivery. Consequently, research and policy now converge on a practical question: which combinations of legal rules, standards-based controls, and technology architectures can simultaneously protect confidentiality, ensure integrity, preserve accessibility, and sustain evidentiary value over time.

**Literature review.** The governance of electronic records rests on two interdependent streams of scholarship and practice: information security governance and digital preservation. The information security stream typically operationalizes protection through confidentiality, integrity, and availability requirements, supported by layered controls such as access differentiation, cryptographic protection, monitoring, and incident response.

This approach is reinforced by the ISO/IEC 27001 family, which positions information security as a management system problem grounded in risk assessment and continuous improvement, while ISO/IEC 27002 provides a control catalogue spanning access control, cryptography, operational security, and incident management. In parallel, records management and archival scholarship emphasizes authenticity, provenance, and long-term usability, recognizing that format obsolescence, metadata decay, and technology turnover can erode evidentiary reliability even in the absence of malicious activity. These concerns are addressed in practice through records management principles such as those codified in ISO 15489-1 and through digital preservation reference models such as OAIS (ISO 14721), which define preservation responsibilities and functional components for trustworthy archives.

A third literature stream connects public governance to cross-border

trust services and cybersecurity regulation. In the EU, the NIS2 framework strengthens baseline cybersecurity obligations across critical sectors, and emphasizes governance, reporting, and resilience as systemic requirements rather than optional technical enhancements. In parallel, eIDAS anchors the legal recognition of electronic signatures, seals, and timestamps as trust services, which is directly relevant to the authentication and integrity verification of official electronic documents. The attached text highlights that integrity verification in public electronic document flows commonly relies on digital signatures as both integrity and authorship authentication mechanisms, but also stresses that legislative inconsistencies and organizational misuse risks can weaken real protection if security is treated in isolation from the broader infrastructure and governance environment.

Finally, the literature on emerging technologies, especially distributed ledger technology, often claims benefits for transparency and tamper resistance in registries. The attached text recognizes blockchain's potential for integrity and accountability in state registries, but also identifies strict preconditions for legitimate deployment, including robust procedures for recording, access governance, and institutional support.

Importantly, it also argues that blockchain is currently ill-suited for long-term archival preservation of legally significant documents beyond ten years due to legal and technical risks, including cryptographic change and emerging quantum concerns.

This position aligns with a broader preservation-oriented view that durable evidentiary value depends on governance, standards, and reproducible verification, not only on immutability claims.

**Aims.** The aim of this article is to develop a coherent analytical framework for strengthening information security and long-term preservation of electronic documents in public governance by integrating legal requirements, international standards, and empirically grounded threat evidence, with a focused assessment of technology choices including archival repositories and distributed ledgers.

**Methodology.** The article applies an integrated qualitative methodology combining formal-legal analysis, comparative analysis, and system-structural reasoning consistent with approaches described in the attached text.

First, legal requirements for electronic document management and archiving are systematized using the Ukrainian legal definition of electronic document circulation as a set of processes for creation, processing, transmission, reception, storage, use, and destruction with integrity verification. Second, institutional and technical requirements are mapped to internationally recognized standards and EU frameworks, including ISO 15489-1, OAIS (ISO 14721), ISO/IEC 27001 and 27002, NIS2, and eIDAS. Third, a threat-informed perspective is added through secondary statistical evidence from ENISA and Verizon to identify dominant incident patterns

affecting public administration and to connect governance prescriptions to observed risks. Fourth, technology options are evaluated through criteria-based comparison emphasizing evidentiary integrity, interoperability, cost realism, and long-horizon validation.

**Results.** The attached text enumerates major information security threats relevant to electronic document management, including theft of protected information, destruction of information or software, unlawful interception, modification of data, unauthorized use, disruption of systems and networks, concealment of information affecting public interests, and unlawful personal data collection or use.

These threats are not purely technical because they reflect mixed failure modes: adversarial intrusion, insider misuse, governance gaps, and weak institutional coordination. A key implication is that electronic document environments require controls that are simultaneously technical and procedural, including identity and access management, cryptography, monitoring, and documented rules for custody and authorized actions.

Table 1 synthesizes a governance-oriented mapping between dominant threats and control domains for public electronic document management. The table condenses the most common threat classes affecting electronic document systems into control priorities that combine management-system logic (policies, roles, monitoring) with technical safeguards (cryptography, logging, resilience). It is designed to support risk-based planning and audit scoping.

**Table 1. Threats and control priorities for electronic document management in public governance**

| Threat class | Primary impact on records | Control priority domains | Illustrative controls (standards-aligned) |
|---|---|---|---|
| Data theft and unlawful access (including protected secrets, personal data) | Confidentiality breach, loss of trust | Access governance; data protection compliance | Role-based access; least privilege; MFA; encryption at rest and in transit; DLP; audit logs (ISO/IEC 27002 guidance) |
| Data modification or tampering | Integrity loss, evidentiary weakness | Integrity assurance; provenance controls | Digital signatures and seals; hashing; immutable logging; change control; segregation of duties |
| System disruption (DDoS, sabotage, outages) | Availability loss, service interruption | Resilience and continuity | Backups; redundancy; traffic filtering; incident playbooks; recovery testing (NIS2 governance emphasis) |
| Insider misuse (authorized users) | Covert leakage, policy circumvention | Organizational controls; monitoring; accountability | Monitoring; privileged access management; training; sanctions; case management workflows |
| Destruction or loss of records (malware, failure, poor preservation) | Long-term loss of evidence | Preservation architecture; migration planning | Trusted repositories; format management; integrity checks; retention controls; OAIS-aligned workflows |

*Source: systematized by the author*

Table 1 shows that the same electronic record can be simultaneously exposed to confidentiality, integrity, and availability risks, which implies that narrow "IT controls only" programs will be structurally insufficient. Instead, controls must be assembled as a governance system that binds legal duties, institutional roles, and technical enforcement into one auditable chain.

A major contribution of the attached text is its emphasis that electronic documents remain within institutional archival systems from creation or receipt until transfer to a state archive or destruction, with access rights regulated by hierarchy and functional responsibilities.

It further notes a specific long-term preservation practice: documents designated for permanent or long-term storage, defined as more than ten years, must be accompanied by paper copies produced immediately after completion, reflecting a risk-hedging approach to authenticity and future accessibility.

This requirement illustrates a practical recognition that long-horizon validation is difficult when cryptographic methods, file formats, and validation infrastructure evolve. It also implies that preservation risk is not merely a storage problem, but a continuing capability problem, meaning institutions must preserve not only bytes but also metadata, validation methods, and documented procedures for reproducible verification. The Ukrainian legal framework also requires integrity verification, preservation periods equivalent to paper documents, duplication across media where needed, recoverability, and metadata about origin and transmission, which together define a compliance baseline for archival design.

Table 2 summarizes a minimal "trust chain" for long-term preservation that integrates legal compliance, records management, and security governance. The table translates long-term preservation into a sequence of capabilities. Each capability is framed as a condition for maintaining evidentiary value and operational usability over extended periods, not only as a technical storage decision.

Table 2 indicates that preservation is a continuing governance obligation that couples records science with cybersecurity. When any element of the trust chain is missing, long-term storage may still exist physically, but the legal and administrative value of the record can collapse because verification, accessibility, or lawful access cannot be sustained.

Threat evidence and cost metrics support the conclusion that public sector electronic document systems operate under increasing stress. IBM's widely cited cost estimates report an average global cost of a data breach of USD 4.88 million in 2024, underscoring that breaches have system-level financial implications beyond purely technical remediation. Meanwhile, the 2025 Verizon DBIR executive summary reports ransomware as a significant component of breaches, with especially high prevalence among smaller organizations and meaningful presence in larger ones, implying that

disruption and extortion patterns should be treated as expected risks rather than exceptional events.

**Table 2. Minimal trust chain for long-term preservation of official electronic documents**

| Capability | What must be preserved | Why it matters | Implementation anchor |
|---|---|---|---|
| Authenticity and provenance | Metadata, origin context, custody records | Courts and auditors need traceable origin and controlled handling | ISO 15489-1 records principles |
| Integrity verification over time | Hashes, signatures, validation artifacts, renewal strategy | Signatures and algorithms may become obsolete | eIDAS trust services logic; long-term validation principle |
| Accessibility and readability | Format migration plans, rendering tools, documentation | Records must remain usable despite software turnover | OAIS reference model for preservation responsibility |
| Confidentiality and lawful access | Access rules, logging, privacy safeguards | Archives often hold sensitive and personal data | Convention 108 principles; ISO/IEC 27002 control domains |
| Resilience and recoverability | Redundancy, backups, disaster recovery procedures | Public services cannot depend on a single point of failure | NIS2 governance orientation to resilience |

*Source: systematized by the author*

For public administration specifically, ENISA reporting highlights high targeting intensity in the EU and emphasizes denial-of-service as a dominant incident type affecting public sector availability and service delivery.

Table 3 consolidates a small set of operational statistics and interprets their governance relevance for electronic record systems. The purpose of this table is not to create a comprehensive threat database, but to connect a few high-salience indicators to concrete governance decisions in electronic document management and archiving.

**Table 3. Selected cyber risk statistics and their governance implications for public electronic document systems**

| Indicator | Reported figure | Practical implication for e-document and archive governance |
|---|---|---|
| Average global cost of a data breach (2024) | USD 4.88 million | Justifies budgeting for prevention, detection, and recovery as core governance functions, not discretionary IT spending |
| Public administration targeting (EU, 2024 sectorial landscape) | Public administration reported as most targeted sector, with a large incident share | Requires hardening of citizen-facing services and continuity planning for registries and document portals |
| Ransomware prominence (2025 DBIR executive summary) | Ransomware frequently present in breaches, with high prevalence in SMEs | Reinforces need for segmented backups, recovery testing, privileged access control, and rapid containment playbooks |

*Source: systematized by the author*

Table 3 demonstrates that the justification for stronger information security and preservation governance is not theoretical. Measurable threat concentration in public administration and high breach costs support an institutional shift toward standards-based controls, resilience engineering, and audit-ready evidence practices.

The attached text offers a balanced position on distributed ledger technologies in public governance. It argues that blockchain can enhance integrity, transparency, and accountability of state registries, and potentially reduce transaction costs, but only if governance preconditions are met, including legally robust procedures, clear access rights, and institutional capacity.

However, it also concludes that blockchain is currently not suitable for long-term archival preservation of legally significant documents beyond ten years, due to risks from technological change and cryptographic evolution, including quantum-related concerns.

This distinction is consequential: it implies that blockchain may serve as an auxiliary integrity layer for registry events and short-to-medium horizon traceability, while trusted digital repositories and preservation models remain the primary solution for archival custody. In practice, this leads to an architectural recommendation: separate “transaction truth” for registry updates from “archival truth” for record preservation, and connect them through interoperable metadata, renewal strategies for validation, and legally recognized trust services.

Table 4 compares technology architecture options for preserving evidentiary integrity and operational usability. The table provides a decision-oriented comparison of common architectures against criteria that matter for public governance: evidentiary integrity, interoperability, cost realism, and long-term validation.

Table 4 supports a conservative but effective conclusion: long-term preservation should remain repository-centered and standards-driven, while blockchain may be selectively used as an auxiliary integrity and transparency instrument in registries where governance conditions are satisfied.

**Discussion.** The results suggest that public governance should treat electronic document security and preservation as a single policy field with multiple layers, rather than as separate IT and archival domains. The Ukrainian framework described in the attached text emphasizes integrity verification and detailed storage obligations, but it also implicitly reveals a capability gap: long-term validation depends on sustained institutional capacity, tool continuity, and governance discipline, which is why paper copies remain mandated for records kept longer than ten years.

**Table 4. Comparative assessment of preservation and integrity architectures for public records**

| Architecture | Strengths | Core limitations | Best-fit use case |
|---|---|---|---|
| Centralized trusted digital repository (OAIS-aligned) | Preservation workflows, metadata governance, format migration, controlled access | Requires sustained funding and institutional capability | Permanent and long-term state archives |
| Records management systems with signature-based integrity checks | Strong operational alignment; integrity verification tied to authorship workflows | Long-term validation requires renewal and tool continuity | Routine administrative workflows, medium horizon records |
| WORM or read-only storage with logging | Reduces tampering risk; supports immutability claims | Does not solve provenance or accessibility over decades | High-integrity retention for specific categories |
| Permissioned blockchain for registry event logging | Tamper-resistant sequencing of events; multi-party synchronization | Not fit for long-term legal preservation; governance and cryptographic evolution risks | Registry audit trails, short-to-medium horizon traceability |
| Hybrid model: repository plus integrity anchoring | Combines preservation strengths with external integrity markers | Requires careful interoperability and legal recognition | High-value registries and documents requiring strong auditability |

*Source: systematized by the author*

From a comparative perspective, EU policy trends reinforce the same logic through different instruments. NIS2 emphasizes governance accountability and resilience across sectors, implying that electronic records are part of critical service continuity rather than merely administrative artifacts. eIDAS, in turn, provides a legal basis for trust services that support signature, seal, and timestamp validation, which directly affects whether integrity verification remains feasible as technologies change.

A further implication concerns interoperability. The attached text notes that effective repositories should enable convenient access for officials and citizens regardless of location and time, and that rapid growth in electronic documents increases urgency for robust long-term preservation and simplified access procedures.

This aligns with OAIS and records management principles, which treat designated communities and controlled dissemination as core requirements, not optional features. Interoperability is therefore a governance choice expressed through open formats, metadata profiles, and institutional mandates, and it determines whether preservation can survive vendor dependence and platform turnover.

Finally, emerging technology adoption should be constrained by evidentiary realism. Blockchain's potential for registry integrity is meaningful, but the attached text's caution regarding long-horizon archival preservation is consistent with the broader principle that "immutability" does not automatically equate to admissible authenticity decades later.

As cryptographic standards evolve and validation ecosystems change, preservation requires renewable trust mechanisms, documented processes, and institutional responsibility. This supports a hybrid modernization pathway: strengthen baseline controls through ISO-aligned management systems and preservation reference models, align legal rules with EU trust services and cybersecurity governance, and then adopt emerging technologies only where they add demonstrable value without undermining long-term validity.

**Conclusions.** Information security in public electronic document management is best understood as a governance system that integrates legal norms, institutional capacity, and technical controls, rather than as a set of isolated security tools.

Long-term preservation creates a distinct risk profile because evidentiary value must survive technology turnover, which explains why legal regimes may require additional safeguards for records stored beyond a decade, including parallel paper retention practices.

Empirical threat reporting and cost metrics confirm that public administration is a high-pressure target environment and that disruption and extortion risks should be treated as expected constraints on e-government reliability. Standards and EU frameworks provide a coherent direction for modernization: NIS2 strengthens governance and resilience expectations, eIDAS supports durable trust services, and ISO and OAIS standards offer implementable architectures for records authenticity and preservation. Blockchain can be valuable for registry integrity and traceability under strict governance conditions, but it should not be treated as a default archival substrate for long-horizon preservation at the current stage of technological and legal development.

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

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

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

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

**References:**

1. Castells, M. (1996). The rise of the network society. Blackwell.
2. Council of Europe. (1981). Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108). https://rm.coe.int/1680078b37
3. ENISA. (2025, November 6). Public administration increasingly targeted by DDoS attacks. https://www.enisa.europa.eu/news/public-administration-increasingly-targeted-by-ddos-

attacks
4. ENISA. (2025). ENISA sectorial threat landscape: Public administration (2024). https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Public%20Administration%20TL%202024_0.pdf
5. European Commission. (n.d.). NIS2 Directive: Securing network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
6. European Parliament and Council of the European Union. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng
7. IBM Security, & Ponemon Institute. (2024). Cost of a data breach report 2024. https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
8. ISO. (2012). ISO 14721:2012. Open archival information system (OAIS): Reference model. https://www.iso.org/standard/57284.html
9. ISO. (2016). ISO 15489-1:2016. Records management: Concepts and principles. https://www.iso.org/standard/62542.html
10. ISO. (2022). ISO/IEC 27001:2022. Information security management systems. https://www.iso.org/standard/27001
11. ISO. (2022). ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection: Information security controls. https://www.iso.org/standard/75652.html
12. Marchenko, V. (2025). Digitalization of Public Administration: Conceptual Foundations, Institutional Change, and Implementation Policy. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 10-26). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-10-26
13. Verizon. (2025). 2025 data breach investigations report: Executive summary. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf
14. Verkhovna Rada of Ukraine. (2003). On electronic documents and electronic documents circulation: Law of Ukraine No. 851-IV (May 22, 2003). https://zakon.rada.gov.ua/go/851-15