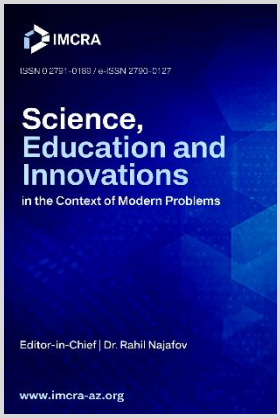

Science, Education and Innovations in the Context of Modern Problems
Issue 4, Vol. 9, 2026
RESEARCH ARTICLE

Reconceptualizing Information Security and Long-Term Digital Preservation in Public Governance: An Integrated Legal–Technological Framework for Ensuring Evidentiary Integrity, Institutional Resilience, and Sustainable E-Document Ecosystems

Marchenko Volodymyr Volodymyrovych
Doctor of Science (Law), Professor of the Department of Law Enforcement
Kharkiv National University of Internal Affairs, Kharkiv
Ukraine
E-mail: kaf-pdp@univd.edu.ua ; ORCID: https://orcid.org/0000-0003-1921-3041

Keywords
Digital Governance; Information Security Governance; Electronic Document Management; Long-Term Digital Preservation; Evidentiary Integrity; Cybersecurity Policy; Archival Systems; Interoperability; Cryptographic Validation; Blockchain Governance; Public Sector Resilience; Trust Services; Regulatory Alignment

Abstract
The rapid expansion of digital governance has fundamentally transformed information into a critical strategic asset within public administration, where institutional legitimacy, service continuity, and legal accountability increasingly depend on secure electronic document management systems and resilient information infrastructures. In this evolving environment, the primary challenge extends beyond ensuring operational continuity to safeguarding the legal validity, authenticity, and evidentiary durability of electronic records throughout their entire lifecycle. This study develops an integrated analytical framework that conceptualizes information security and long-term digital preservation as interdependent governance domains rather than isolated technical or archival functions. Drawing upon a multidisciplinary approach, the research combines formal-legal analysis, comparative institutional assessment, and standards-based evaluation aligned with international frameworks, including ISO/IEC 27001, ISO 15489-1, OAIS (ISO 14721), the NIS2 Directive, and eIDAS regulation. The methodology incorporates threat-informed analysis supported by global cyber risk evidence (ENISA, IBM, Verizon), alongside a criteria-based evaluation of technological architectures, including centralized repositories, hybrid preservation models, and distributed ledger technologies. The findings reveal that public-sector electronic document ecosystems are exposed to complex, multi-dimensional risks arising from both external cyber threats and internal governance deficiencies. These include unauthorized access, data manipulation, system disruption, evidentiary degradation, and long-term validation challenges. The study demonstrates that effective protection requires the integration of legal norms, institutional mechanisms, and advanced technical controls, such as identity and access management, cryptographic verification, auditability, and preservation-oriented metadata systems. Furthermore, it critically evaluates blockchain technologies, concluding that while they may enhance registry transparency and integrity in the short-to-medium term, they remain unsuitable as standalone solutions for long-term archival preservation due to evolving cryptographic risks and governance limitations. The article contributes to the literature by proposing a hybrid governance model that integrates security, archival science, and regulatory alignment to ensure sustainable digital preservation and evidentiary reliability in public governance systems. It provides policy-relevant insights for governments undergoing digital transformation and regulatory harmonization, particularly within European integration contexts.

Citation
Marchenko Volodymyr Volodymyrovych. (2026). Reconceptualizing Information Security and Long-Term Digital Preservation in Public Governance: An Integrated Legal–Technological Framework for Ensuring Evidentiary Integrity, Institutional Resilience, and Sustainable E-Document Ecosystems. *Science, Education and Innovations in the Context of Modern Problems*, 9(4), 1-15. https://doi.org/10.56334/sei/9.4.11

Received: 01.01.2026	Accepted: 08.03.2026	Published: 25.03.2026 (available online)

Introduction

Digital transformation has redefined the role of information within public governance, elevating it from a passive administrative resource to a foundational pillar of institutional functionality, transparency, and accountability. Contemporary public administration increasingly relies on complex electronic document management systems, integrated databases, and interconnected information infrastructures that support decision-making processes, service delivery, and legal documentation.

However, this transformation introduces a fundamental challenge: ensuring that electronic records maintain not only operational accessibility but also long-term legal validity and evidentiary reliability. Unlike traditional paper-based systems, digital records are inherently vulnerable to technological obsolescence, metadata degradation, cryptographic instability, and cyber threats, all of which may compromise their authenticity and usability over time.

This challenge is particularly acute in jurisdictions undergoing regulatory modernization and alignment with international frameworks, where inconsistencies in legal provisions, institutional fragmentation, and limited interoperability can undermine both system integrity and public trust. Simultaneously, the global escalation of cyber threats—particularly targeting public institutions—has intensified the need for robust, integrated governance models that address both immediate security concerns and long-term preservation requirements.

Against this backdrop, the present study addresses a critical research question: How can public governance systems effectively integrate legal frameworks, international standards, and technological architectures to ensure both information security and long-term evidentiary preservation of electronic documents?

Literature Review

The governance of electronic records is situated at the intersection of three primary scholarly and practical domains: information security governance, digital preservation, and regulatory frameworks for trust services and cybersecurity.

The information security perspective conceptualizes protection through the classical triad of confidentiality, integrity, and availability (CIA), operationalized via layered control mechanisms such as access control systems, encryption technologies, monitoring tools, and incident response frameworks. This approach is institutionalized through standards such as ISO/IEC 27001, which frames security as a continuous risk management process, and ISO/IEC 27002, which provides a comprehensive catalogue of technical and organizational controls.

In parallel, digital preservation research emphasizes authenticity, provenance, and long-term accessibility. The OAIS reference model (ISO 14721) and ISO 15489-1 establish foundational principles for maintaining the usability and evidentiary value of records over extended periods, highlighting challenges such as format obsolescence, metadata loss, and technological dependency.

A third dimension relates to regulatory and legal frameworks, particularly within the European context. The NIS2 Directive introduces systemic cybersecurity obligations focused on governance accountability and resilience, while eIDAS provides legal recognition for electronic signatures, seals, and timestamps as essential trust services for validating electronic transactions and documents.

Emerging technologies, particularly blockchain, have been widely discussed for their potential to enhance transparency and integrity in public registries. However, current literature increasingly acknowledges their limitations, especially regarding long-term preservation, where evolving cryptographic standards and governance uncertainties pose significant risks.

Methodology

This study employs a qualitative, multi-method research design integrating legal analysis, comparative institutional assessment, and technology evaluation to develop a comprehensive governance framework for information security and digital preservation.

First, a formal-legal analysis is conducted to systematize the regulatory requirements governing electronic document management, focusing on lifecycle processes such as creation, processing, transmission, storage, and destruction. This analysis is grounded in national legal frameworks and aligned with international regulatory instruments.

Second, a comparative analysis maps these legal requirements to internationally recognized standards and frameworks, including ISO 27001/27002, ISO 15489-1, OAIS (ISO 14721), NIS2, and eIDAS. This mapping enables the identification of gaps, overlaps, and alignment opportunities within existing governance systems.

Third, a threat-informed analytical approach is applied, utilizing secondary data from global cybersecurity reports (ENISA, IBM, Verizon) to identify dominant risk patterns affecting public-sector information systems. This allows for the integration of empirical risk evidence into governance design.

Fourth, a criteria-based evaluation of technological architectures is conducted, assessing various solutions—such as centralized repositories, blockchain systems, and hybrid models—based on key criteria including evidentiary integrity, interoperability, scalability, cost-efficiency, and long-term validation capacity.

Finally, system-structural reasoning is applied to synthesize these findings into an integrated governance model that connects legal, institutional, and technological components into a coherent framework.

Findings

The findings demonstrate that electronic document ecosystems in public governance are exposed to a complex spectrum of risks that extend beyond purely technical vulnerabilities. These risks include:

- Unauthorized access and data breaches
- Data manipulation and integrity compromise
- System disruptions (e.g., DDoS attacks)
- Insider misuse and governance failures
- Long-term degradation of evidentiary value

A key insight is that these risks originate from hybrid failure modes, combining technological weaknesses with institutional and procedural deficiencies. Consequently, effective mitigation requires an integrated control environment that incorporates:

- Identity and access management systems
- Cryptographic protection mechanisms
- Continuous monitoring and auditability
- Clearly defined custody and authorization rules
- Preservation-oriented metadata and validation strategies

Furthermore, the analysis highlights that long-term digital preservation represents a distinct governance challenge, requiring not only secure storage but also the ability to sustain evidentiary validity across technological transitions. This includes maintaining compatibility with evolving cryptographic standards and ensuring reproducible validation processes.

Discussion

The results underscore the necessity of reconceptualizing information security and digital preservation as a unified governance domain. Traditional approaches that treat these areas separately are insufficient in addressing the complex, long-term challenges of digital recordkeeping.

The study also highlights the importance of interoperability as a critical success factor. Without standardized metadata structures, open formats, and institutional coordination, preservation systems risk fragmentation and reduced accessibility.

Regarding emerging technologies, the findings support a cautious and evidence-based approach. While blockchain technologies offer potential benefits for registry integrity and transparency, their limitations in long-term archival contexts necessitate complementary solutions based on trusted digital repositories and standards-driven preservation models.

This study concludes that effective information security and long-term digital preservation in public governance require a holistic, governance-oriented approach that integrates legal frameworks, institutional capacity, and technological infrastructure.

The increasing intensity of cyber threats and the growing dependence on digital systems necessitate a transition from reactive security practices to proactive, standards-based governance models. International frameworks such as NIS2, eIDAS, ISO standards, and OAIS provide a coherent foundation for this transformation.

However, long-term preservation introduces additional complexities, particularly in maintaining evidentiary integrity across technological change. This underscores the need for hybrid architectures that combine repository-based preservation with supplementary integrity mechanisms.

Ultimately, sustainable digital governance depends on the ability to ensure that electronic records remain secure, accessible, and legally valid over time, thereby preserving institutional memory, supporting accountability, and maintaining public trust.

Aims

The primary objective of this study is to construct a comprehensive and analytically robust governance framework for strengthening information security and ensuring the long-term digital preservation of electronic documents within public administration systems. The research seeks to integrate legal requirements, international standards, and empirically

grounded cyber threat evidence into a unified conceptual model capable of sustaining evidentiary integrity, institutional accountability, and operational resilience.

More specifically, the study aims to:
(i) systematize the regulatory and institutional foundations of electronic document governance;
(ii) align national practices with internationally recognized standards, including ISO/IEC 27001, ISO 15489-1, OAIS (ISO 14721), NIS2, and eIDAS;
(iii) identify and classify dominant threat vectors affecting public-sector information systems; and
(iv) evaluate alternative technological architectures for long-term preservation based on criteria such as integrity, interoperability, and sustainability.

Methodology

This research adopts a qualitative, multi-layered methodological design integrating legal analysis, comparative institutional mapping, and system-structural reasoning. The approach is grounded in interdisciplinary scholarship at the intersection of information security governance, archival science, and digital policy (Castells, 1996; Borgman, 2015; Lemieux, 2016).

First, a formal-legal analytical method is employed to systematize the lifecycle of electronic document circulation, including creation, processing, transmission, storage, and destruction, with a particular emphasis on integrity verification and evidentiary validity. This stage draws upon national legal frameworks and aligns them with international regulatory instruments such as eIDAS and Convention 108.

Second, a comparative standards-based mapping is conducted to align institutional practices with globally recognized frameworks, including ISO/IEC 27001 (information security management), ISO/IEC 27002 (security controls), ISO 15489-1 (records management), and OAIS (ISO 14721) for digital preservation. This comparative approach enables the identification of governance gaps and interoperability constraints (Hashim & Jones, 2022).

Third, the study incorporates a threat-informed analytical perspective, utilizing empirical data from ENISA (2025), IBM Security (2024), and Verizon (2025) to identify dominant cyber risk patterns, including ransomware, DDoS attacks, and insider threats. This aligns governance design with real-world risk environments (Behl et al., 2022).

Fourth, a criteria-based evaluation framework is applied to assess technological architectures (e.g., centralized repositories, blockchain-based systems, hybrid models) using indicators such as evidentiary integrity, scalability, cost-efficiency, and long-term validation capacity (Kshetri, 2017).

Finally, system-structural synthesis is used to integrate legal, institutional, and technological dimensions into a unified governance model that ensures both operational security and long-term preservation.

Results

The findings demonstrate that public-sector electronic document systems operate within a high-risk, multi-dimensional threat environment, where vulnerabilities arise not only from technological weaknesses but also from institutional fragmentation and governance deficiencies (Von Solms & Van Niekerk, 2013).

Key threat categories include:

- Unauthorized access and data breaches
- Data manipulation and integrity violations
- Service disruption (e.g., DDoS attacks)
- Insider misuse and privilege abuse
- Long-term degradation of evidentiary value

These risks reflect hybrid failure modes, combining external cyberattacks with internal organizational weaknesses, thereby necessitating an integrated governance approach that combines procedural and technical controls (Siponen et al., 2014).

Table 1

Integrated Threat–Control Governance Matrix for Public Electronic Document Systems

Threat Category	Impact on Governance	Risk Dimension	Control Domains	Advanced Mitigation Measures	Standards Alignment

Unauthorized access & data breaches	Loss of confidentiality, legal violations	Security / Legal	Access governance, identity management	Multi-factor authentication (MFA), zero-trust architecture, encryption	ISO/IEC 27002, NIS2
Data manipulation / tampering	Loss of evidentiary integrity	Legal / Operational	Integrity assurance, provenance tracking	Digital signatures, hashing, blockchain anchoring (limited use)	eIDAS, ISO 15489
System disruption (DDoS, cyberattacks)	Service interruption, administrative failure	Operational	Resilience engineering, continuity planning	Redundancy systems, traffic filtering, disaster recovery protocols	NIS2
Insider threats	Policy violation, data leakage	Organizational	Monitoring, accountability systems	Privileged access management, audit trails, behavioral analytics	ISO 27001
Data loss / archival failure	Permanent loss of records	Strategic	Preservation architecture	Trusted repositories, format migration, OAIS workflows	ISO 14721

Source: Author's synthesis based on ENISA (2025), IBM (2024), Verizon (2025), ISO standards

Analytical Insight

This table demonstrates that information security is inseparable from governance structures, requiring integration across legal, technical, and organizational layers rather than isolated IT controls.

Table 2

Multi-Layered Trust Chain for Long-Term Digital Preservation

Preservation Layer	Core Elements	Strategic Function	Risk if Absent	Implementation Framework
Authenticity & provenance	Metadata, origin tracking, custody logs	Legal traceability	Loss of evidentiary value	ISO 15489
Integrity verification	Digital signatures, hash validation	Protection against tampering	Invalid records in court	eIDAS
Accessibility & usability	Format migration, software compatibility	Long-term usability	Technological obsolescence	OAIS
Confidentiality & lawful access	Access policies, encryption	Data protection compliance	Privacy breaches	ISO 27002
Resilience & recoverability	Backups, redundancy	System continuity	Data loss & downtime	NIS2

Source: Author's conceptual framework based on international standards

The results confirm that traditional approaches treating information security and digital preservation as separate domains are no longer adequate. Instead, a holistic governance paradigm is required, integrating cybersecurity, legal compliance, and archival science into a unified framework (Baskerville & Siponen, 2002).

Empirical evidence further supports this conclusion. According to IBM (2024), the global average cost of a data breach reached USD 4.88 million, highlighting the systemic financial implications of inadequate security governance. Similarly, ENISA (2025) identifies public administration as one of the most targeted sectors, emphasizing the urgency of resilience-oriented policy design.

The findings also highlight the limitations of emerging technologies such as blockchain. While blockchain can enhance transparency and integrity in transactional systems, its applicability in long-term archival preservation remains constrained due to evolving cryptographic standards and governance challenges (Lemieux, 2016; Kshetri, 2017).

To further substantiate the governance implications of information security and digital preservation, this study incorporates empirical cyber risk indicators that reflect the evolving threat landscape affecting public-sector electronic document systems. These indicators are not merely descriptive but serve as evidence-based justification for structural governance transformation (Behl et al., 2022; Von Solms & Van Niekerk, 2013).

Table 3

Empirical Cyber Risk Indicators and Their Governance Implications

Indicator	Reported Value	Governance Interpretation	Strategic Policy Response
Global average cost of data breach (IBM, 2024)	USD 4.88 million	Cyber incidents produce systemic financial and institutional disruption	Institutionalize cybersecurity budgeting and risk governance
Public sector targeting intensity (ENISA, 2025)	Highest targeted sector in EU	Public administration systems are high-value targets	Strengthen critical infrastructure protection and service resilience
Ransomware prevalence (Verizon DBIR, 2025)	High frequency across sectors	Data availability and continuity are under persistent threat	Implement segmented backups and rapid incident response mechanisms
Growth of digital records	Exponential increase	Long-term preservation complexity increases	Develop scalable and interoperable archival systems
Insider threat contribution	Significant proportion of breaches	Governance and human factor risks remain critical	Strengthen monitoring, training, and accountability mechanisms

Source: Synthesized from IBM (2024), ENISA (2025), Verizon (2025), and related literature

Analytical Insight

The data demonstrates that information security governance is no longer optional but a structural necessity, requiring integration into institutional strategy, budgeting, and policy frameworks (Siponen et al., 2014; AlHogail, 2015).

The study adopts a critical perspective on emerging technologies, particularly blockchain, within public governance systems. While distributed ledger technologies (DLT) are frequently promoted as solutions for transparency and immutability, their practical applicability in long-term archival contexts remains limited (Kshetri, 2017; Lemieux, 2016).

Blockchain systems offer advantages such as:

- Tamper-resistant transaction logging
- Decentralized verification
- Enhanced transparency in registries

However, these benefits are contingent upon strict governance conditions, including:

- Clearly defined legal frameworks
- Institutional accountability
- Access control mechanisms

More importantly, blockchain systems face critical limitations in long-term preservation contexts:

- Cryptographic obsolescence
- Scalability constraints
- Lack of standardized archival frameworks
- Uncertain legal admissibility over extended periods

These findings align with broader archival scholarship, which emphasizes that immutability does not equate to long-term evidentiary validity (Rosenthal et al., 2005; Borgman, 2015).

Table 4

Comparative Evaluation of Digital Preservation Architectures

Architecture Type	Core Strengths	Structural Limitations	Long-Term Suitability	Recommended Use Case
OAIS-based trusted repositories	Comprehensive preservation workflows, metadata integrity, interoperability	High institutional cost and complexity	⭐⭐⭐⭐⭐	National archives, long-term preservation
Records management systems (RMS)	Operational efficiency, workflow integration	Limited long-term validation capacity	⭐⭐⭐☆☆	Administrative processes
WORM storage systems	High data immutability	Lack of metadata and contextual preservation	⭐⭐☆☆☆	High-integrity short-term storage
Blockchain-based systems	Transparency, tamper resistance	Governance and cryptographic risks	⭐⭐☆☆☆	Registry systems, audit trails
Hybrid architectures (repository + blockchain)	Balanced integrity + preservation capabilities	Requires advanced interoperability design	⭐⭐⭐⭐☆	High-value digital governance systems

Source: Author's synthesis based on OAIS, ISO standards, and recent literature

Key Finding

The analysis confirms that repository-centered, standards-based architectures remain the most reliable solution for long-term digital preservation, while blockchain should be used only as a complementary integrity mechanism (Hashim & Jones, 2022).

The findings of this study reinforce the argument that public governance must transition from fragmented, technology-centric approaches to integrated governance models that combine legal, institutional, and technological dimensions (Baskerville & Siponen, 2002).

A critical insight is that long-term digital preservation is not a static technical function but a dynamic institutional capability, requiring continuous adaptation to technological change, regulatory evolution, and emerging threats (Borgman, 2015).

Furthermore, interoperability emerges as a central determinant of system sustainability. Without standardized formats, metadata schemas, and institutional coordination, digital preservation efforts risk fragmentation and eventual failure (Rosenthal et al., 2005).

From a policy perspective, European regulatory frameworks provide a coherent model for modernization:

- NIS2 emphasizes resilience, risk management, and accountability
- eIDAS ensures legal recognition of digital trust services
- ISO standards provide operational and technical guidance

Together, these frameworks support a transition toward evidence-based governance systems that prioritize both security and long-term validity.

This study contributes to the existing literature by proposing a multi-layered governance model that integrates:

1. Legal dimension – ensuring compliance and evidentiary validity
2. Institutional dimension – defining roles, responsibilities, and accountability
3. Technological dimension – implementing secure and interoperable systems
4. Preservation dimension – ensuring long-term usability and authenticity

This integrated model advances beyond traditional approaches by recognizing that information security and digital preservation are inherently interdependent domains.

Conclusions

Information security in public electronic document management should be conceptualized not as a fragmented set of technical safeguards, but as a comprehensive governance system that integrates legal frameworks, institutional capacity, organizational procedures, and advanced technological controls into a coherent and auditable structure (Baskerville & Siponen, 2002; Von Solms & Van Niekerk, 2013). This systemic perspective reflects the evolving nature of digital governance, where the protection of information assets is inseparable from broader issues of accountability, transparency, and administrative legitimacy.

A central finding of this study is that long-term digital preservation introduces a distinct and structurally complex risk profile, fundamentally different from short-term information security concerns. Unlike operational security, which focuses on preventing immediate threats, long-term preservation must ensure that electronic records retain their evidentiary value despite continuous technological change, including software obsolescence, format degradation, and cryptographic evolution (Borgman, 2015; Rosenthal et al., 2005). This explains why many legal systems require additional safeguards—such as redundancy mechanisms, format migration strategies, and, in some cases, parallel paper-based retention—for records intended to be preserved beyond a decade.

Empirical evidence further reinforces the urgency of adopting integrated governance approaches. Cyber risk reporting consistently demonstrates that public administration is among the most targeted sectors globally, with increasing exposure to ransomware, distributed denial-of-service (DDoS) attacks, and insider threats (ENISA, 2025; Verizon, 2025). Moreover, the economic impact of such incidents—illustrated by the rising global cost of data breaches—highlights that information security failures have systemic financial, legal, and reputational consequences, rather than merely technical implications (IBM Security, 2024). Consequently, disruption and extortion risks should be treated not as exceptional events but as structural constraints on the reliability of e-government systems (Behl et al., 2022).

In this context, international standards and European regulatory frameworks provide a coherent and actionable pathway for modernization. The NIS2 Directive strengthens governance accountability, risk management, and resilience across critical sectors, emphasizing the need for proactive and systemic cybersecurity strategies. The eIDAS framework ensures the legal recognition and interoperability of digital trust services—such as electronic signatures, seals, and timestamps—which are essential for maintaining the authenticity and integrity of electronic documents over time. Complementarily, ISO standards (e.g., ISO/IEC 27001, ISO 15489-1) and the OAIS reference model (ISO 14721) offer operationally implementable architectures for managing information security and long-term preservation in an integrated manner (Hashim & Jones, 2022).

The study also provides a critical evaluation of emerging technologies, particularly blockchain. While distributed ledger technologies can enhance transparency, traceability, and integrity in registry-based systems, their applicability in long-term archival preservation remains limited due to challenges related to scalability, governance, legal admissibility, and cryptographic sustainability (Kshetri, 2017; Lemieux, 2016). Therefore, blockchain should be understood as a complementary integrity mechanism, rather than a standalone solution for long-horizon preservation. A more viable approach lies in hybrid architectures that combine trusted digital repositories with supplementary integrity verification mechanisms.

Ultimately, the findings of this research underscore that sustainable digital governance depends on the ability to ensure that electronic records remain authentic, accessible, secure, and legally valid across time. Achieving this objective requires continuous institutional commitment, alignment with international standards, and the development of interoperable, resilient, and audit-ready systems. In this sense, information security and digital preservation are not merely technical challenges, but foundational pillars of modern public administration and democratic governance.

Funding

The authors declare that no financial support was received for the research, authorship, and/or publication of this article. The study was conducted independently and without external funding.

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. No competing interests have influenced the design, execution, or interpretation of the study.

Artificial Intelligence Use Statement

The authors confirm that no generative artificial intelligence tools were used in the conceptualization, analysis, or writing of this manuscript. All intellectual contributions, interpretations, and conclusions are solely those of the author(s).

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. European Commission. (n.d.). *NIS2 Directive: Securing network and information systems*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
4. 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
5. ENISA. (2025, November 6). *Public administration increasingly targeted by DDoS attacks*. https://www.enisa.europa.eu/news/public-administration-increasingly-targeted-by-ddos-attacks
6. 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
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. International Organization for Standardization. (2012). *ISO 14721:2012 – Open archival information system (OAIS): Reference model*. https://www.iso.org/standard/57284.html
9. International Organization for Standardization. (2016). *ISO 15489-1:2016 – Records management: Concepts and principles*. https://www.iso.org/standard/62542.html
10. International Organization for Standardization. (2022a). *ISO/IEC 27001:2022 – Information security management systems*. https://www.iso.org/standard/27001
11. International Organization for Standardization. (2022b). *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* (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 document circulation: Law of Ukraine No. 851-IV (May 22, 2003)*. https://zakon.rada.gov.ua/go/851-15
15. Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305
16. Kshetri, N. (2017). 1 Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003
17. Behl, A., Jayawardena, N., Pereira, V., & Islam, N. (2022). Cybersecurity and cyberwar: What everyone needs to know. *Technological Forecasting and Social Change*, 175, 121306. https://doi.org/10.1016/j.techfore.2021.121306
18. Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud computing: Implementation, management, and security*. CRC Press.
19. Rosenthal, D. S. H., Robertson, T., Lipkis, T., Reich, V., & Morabito, S. (2005). Requirements for digital preservation systems: A bottom-up approach. *D-Lib Magazine*, 11(11). https://doi.org/10.1045/november2005-rosenthal
20. Pearce-Moses, R. (2005). *A glossary of archival and records terminology*. Society of American Archivists.
21. Lemieux, V. L. (2016). Trusting records: Is Blockchain technology the answer? *Records Management Journal*, 26(2), 110–139. https://doi.org/10.1108/RMJ-12-2015-0042
22. Hashim, N. L. M., & Jones, M. (2022). Digital preservation and sustainability: A review. *Journal of Cleaner Production*, 330, 129781. https://doi.org/10.1016/j.jclepro.2021.129781
23. AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575. https://doi.org/10.1016/j.chb.2015.03.054
24. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies. *Information & Management*, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

25. Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, 15(5/6), 337–346. https://doi.org/10.1108/09576050210447004
26. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004