Development of an Information Security Governance Framework in Fragmented Circumstances

Maksim Iavich[1,2], Vladimer Svanadze[1,2] and Ketevani Grdzelidze[2]

[1]*Caucasus University, 1 Paata Saakadze St, Tbilisi, Georgia, 0102*
[2]*Scientific Cyber Security Association, 9b Kipshidze, Tbilisi, Georgia, 0162*

Abstract

The transition from a seamless global internet to a fragmented "Splinternet" poses a fundamental challenge to organizations operating under different legislations and on various markets. While ISO/IEC 27001 and NIST Cyber Security Framework 2.0 provide robust frameworks for information security and governance within the organization, they largely assume a uniform operating environment and lack of specific mechanics for navigating contradictory geopolitical, technical and regulatory mandates. This paper proposes the adoption of R-A-I-T-M (Regulatory Assessment, Align, Implement, Train, Monitor) framework as an overlay for inclusion of fragmentation risks. By mapping RAITM's five adaptive phases to the functions of already existing frameworks, we demonstrate a modular governance model that enables transnational organizations to maintain global interoperability while adhering to local sovereignty requirements. The paper concludes that RAITM provides the necessary toolkit for "Sovereign Resilience", transforming cybersecurity from a compliance exercise into a dynamic response to the four main drivers of internet fragmentation.

Keywords

Internet Fragmentation; Information Security Governance; Cyber Security; RAITM Framework; IS Framework

1. Introduction

The basic and foundational principle of the Internet has always been its openness and interoperability. Consequently, cyber- and information security governance frameworks have always assumed a flat, borderless network at the core of their operations. Internationally acknowledged and applied standards, such as ISO/IEC 27001 and NIST CSF 2.0, were designed with the assumption that standards and frameworks designed in one corner of the world would be applicable anywhere else. I.E., the system and security control developed and implemented in Berlin would identically function in Washington or Sydney.

While ISO/IEC 27001 and NIST CSF 2.0 provide robust foundations for internal security governance, they operate under an implicit assumption of a unified global digital environment. This paper identifies a critical gap: these frameworks lack structured mechanisms to address the geopolitical and regulatory fragmentation increasingly defining today's digital landscape. The proposed RAITM framework is designed to fill this gap by providing a cyclical, adaptive overlay that integrates external fragmentation risks into core governance processes.

IVUS 2026: Information Society and University Studies 2026, May 12, Kaunas, Lithuania

miavich@cu.edu.ge (M. Iavich); vsvanadze@cu.edu.ge (V. Svanadze); k.grdzelidze@gmail.com (K. Grdzelidze)

Copyright © 2026 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-06

CEUR-WS.org/Vol-4317/paper6.pdf

Yet, during the past decade, the internet has been exposed to processes that threaten its universality and interoperability. The research has identified four main drivers for internet fragmentation:

1. Geopolitical Driver (i.e. State sovereignty and national security);
2. Regulatory Driver (legislative divergence);
3. Economic/commercial Driver (private corporations creating closed ecosystems, "Walled Garden" effect);
4. Technical Driver (splintering of the underlying logical infrastructure of the internet) [1].

Due to varying causes of fragmentation, as well as complex regulatory environments, companies operating or aspiring to operate in various markets face difficulty in developing a coherent aUSnd comprehensive IS governance framework, which would enable overall management of information systems, without creating the so-called "Walled Gardens" and isolating them from the internet. Transnational organizations must adhere to global standards (ISO/NIST) to maintain trust and a high level of security, yet strict adherence to a single global policy and approach often violates local sovereignty and data processing laws (such as GDPR, CSL in China, etc.). Conversely, hyper-localization creates smaller parts and fragments within the organization and leaves it vulnerable to regional threats.

Within the present research, we propose the implementation of the RAITM Framework comprising of five components:

1. Regulatory Assessment;
2. Alignment;
3. Implementation;
4. Training'
5. Monitoring. The framework will serve as a "middleware" between strict requirements of ISO/NIST frameworks and turbulent reality of fragmented internet.

2. Writing Policies in Fragmented Environment

National governments and regional institutions are increasingly attempting to assert control over their "national cyberspace". For decades now, cyberspace has been considered a fifth domain for national security, alongside land, sea, air, and space. Consequently, ensuring security and asserting power over cyberspace has become a cornerstone for many nation-states and international organizations. Internet fragmentation on any level can be divided into four main categories: governmental fragmentation, commercial fragmentation, technical fragmentation, and legal fragmentation. All these types of fragmentation are often intertwined in the process of the establishment of national sovereignty.

For example, the US-based companies face immense difficulties in adapting their operational philosophy to the EU's legislation. The US philosophy towards the practices of how to retain, transfer, and collect data is more global, free-flowing. At the same time, the European Union under GDPR has a more rights-based, strict approach towards data protection. Consequently, the US and EU systems were designed with conflicting priorities for data. This renders US systems inherently incompatible with the GDPR's demands without significant re-engineering of their data protection and data-processing practices, as well as policies thereof [2].

Historically, the US regulatory environment prioritizes data liquidity and open innovation, and it is primarily viewed as a commercial asset or commodity, i.e., under the company's ownership and disposal. Consequently, the companies are able to train algorithms, monetize on the data analysis, etc. In addition, companies are able to retain and collect more data than is immediately necessary. In this regard, the approach is to have data in case of necessity and its future value.

Contrary to this, GDPR requires personal data to be treated as a human right and the architecture of any data-processing system to be based on the principle of privacy by design and data minimization. Privacy by design requires companies to build their systems from the ground up with data protection principles embedded in them. Data minimization ensures that companies retain only the data that is necessary for their operation, and the purposes for any process should be clearly identified.

3. Writing Policies in Fragmented Environments

As mentioned above, increasing fragmentation significantly affects the adaptability of internal governance frameworks and companies' ability to enter new markets and leverage the global reach of the internet. In this regard, the development of internal policies and system management networks becomes more than an issue of compliance; it becomes a strategic instrument that allows companies to ensure alignment with regulatory obligations, operational resilience, and organizational values. The process of writing, adopting, and implementing information policies must be able to anticipate multiple, often conflicting, regulatory regimes and technical standards. Such environments demand that organizations design policies capable of withstanding disruption, supporting cross-border operations, and preserving the principles of openness and interoperability. Consequently, fragmentation generates a multidimensional policy challenge [3]. On one side, organizations must comply with local regulations governing data storage, transfer, and encryption, while at the same time, they must safeguard their operational continuity across various regions, even when access to the platform or services is suddenly restricted. In this regard, the rapid emergence of digital sovereignty agendas, localization rules, and regional data protection frameworks underscores the urgency of coherent, consistent policies. In a world where the legal and technical foundations of connectivity are increasingly jurisdiction-bound, the policies guiding digital operations must remain dynamic, layered, and contextually adaptable [3].

In modern multinational corporations, policy design has evolved from a documentation exercise to a complex governance process involving cross-functional teams of legal experts, technologists, information security specialists, and risk managers. Policy writing in fragmented environments can therefore be described as “policy engineering” – a deliberate and systematic act of designing adaptable governance mechanisms that integrate various technical standards, legislative requirements, and ethical norms. This approach requires the organization to think beyond compliance toward a strategic synthesis of resilience, interoperability, and trust. Emerging practices such as compliance-as-code and automated monitoring of regulatory changes further redefine how governance operates across jurisdictions [4].

4. Policy Design Principles

Effective policy developments in fragmented environments rest on three interdependent principles: (1) resilience; (2) compliance; (3) adaptability. These principles cannot be applied and analyzed separately from each other; rather, they create a unified system that allows organizations to respond proportionally to shifting risks and ever-changing regulatory demands [5].

Resilience refers to an organization's ability to maintain essential operations despite disruption, which requires: (1) more than redundant technical systems; (2) governance mechanisms that integrate business continuity plans (BCP), crisis communication; (3) multi-jurisdictional risk assessment. For example, global service providers need to plan for restrictions on access to regional cloud systems or disruption of content delivery networks due to geopolitical disputes. Consequently, policies must include fallback communication mechanisms, mirrored infrastructure strategies, and pre-defined decision pathways for rerouting data or services.

Resilience should also extend to information and human resources management. In this regard, regular “resilience drills”, where communication and operational continuity are tested under simulated isolation scenarios, can help ensure that policies are not only written but they are operational and executable. This anticipatory posture allows organizations to respond effectively to unpredictable fragmentation events such as sanctions, censorship, or technical shutdowns.

Compliance should be conceptualized as a form of strategic alignment rather than a restrictive instrument for transnational companies. Compliance frameworks that are transparent and proactive not only mitigate legal exposure but also enhance institutional legitimacy and stakeholder trust. It is vital for the compliance framework to extend beyond traditional audit procedures and encompass ethical data

handling, cross-border accountability, and human rights considerations across the complete platform and representations.

In this sense, compliance becomes a multidimensional value – connecting legality, ethics, and corporate reputation with each other. The organizations that demonstrate visible commitment to privacy, transparency, and user autonomy are more likely to gain the trust of both users and regulators. A proactive compliance posture can thus serve as a competitive differentiator rather than a mere defensive measure.

This approach to compliance allows companies to balance national obligations with universal values such as privacy and freedom of expression. Adaptability ensures that policies remain relevant amid changing legislative and regulatory requirements and technological developments. Static or overly strict documentation will not allow for the necessary flexibility towards increasing fragmentation and emerging isolation processes. Adaptive policy models incorporate modularity, allowing organizations to update individual clauses or appendices without reauthoring entire documents. Moreover, adaptability depends on strong feedback mechanisms between policy writers, legal experts, and operational staff, ensuring that lessons learned from practice directly inform periodic revisions.

In practice, the three principles – Resilience, Compliance, and Adaptability – form a continuous improvement cycle, referred to here as the RCA model. Similar to quality management systems or information security management frameworks, the RCA model ensures that every iteration of policy design builds on the insights and failures of previous implementations. This cyclical approach transforms policy from a static artifact into a living governance instrument.

Together, these principles enable organizations to construct a policy architecture that is resilient, responsive, and rooted in shared ethical and legal commitments (see Figure 1).

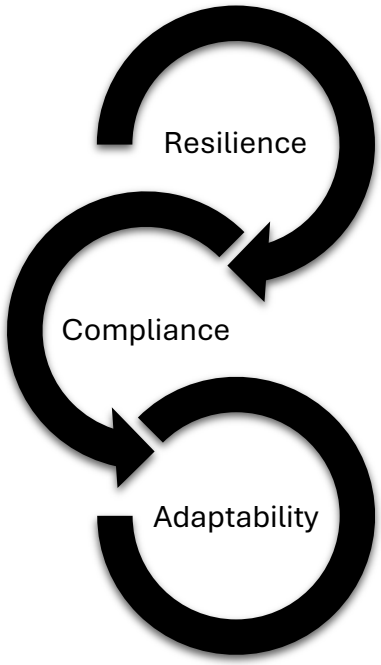


Figure 1: The RCA Model (Resilience-Compliance-Adaptability) – a continuous governance loop for managing fragmentation across jurisdictions.

The exact structure of policy development and framework will vary depending on the type, scale, and field of operation of the organization. Yet, there are four core domains that should be taken into consideration for the management of the fragmentation and overcoming the consequent challenges:

communication continuity, data governance, security controls, and compliance monitoring. In addition, data governance remains an "Achilles heel" of digital policy in a fragmented environment [3]. As mentioned above, changing localization rules and data management regulations creates tension between operational efficiency and legal compliance. Policies should provide a detailed framework for categorizing data by sensitivity and geographic relevance, ensuring that localization requirements are met without compromising global analytics or AI-driven insights.

Furthermore, governance policies should extend beyond compliance to include principles of data ethics, algorithmic transparency, and fairness. In fragmented environments, AI models trained on region-specific data may inherit localized biases. Therefore, organizations must implement ethical review procedures and fairness audits to ensure responsible data processing in line with regional laws. This integration of ethics into governance creates a foundation for trust and social legitimacy in an increasingly divided internet landscape [2].

Policies should outline clear responsibilities for identifying and reporting non-compliance, as well as escalation procedures that connect local compliance teams with corporate governance boards. Regular reporting cycles, supported by data-driven dashboards, help organizations anticipate regulatory changes rather than merely react to them. In addition, transparency reports can serve as an external instrument of accountability, demonstrating good faith compliance even in contested environments.

5. Practical Framework for Organizations

To translate these principles into operational practice, organizations require a structured methodology that links strategic foresight, governance mechanisms, and technical execution. The framework we propose in this paper is a R-A-I-T-M framework – comprising the phases Regulatory Assessment (Risk), Align, Implement, Train, and Monitor (see Figure 2). Rather than a linear model, R-A-I-T-M is designed as a continuous governance cycle that facilitates iterative adaptation to regulatory and geopolitical change. It functions as both a diagnostic and developmental mechanism through which organizations can transform regulatory uncertainty into structured adaptability. Each phase is analytically distinct yet operationally interdependent, creating an iterative loop of evaluation, execution, and refinement.

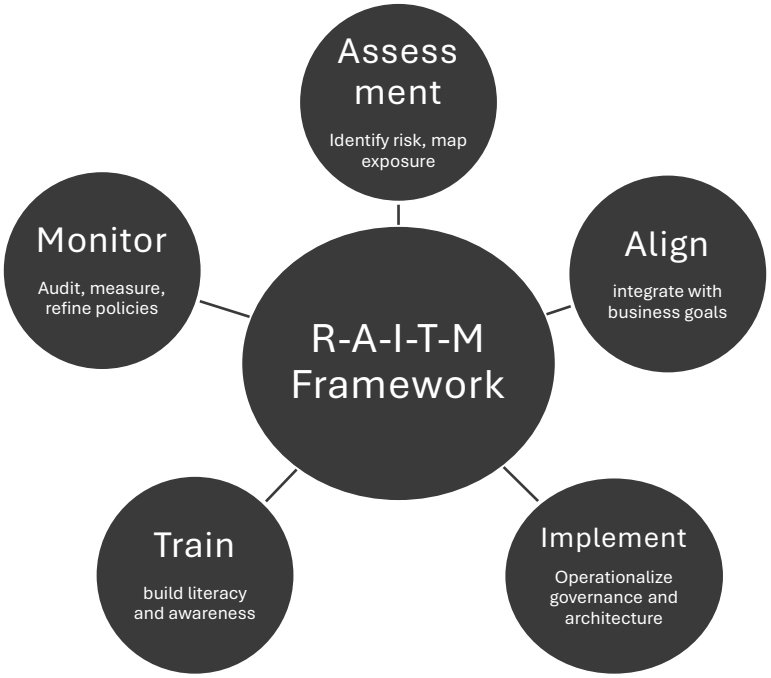


Figure 2: R-A-I-T-M conceptual model for policy development in fragmented digital environments.

For example, a multinational cloud provider might apply RAITM to navigate conflicting data residency laws between the EU (GDPR) and China (CSL). In the Assessment phase, it would map data flows and legal obligations in each region. Alignment would involve developing a dual-architecture strategy, separating EU and China data processing modules. Implementation would see the deployment of region-specific encryption and access controls. Training would ensure local and global teams understand sovereignty-sensitive workflows, and Monitoring would use compliance dashboards to track adherence to both regimes in real-time, triggering adjustments as laws evolve.

The RAITM framework operates not as a linear checklist but as a dynamic governance cycle, where each phase informs and reinforces the next. This can be conceptually expressed as:

$$\text{Sovereign Resilience} = [(\text{Assessment} \oplus \text{Alignment})] \rightarrow [(\text{Implementation} \otimes \text{Training})] \rightarrow \text{Monitoring}^*$$

- Where:
- $\oplus$ denotes integration of risk insight with strategic goals,
- $\otimes$ represents embedding of governance into both technology and culture,
- $\rightarrow$ indicates sequential yet iterative progression,
- Monitoring^* reflects continuous feedback that renews the cycle.

This formulation underscores that resilience in fragmented environments emerges from the interaction of structured analysis, aligned execution, and perpetual adaptation — not from static compliance alone.

The assessment phase is the foundation of the governance process, as it allows to depict the full risk and regulatory environment of the organization. Before any policy intervention can be launched, organizations must first develop an accurate understanding of the multidimensional risk landscape in which they operate. Following the assessment, the alignment phase translated empirical knowledge into organizational purpose. Alignment is where compliance ceases to be reactive and becomes strategic. The primary aim is to ensure that digital governance objectives align with business goals, ethical commitments, and stakeholder expectations. To achieve alignment, organizations must embed governance considerations directly in their corporate strategy. Instead of treating regulatory conformity as an external imposition, alignment reframes it as an internal value-creation process. The implementation phase entails the transition from mere policy formulation to material practice. It is a stage where governance ceases to be an abstract concept and is translated into infrastructural solutions. Implementation requires the institutionalization of accountability and the technological embedding of compliance within organizational systems. An essential component of implementation is the creation of governance architecture, which will be a coherent structure of roles, responsibilities, and workflows that ensures the consistent execution of policies. Technically, implementation benefits from modularization, i.e., decomposition of IT systems into discrete components that can be independently adapted to jurisdictional requirements. For example, encryption modules may be swapped out to meet national

certification standards without altering the organization's entire infrastructure. This modular approach not only enhances compliance agility but also reduces systemic risk by localizing potential points of failure. The training phase is essential to the internalization of policies and procedures by the individuals who enact them. Training must move beyond mere procedural instruction. Effective capacity-building programs address the reasoning behind compliance. Employees need to understand how their specific actions, such as data handling, configuration systems, and communication across jurisdictions, contribute to the organization's overall governance posture. This requires teaching strategies that combine conceptual instruction with experimental learning. Simulation exercises, tabletop scenarios, and interactive workshops will play a vital role in allowing employees to experience the practical consequences of policy breaches or regulatory changes. Such methods will foster the ability to anticipate and interpret governance challenges as part of daily decision-making. The monitoring phase represents the dynamic conclusion of the R-A-I-T-M cycle and its immediate renewal. In fragmented digital ecosystems, where regulatory conditions evolve rapidly, static compliance is functionally obsolete. Effective and continuous monitoring entails technical oversight and regulatory intelligence. On the technical side, organizations must deploy continuous auditing mechanisms, such as log analytics, anomaly detection, and configuration drift monitoring. Integration of Security Information and Event Management Systems (SIEM), governance dashboards, and data-loss-prevention (DLP) tools allows for comprehensive visibility across various platforms, integrations, and the organization in general. These instruments transform compliance data into actionable intelligence.

The R-A-I-T-M framework complements existing frameworks for information security governance and serves as a go-between between ISO/IEC 27001, NIST CSF 2.0 requirements and the need to comply with a fragmented framework.

Namely, ISO/IEC 27001 remains a "gold standard" for information security management systems. However, its strength – standardization is its weakness in a fragmented world. Clause 4 (Context of the Organization) requires understanding external issues, but traditional interpretations rarely account for geopolitical fragmentation as a technical constraint. At the same time, the newer version of the NIST Cybersecurity Framework, in addition to traditional domains (Identify, Protect, Detect, Respond, Recover), creates a "strategic" umbrella that mandates cybersecurity be integrated into the broader risk management process. However, similarly to ISO, NIST lacks a "geopolitical approach". These are where the R-A-I-T-M framework complements the process [6-8]. The correlation between components of ISO/IEC 27001, NIST Cyber Security Framework 2.0, and R-A-I-T-M framework in connection to RCA logic is outlined in Table 1.

Table 1
Correlation of NIST CSF 2.0, ISO/IEC 27001 and R-A-I-T-M Framework in connection with RCA logic.

RCA Logic/Framework	NIST CSF 2.0	ISO/IEC 27001	R-A-I-T-M Framework
Resilience	Protect, Detect, Recover	Clause 8, Annex A, BC & Availability Controls	Implement/Monitor
Compliance	Govern	Clauses 4-6 (Context, Leadership, Planning)	Assess/Align/Train
Adaptability	Respond, Recover	Clause 9-10 (Evaluation & Improvement)	Monitor -> Adjust

In summary, the R-A-I-T-M framework provides a holistic framework for organizations to navigate the complex interplay among regulatory fragmentation, technical uncertainty, and ethical responsibility. Its strength lies not in a prescriptive rigidity but in procedural dynamism: assessment generates knowledge, alignment contextualizes it, implementation operationalizes it, training socializes it, and monitoring revitalizes it. Together, these stages form a continuous governance ecology, one that transforms uncertainty into structured resilience [9,10]. By implementing this cyclical model into their organizational structures, institutions can ensure reactive compliance and move toward a principle-driven approach to digital sovereignty [4].

6. Conclusion

Global digital fragmentation presents a structural challenge to the stability and security of the internet. As states assert digital sovereignty through data localization laws, platform regulation, and various security standards, rigid, organization-centric policies can not be considered an effective instrument for adaptation. Transnational organizations face a paradox: on the one hand, they must comply with divergent legal systems, while on the other hand, they must maintain interoperability and coherence across the company. This tension redefines governance from a static exercise in compliance into a dynamic process of negotiation among technical, political, and ethical domains.

The analysis presented in the article demonstrates that an effective organizational governance structure in such an environment cannot rely on traditional policy development and implementation paradigms rooted in centralized authority. Organizations must adopt an adaptive architecture that is capable of maintaining operational continuity despite constant disruptions. The proposed R-A-I-T-M framework (Regulatory Assessment (Risks), Align, Implement, Train, Monitor) offers a structured, yet flexible methodology for achieving this balance. By combining empirical assessment, strategic integration, infrastructural execution, cultural reinforcement, and continuous feedback, the model translates abstract principles of resilience and openness into repeatable operational practice.

The framework also challenges the dominant reflex in corporations to build closed, self-contained ecosystems or “walled gardens”. While such enclosures may appear to offer immediate control and simplified compliance, they erode the foundation of the global internet by restricting interoperability, diminishing user agency, and concentrating informational power. Openness and adherence to shared standards foster trust, transparency, and cross-jurisdictional collaboration. They transform governance from unilateral control to multilateral coordination. Organizations that embrace openness are more likely to maintain regulatory goodwill, attract cooperative partners, and sustain innovation capacity in volatile geopolitical conditions. Furthermore, the discussion underscores that policy resilience is not solely a technical or legal undertaking, but an ethical one. Policies that integrate inclusivity, transparency, and accountability do not merely satisfy regulatory requirements – they reinforce the organization's legitimacy in the digital public sphere. The balance between sovereignty and universality, control and openness, must therefore be pursued not as a compromise but as an operational principle guiding every layer of governance. The RAITM framework's primary limitation lies in its requirement for organizational maturity—including cross-functional collaboration, executive buy-in, and investment in adaptive technologies—which may pose challenges for smaller enterprises or those in early stages of digital governance. Future research should focus on empirical validation of RAITM through sector-

specific case studies (e.g., finance, healthcare) and the development of lightweight implementations for resource-constrained organizations

In conclusion, the future of digital governance will not be determined by any single regulatory order or technological platform, but a comprehensive, collective ability to write policies that are resilient, interoperable, and principled [1,4]. In this regard, the capacity of the proposed R-A-I-T-M framework positions policy as a living process comprised of continuous informed assessment, enacted through technology, sustained by human understanding and reformed through monitoring.

7. Acknowledgements

This research is funded by the Internet Corporation for Assigned Names and Numbers (ICANN) through the ICANN Grant Program. The views and opinions expressed in this research are those of the author(s) and do not reflect the official policy or position of ICANN.

8. Declaration on Generative AI

The authors have not employed any Generative AI tools.

9. References

[1] R. Radu, G. De. Gregorio. The New Era of Internet Governance, in: Cristiano F., Van Deb Berd B. (eds), Hybridity, Conflict, and the Global Politics of Cybersecurity, 1st. ed, Lanham: Rowman & Littlefield, Leiden, The Netherlands, (2025) 15-30. https://doi.org/10.5040/9798881813529.ch-2

[2] L. Magnusson, S. Iqbal, P. Elm, F. Dalipi, Information security governance in the public sector: investigations, approaches, measures, and trends, International Journal of Information Security (2025). https://doi.org/10.1007/s10207-025-01097-x.

[3] V. Svanadze, M. Iavich, Impact of Internet Fragmentation on the Unity, Security and Stability of Global Internet. In: Proceedings of the 4th. International Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CEUR-WS.org, Bratislava, Slovakia, 2024, pp.520-525, https://ceur-ws.org/Vol-3654/short23.pdf.

[4] M. Mayer, P. K. Nock, Digital fragmentations, technological sovereignty and new perspectives on the global digital economy, Global Political Economy, (2025), https://doi.org/10.1332/26352257Y2024D000000029.

[5] J.C. Morse, Information Fragmentation and Global Governance in Hard Times, Ethics & International Affairs (2025) 159-172, doi:10.1017/S0892679425100130.

[6] D. F. Tanjung, O.D. Nurhayati, A. Wibolo, Design Information Security in Electronic-Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001:2022 and CIS Control, International Journal of Innovative Science and Research Technology (IJISRT) (2024) 523-530, https://doi.org/10.38124/ijisrt/IJISRT24JUN1212.

[7] J.S. Holtrop, P.A. Estabrooks, B. Gaglio, S.M. Harden, R.S. Kessler, D.K. King, B.M. Kwan, M.G. Ory, B.A. Rabin, R.C. Shelton, R.E. Glasgow, Understanding and applying the RE-AIM framework:

clarifications and resources, Journal of clinical and translational science, 5.1:e126 (2021). https://doi.org/10.1017/cts.2021.789.

[8] M.P. Jolles, M.P. Fort, R.E. Glasgow, Aligning the planning, development, and implementation of complex interventions to local contexts with an equity focus: application of the PRISM/RE-AIM Framework, International Journal for Quity in Health, 23.1:41 (2024). doi:10.1186/s12939-024-02130-6.

[9] D. Tang, J. Li, Z. Zhao, V. Boamah, D.D. Lansana, The influence of industrial structure transformation on urban resilience based on 110 prefecture-level cities in the Yangtze River, Sustainable Cities and Society, 96 (2023). https://doi.org/10.1016/j.scs.2023.104621.

[10] Y. Yuan, H. Tan, L. Liu, The effects of digital transformation on supply chain resilience: a moderated and mediated model, Journal of Enterprise Information Management, 37.2 (2024) 488-510, https://doi.org/10.1108/JEIM-09-2022-0333.