Journal of Cyber Law and Information Security
Volume 4, Number 2, 2025

Legal Effectiveness of Data Protection and Cybersecurity Frameworks in Indonesia: The Enforcement and Compliance Gap

Subur Gunawan [1]

[1] Program Pascasarjana Universitas Putra Bangsa, Kebumen, Indonesia

Abstract

Article history:
Received: July 27, 2025
Revised: September 3, 2025
Accepted: October 24, 2025
Published: December 30, 2025

Keywords:
compliance,
cybersecurity governance,
data protection law,
digital governance,
enforcement,
legal effectiveness.

Identifier:
Zera Open
Page: 116-138
https://zeraopen.com/journal/jclis

The effectiveness of data protection and cybersecurity legal frameworks has become a critical issue in digital governance, particularly in developing countries such as Indonesia. Although regulatory instruments such as the Personal Data Protection Law and the Electronic Information and Transactions Law provide a formal legal foundation, their practical effectiveness remains limited. This study examines how these frameworks address digital risks and analyzes the urgency of strengthening enforcement and compliance mechanisms. Using a normative juridical method combined with systematic and sociological approaches, the study evaluates the relationship between legal norms and their implementation. The findings indicate that regulatory frameworks exist but fail to achieve optimal effectiveness due to weak enforcement, low compliance, and institutional fragmentation. This condition creates a persistent gap between legal objectives and actual outcomes, allowing cybersecurity risks and data breaches to continue. Strengthening enforcement capacity, improving institutional coordination, and enhancing compliance mechanisms are therefore essential to ensure effective cybersecurity governance in Indonesia.

*Corresponding author:
(Subur Gunawan)

©2025 The Author(s).
This is an open-access article under CC-BY-SA license (https://creativecommons.org/licence/by-sa/4.0/)

1. Introduction

The rapid expansion of digital technologies has fundamentally transformed governance structures, placing data protection and cybersecurity at the center of contemporary legal systems. Legal frameworks governing personal data and digital transactions are increasingly recognized as essential instruments for safeguarding privacy, ensuring trust, and maintaining the integrity of digital ecosystems. In this context, the effectiveness of data protection law is not determined solely by its formal existence, but by its capacity to regulate behavior and prevent harm in practice. Lynskey (2023) emphasizes that effective data protection requires not only comprehensive legal norms but also institutional mechanisms capable of enforcing compliance. Similarly, Wacks (2021) argues that the legitimacy of legal systems depends on their ability to translate normative principles into real-world outcomes. This indicates that the relationship between law and effectiveness is inherently dependent on enforcement and compliance dynamics rather than mere legislative presence.

The development of cybersecurity and data protection regulations reflects a broader shift toward digital governance, where states seek to manage risks associated with data misuse, cyber threats, and technological innovation. Regulatory frameworks have expanded significantly to address these challenges, incorporating legal, institutional, and policy instruments designed to ensure security and accountability. Savaş and Karataş (2022) highlight that cybersecurity governance involves the coordination of legal and institutional arrangements to mitigate digital risks. Similarly, Bechara and Schuch (2021) argue that global regulatory efforts

increasingly emphasize the need for coherent cybersecurity frameworks to address transnational threats. However, the proliferation of regulations does not automatically guarantee their effectiveness. This suggests that the existence of legal frameworks must be critically examined in relation to their implementation and enforcement capacity.

Despite the growing sophistication of data protection and cybersecurity laws, empirical studies indicate persistent gaps between regulatory design and practical outcomes. Bachňáková et al. (2024) demonstrate that even well-developed legal frameworks, such as the GDPR, face significant enforcement challenges that limit their effectiveness. Malik et al. (2025) further emphasize that developing countries encounter structural constraints, including limited institutional capacity and regulatory fragmentation, which undermine the implementation of data protection laws. These findings suggest that legal effectiveness is constrained by systemic factors that extend beyond the content of legislation. As a result, regulatory frameworks may exist in a formal sense but fail to achieve their intended protective function. This highlights the need to analyze legal systems not only in terms of their design but also in terms of their operational realities.

In the Indonesian context, the enactment of Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi and Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik reflects a significant effort to establish a comprehensive legal framework for data protection and cybersecurity. These regulations provide formal legal foundations for governing personal data processing, digital transactions, and cyber-related activities. However, existing

studies indicate that the implementation of these frameworks remains limited due to institutional and regulatory challenges. Razi and Markus (2024) highlight that enforcement mechanisms for data protection in Indonesia are still developing and often lack coordination. Similarly, Syailendra et al. (2024) emphasize that regulatory ambiguity and institutional fragmentation hinder effective implementation. This suggests that Indonesia's legal framework, while formally established, has not yet achieved full effectiveness in addressing digital risks.

The persistence of enforcement and compliance challenges reflects a broader theoretical issue concerning the gap between "law in books" and "law in action." Puaschunder (2022) argues that legal systems often exhibit discrepancies between normative expectations and actual enforcement outcomes, particularly in complex regulatory environments. This perspective is particularly relevant in the context of digital governance, where rapid technological change outpaces institutional adaptation. As a result, legal frameworks may fail to produce effective regulatory outcomes despite their formal comprehensiveness. This gap underscores the importance of examining not only the existence of laws but also the conditions under which they are enforced and complied with. Consequently, legal effectiveness must be understood as a function of both normative design and institutional performance.

Based on these considerations, this study aims to analyze the effectiveness of data protection and cybersecurity legal frameworks in addressing digital risks in Indonesia and to examine the urgency of strengthening enforcement and compliance to improve cybersecurity governance. Using a normative juridical method combined with systematic and sociological approaches, the study evaluates the relationship

between regulatory frameworks and their implementation in practice. The analysis focuses on identifying the structural factors that limit legal effectiveness, particularly in relation to enforcement capacity and compliance behavior. By addressing these issues, the study contributes to a deeper understanding of the governance challenges underlying digital regulation in Indonesia. Furthermore, it provides policy-relevant insights into how legal frameworks can be strengthened to achieve more effective and coherent cybersecurity governance. Through this approach, the study aligns with broader efforts to enhance the role of law in managing digital transformation and mitigating cyber risks.

2. Literature Review

The concept of legal effectiveness in data protection has increasingly been understood as the ability of regulatory frameworks to translate normative principles into actual behavioral compliance and risk mitigation outcomes. Rather than focusing solely on the existence of legal provisions, recent scholarship emphasizes the importance of enforcement mechanisms and institutional capacity in determining whether data protection laws achieve their intended objectives. Lynskey (2023) argues that data protection regimes must be assessed based on their capacity to ensure substantive protection rather than formal compliance alone. Similarly, Bachňáková et al. (2024) demonstrate that even robust regulatory frameworks such as the GDPR encounter limitations in enforcement, particularly when supervisory authorities face resource and coordination constraints. Malik et al. (2025) further highlight that in developing countries, structural challenges such as fragmented

institutions and limited regulatory capacity significantly reduce the effectiveness of data protection laws. These perspectives indicate that legal effectiveness is contingent upon the interaction between regulatory design and enforcement capability, rather than the comprehensiveness of legislation alone.

In parallel, cybersecurity regulation has evolved as a critical component of digital governance, reflecting the need to address risks associated with cyber threats and data vulnerabilities. Cybersecurity governance is typically conceptualized as a system of legal, institutional, and policy arrangements designed to manage digital risks through coordinated action. Savaş and Karataş (2022) emphasize that effective cybersecurity governance requires the integration of legal frameworks with institutional coordination mechanisms. Similarly, Bechara and Schuch (2021) argue that global cybersecurity regulation faces challenges due to the transnational nature of cyber threats, which complicates enforcement and regulatory consistency. Kumar et al. (2024) further note that cybersecurity laws often struggle to achieve effectiveness when enforcement mechanisms are weak or inadequately aligned with institutional capacities. These findings suggest that cybersecurity regulation cannot be evaluated solely in terms of legal completeness, but must be analyzed in relation to governance structures and enforcement practices. Consequently, the effectiveness of cybersecurity law is closely linked to broader issues of regulatory governance and institutional coordination.

A central issue in assessing legal effectiveness is the problem of enforcement failure, which reflects the inability of regulatory systems to ensure compliance and implement legal norms effectively. Enforcement failure is often associated with

limited institutional capacity, weak regulatory oversight, and insufficient coordination among enforcement bodies. Andarge and Lichtenberg (2020) argue that regulatory compliance is highly dependent on the credibility and consistency of enforcement, and that gaps in enforcement significantly reduce the effectiveness of legal frameworks. Sumkoski et al. (2025) further highlight that regulatory weaknesses, including ambiguous authority and fragmented governance structures, contribute to ineffective enforcement outcomes. Rusydi (2024) emphasizes that cybersecurity legal frameworks often fail not because of inadequate laws, but because enforcement mechanisms are not sufficiently developed or operationalized. These perspectives indicate that enforcement failure is a structural issue that undermines the practical impact of legal systems. As a result, the presence of legal norms does not necessarily translate into effective governance outcomes when enforcement remains weak.

In addition to enforcement challenges, compliance behavior represents another critical dimension influencing the effectiveness of data protection and cybersecurity regulations. Compliance is shaped by organizational capacity, regulatory clarity, and the perceived legitimacy of legal frameworks. Lonzetta and Hayajneh (2021) highlight that organizations often struggle to comply with data protection laws due to complexity, resource constraints, and lack of clear guidance. Similarly, Oyetunji (2024) emphasizes that compliance challenges are frequently linked to insufficient awareness and weak institutional support mechanisms. Alkhamsi and Alqahtani (2024) further argue that the absence of structured compliance frameworks and monitoring systems reduces the ability of organizations

to adhere to regulatory requirements. These findings suggest that compliance is not merely a matter of legal obligation but is influenced by broader governance conditions. Therefore, ineffective compliance further reinforces the gap between regulatory intent and actual outcomes.

The Indonesian context provides a specific illustration of how enforcement and compliance challenges affect the effectiveness of data protection and cybersecurity frameworks. The introduction of the Personal Data Protection Law and the continued application of the Electronic Information and Transactions Law reflect significant regulatory progress in addressing digital risks. However, empirical studies indicate that implementation remains uneven and constrained by institutional limitations. Razi and Markus (2024) highlight that enforcement mechanisms in Indonesia are still evolving and lack sufficient coordination across regulatory bodies. Syailendra et al. (2024) further emphasize that legal ambiguity and institutional fragmentation hinder effective implementation of data protection regulations. Prasetyo et al. (2025) add that despite the presence of comprehensive legal frameworks, practical challenges such as limited resources and weak oversight reduce regulatory effectiveness. These findings indicate that Indonesia's regulatory environment reflects a broader pattern in which legal development outpaces enforcement and compliance capacity.

From a theoretical perspective, the gap between legal norms and their implementation can be understood through the distinction between "law in books" and "law in action," which highlights the divergence between formal legal frameworks and actual enforcement practices. Puaschunder (2022) argues that this

gap is particularly evident in complex regulatory environments where institutional capacity and behavioral factors influence legal outcomes. Wacks (2021) further emphasizes that legal systems must be evaluated not only based on their normative content but also on their ability to produce tangible effects in society. This theoretical framework provides a foundation for analyzing the effectiveness of data protection and cybersecurity laws in Indonesia. It suggests that the key issue is not the absence of regulation, but the failure to operationalize legal norms through effective enforcement and compliance mechanisms. Therefore, understanding legal effectiveness requires a holistic approach that integrates normative, institutional, and behavioral dimensions.

3. Methods

This study employs a normative juridical research method combined with systematic and sociological approaches to analyze the effectiveness of data protection and cybersecurity legal frameworks in Indonesia and to examine the urgency of strengthening enforcement and compliance mechanisms. The normative juridical approach is used to assess legal norms, statutory provisions, and regulatory frameworks governing data protection and cybersecurity, particularly those embodied in Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi and Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. This approach enables the identification of the formal legal structure and the intended regulatory objectives of these frameworks. However, as emphasized in legal theory, the existence of norms alone is insufficient to determine

effectiveness, as legal outcomes depend on their implementation in practice (Wacks, 2021). Therefore, this study extends beyond doctrinal analysis to incorporate broader evaluative dimensions. By doing so, it situates legal analysis within the context of governance performance and regulatory outcomes.

The systematic approach is applied to examine the internal coherence and interrelationship between different legal instruments and governance mechanisms within Indonesia's digital regulatory framework. This involves analyzing how data protection and cybersecurity regulations are structured, how responsibilities are distributed among institutions, and how regulatory provisions are intended to operate collectively. Such an approach is essential for identifying inconsistencies, overlaps, and gaps within the legal framework that may affect its effectiveness. As noted in regulatory governance literature, fragmented or poorly coordinated legal systems often lead to reduced enforcement capacity and inconsistent policy outcomes (Sumkoski et al., 2025). This indicates that legal effectiveness is influenced not only by the content of individual regulations but also by their systemic integration. Consequently, the systematic analysis allows this study to evaluate whether Indonesia's regulatory framework functions as a coherent system or as a collection of disconnected legal instruments.

In addition, a sociological approach is employed to assess how data protection and cybersecurity laws are implemented and experienced in practice, particularly in relation to enforcement and compliance behavior. This approach focuses on the interaction between legal norms, institutional actors, and regulated entities, thereby capturing the "law in action" dimension of legal effectiveness. Puaschunder (2022)

highlights that discrepancies between formal legal frameworks and their practical application are common in complex regulatory environments, especially when institutional capacity is limited. Similarly, Andarge and Lichtenberg (2020) emphasize that enforcement credibility and consistency play a decisive role in shaping compliance behavior. By incorporating a sociological perspective, this study is able to analyze how enforcement weaknesses and compliance challenges affect the actual performance of legal frameworks. This enables a more comprehensive understanding of the gap between regulatory intent and real-world outcomes.

The sources of legal materials used in this study consist of both primary and secondary materials selected based on relevance and academic credibility. Primary legal materials include national legislation governing data protection and cybersecurity, while secondary materials consist of peer-reviewed journal articles and scholarly works addressing legal effectiveness, enforcement, compliance, and digital governance. The selection of sources prioritizes recent and high-quality academic contributions to ensure analytical rigor and relevance. As highlighted in studies on compliance challenges, the integration of empirical and theoretical literature is essential for understanding the practical limitations of regulatory frameworks (Lonzetta & Hayajneh, 2021; Oyetunji, 2024). The analysis is conducted through qualitative legal interpretation using systematic reasoning and normative evaluation, supported by sociological insights into enforcement and compliance dynamics. This methodological combination allows the study to identify structural weaknesses in legal frameworks and to assess their implications for cybersecurity governance.

Through this integrated methodological design, the study is able to address both research questions by linking legal structure to governance outcomes. The normative analysis supports the evaluation of legal effectiveness (RQ1) by examining whether existing frameworks are capable of addressing digital risks. At the same time, the sociological and systematic approaches provide the basis for analyzing the urgency of strengthening enforcement and compliance (RQ2) by identifying the factors that limit regulatory performance. This combination ensures that the study does not remain confined to formal legal analysis but instead captures the broader governance context in which legal frameworks operate. As a result, the methodology enables a comprehensive and multi-dimensional assessment of data protection and cybersecurity regulation in Indonesia. It also provides a robust foundation for deriving normative and policy-relevant conclusions regarding the improvement of cybersecurity governance.

4. Results

4.1. Legal Effectiveness of Data Protection and Cybersecurity Frameworks

The findings indicate that Indonesia has established a formal legal framework for data protection and cybersecurity through instruments such as Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi and Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. These regulations provide a normative foundation for governing personal data processing, digital transactions, and cyber-related activities. From a legal perspective, such frameworks are designed to ensure accountability, define obligations, and mitigate

risks associated with digital systems. However, the existence of comprehensive legal provisions does not automatically guarantee their effectiveness in practice. Lynskey (2023) emphasizes that legal effectiveness depends on the ability of regulatory systems to ensure actual protection rather than merely formal compliance. Similarly, Prasetyo et al. (2025) highlight that Indonesia's data protection law reflects significant normative progress but still faces challenges in translating legal provisions into effective outcomes.

A critical limitation in the effectiveness of these frameworks lies in the gap between regulatory design and implementation. Although legal provisions establish obligations and institutional roles, their operationalization remains constrained by limited enforcement mechanisms and coordination challenges. Bachňáková et al. (2024) demonstrate that even mature regulatory systems experience enforcement limitations when institutional capacity is insufficient. In the Indonesian context, Razi and Markus (2024) emphasize that enforcement mechanisms are still evolving and lack institutional integration, leading to inconsistencies in regulatory application. This indicates that legal frameworks operate more effectively at the normative level than at the practical level. As a result, regulatory objectives are not consistently achieved across sectors and institutions. The effectiveness of the legal framework is therefore constrained by the inability to fully implement its provisions.

In addition to enforcement limitations, the effectiveness of data protection and cybersecurity frameworks is influenced by broader governance challenges, particularly the lack of coordination among institutions responsible for regulation and oversight. Cybersecurity governance requires the integration of legal frameworks

with institutional mechanisms capable of managing complex digital risks. Savaş and Karataş (2022) argue that effective cybersecurity governance depends on coordinated legal and institutional arrangements. Similarly, Bechara and Schuch (2021) highlight that fragmented governance structures reduce the ability of regulatory systems to respond effectively to cyber threats. In Indonesia, the absence of strong coordination mechanisms results in overlapping responsibilities and regulatory ambiguity. This fragmentation weakens the implementation of legal provisions and reduces the overall effectiveness of governance. Consequently, legal frameworks fail to function as cohesive systems capable of addressing digital risks comprehensively.

The limited effectiveness of legal frameworks is further reflected in their inability to prevent persistent data breaches and cybersecurity incidents. Malik et al. (2025) emphasize that structural constraints in developing countries, such as limited institutional capacity and regulatory fragmentation, undermine the protective function of data protection laws. Syailendra et al. (2024) similarly highlight that regulatory ambiguity and weak institutional arrangements contribute to ineffective implementation in Indonesia. These conditions create an environment in which legal obligations are not consistently enforced, and violations are not adequately deterred. As a result, data protection and cybersecurity risks continue to persist despite the existence of formal legal frameworks. This demonstrates that legal effectiveness is not determined solely by the presence of regulations, but by their capacity to produce tangible outcomes. Therefore, Indonesia's data protection and cybersecurity

frameworks can be considered formally comprehensive but practically limited in effectiveness

4.1. Urgency of Strengthening Enforcement and Compliance

The urgency of strengthening enforcement and compliance mechanisms arises from the structural weaknesses that limit the effectiveness of existing legal frameworks. Enforcement plays a central role in ensuring that legal norms are translated into actual behavior, and its absence significantly reduces regulatory impact. Andarge and Lichtenberg (2020) argue that compliance is highly dependent on the credibility and consistency of enforcement, as weak enforcement reduces incentives for adherence to legal obligations. Rusydi (2024) further emphasizes that cybersecurity legal frameworks often fail not due to inadequate laws, but because enforcement mechanisms are not sufficiently operationalized. These findings indicate that enforcement failure is a primary factor contributing to the persistence of cybersecurity risks. Without effective enforcement, legal frameworks remain largely symbolic rather than functional. This underscores the necessity of strengthening enforcement mechanisms to improve regulatory effectiveness.

Institutional weaknesses further reinforce the urgency of improving enforcement capacity within Indonesia's cybersecurity governance system. Effective enforcement requires clear institutional mandates, coordination among regulatory bodies, and adequate resources to monitor and sanction violations. Sumkoski et al. (2025) highlight that regulatory systems characterized by fragmented authority and weak coordination are less capable of enforcing legal norms effectively. Kumar et al. (2024) similarly emphasize that cybersecurity regulations often face implementation

challenges when institutional responsibilities are unclear or overlapping. In Indonesia, such institutional fragmentation limits the ability of authorities to enforce data protection and cybersecurity laws consistently. This results in uneven regulatory application and reduced deterrence of non-compliance. Therefore, strengthening institutional capacity and coordination is essential for improving enforcement effectiveness.

In addition to enforcement challenges, compliance behavior among regulated entities represents a critical factor influencing the overall effectiveness of legal frameworks. Compliance is shaped not only by legal obligations but also by organizational capacity, regulatory clarity, and enforcement expectations. Lonzetta and Hayajneh (2021) highlight that organizations frequently struggle to comply with data protection laws due to complexity and resource constraints. Oyetunji (2024) further emphasizes that limited awareness and insufficient institutional support contribute to low levels of compliance. These challenges are compounded when enforcement is weak, as organizations face fewer incentives to adhere to regulatory requirements. As a result, compliance becomes inconsistent and often superficial. This indicates that improving compliance requires both stronger enforcement and clearer regulatory guidance.

The combined effect of weak enforcement and low compliance creates systemic risks that undermine the effectiveness of cybersecurity governance. When legal frameworks are not effectively enforced and compliance remains limited, regulatory systems fail to achieve their protective objectives. Alkhamsi and Alqahtani (2024) argue that the absence of structured compliance frameworks and monitoring

mechanisms reduces the ability of organizations to meet regulatory standards. Prasetyo et al. (2025) further highlight that in Indonesia, these weaknesses contribute to ongoing vulnerabilities in data protection and cybersecurity. This creates a regulatory environment in which risks persist despite the presence of formal legal frameworks. Consequently, strengthening enforcement and compliance is not merely a regulatory improvement but an urgent necessity for effective governance. Addressing these issues is essential to ensure that legal frameworks can function as intended in mitigating digital risks.

5. Discussion

The findings of this study demonstrate that the primary limitation of data protection and cybersecurity frameworks in Indonesia does not lie in the absence of legal regulation, but in the structural inability of these frameworks to operate effectively within the governance system. Although legal instruments provide a comprehensive normative foundation, their effectiveness is constrained by weak enforcement mechanisms and fragmented institutional arrangements. This indicates that legal development has outpaced institutional capacity, resulting in a regulatory environment where rules exist without sufficient mechanisms to ensure their implementation. Consequently, the gap between formal legal frameworks and actual outcomes becomes a defining feature of cybersecurity governance. This gap transforms legal systems into symbolic instruments rather than functional tools for risk mitigation. As a result, the persistence of data breaches and cybersecurity risks reflects a systemic governance failure rather than a purely legal deficiency.

The interaction between enforcement and compliance further reveals that regulatory effectiveness is inherently dependent on the alignment between institutional capacity and behavioral incentives. Weak enforcement reduces the credibility of legal systems, which in turn diminishes the motivation of regulated entities to comply with legal obligations. This creates a self-reinforcing cycle in which low enforcement leads to low compliance, and low compliance further weakens the overall effectiveness of regulation. In such conditions, legal norms fail to shape behavior, and regulatory frameworks lose their deterrent function. Moreover, compliance challenges are not solely the result of organizational limitations but are also influenced by regulatory ambiguity and lack of clear guidance. This suggests that improving compliance requires not only stronger enforcement but also greater clarity and consistency in regulatory design. Therefore, enforcement and compliance must be understood as interdependent elements of an effective governance system.

From a broader governance perspective, the findings highlight the need to reconceptualize cybersecurity regulation as an integrated system rather than a collection of legal instruments. Fragmentation across institutions and overlapping regulatory responsibilities limit the ability of the governance system to respond effectively to digital risks. Addressing these challenges requires a shift toward coordinated governance models that emphasize institutional integration, clear allocation of authority, and consistent regulatory practices. Strengthening enforcement capacity must be accompanied by reforms that enhance coordination and reduce fragmentation within the regulatory system. In addition, fostering a regulatory environment that promotes compliance through clarity, predictability,

and accountability is essential for improving legal effectiveness. Without such systemic reforms, legal frameworks will continue to operate below their potential and fail to address evolving cybersecurity risks. Therefore, the improvement of cybersecurity governance in Indonesia depends on the transformation of both institutional structures and regulatory practices.

6. Conclusion

This study concludes that the effectiveness of data protection and cybersecurity legal frameworks in Indonesia is fundamentally constrained not by the absence of regulation, but by limitations in enforcement and compliance mechanisms. Although the legal system provides a comprehensive normative structure through established statutes, its practical impact remains limited due to the inability to ensure consistent implementation. This indicates that legal effectiveness is not determined by the existence of rules, but by the capacity of governance systems to operationalize those rules in practice. As a result, the persistence of cybersecurity risks reflects a structural gap between regulatory intent and actual outcomes. This gap demonstrates that legal frameworks alone are insufficient to address complex digital challenges without corresponding institutional support. Therefore, the effectiveness of cybersecurity governance in Indonesia remains partial and conditional.

The findings further highlight that strengthening enforcement and compliance is not merely a complementary reform, but a central requirement for improving the performance of legal frameworks. Weak enforcement undermines the

credibility of legal systems, while low compliance reduces the ability of regulations to shape behavior and mitigate risks. This creates a systemic condition in which legal norms fail to achieve their intended objectives, allowing vulnerabilities to persist despite formal regulatory coverage. Addressing this issue requires a comprehensive approach that enhances enforcement capacity, clarifies institutional responsibilities, and improves regulatory coordination. In addition, fostering a compliance-oriented environment through clearer guidance and accountability mechanisms is essential for ensuring that legal obligations are effectively implemented. Without such improvements, regulatory frameworks will continue to function below their intended capacity.

Finally, this study emphasizes that the future of cybersecurity governance in Indonesia depends on the transition from a formally comprehensive legal system to a functionally effective governance structure. This transition requires not only strengthening individual components such as enforcement and compliance, but also improving the overall coherence and integration of the regulatory system. A more coordinated and institutionally aligned approach is necessary to address the complexity of digital risks and to ensure consistent policy outcomes. By aligning legal frameworks with enforcement capacity and compliance behavior, Indonesia can enhance the effectiveness of its cybersecurity governance. Such transformation is essential for building a resilient digital environment that can respond to evolving technological challenges. Therefore, the improvement of legal effectiveness must be positioned as a strategic priority in the development of digital governance.

.

References

Alkhamsi, N. N., & Alqahtani, S. S. (2024). Compliance framework for personal data protection law standards. *International Journal of Advanced Computer Science & Applications, 15*(7).

Andarge, T., & Lichtenberg, E. (2020). Regulatory compliance under enforcement gaps. *Journal of Regulatory Economics, 57*(3), 181–202.

Bachňáková Rózenfeldová, L., Sokol, P., Hučková, R., & Mesarčík, M. (2024). Personal data protection enforcement under GDPR—the Slovak experience. *International Data Privacy Law, 14*(3), 278–297.

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime, 28*(2), 359–374.

Kumar, V. A., Bhardwaj, S., & Lather, M. (2024). Cybersecurity and safeguarding digital assets: An analysis of regulatory frameworks, legal liability and enforcement mechanisms. *Productivity, 65*(1), 1–10.

Lonzetta, A. M., & Hayajneh, T. (2021). Challenges of complying with data protection and privacy regulations. *EAI Endorsed Transactions on Scalable Information Systems, 8*(30), e4.

Lynskey, O. (2023). Complete and effective data protection. *Current Legal Problems, 76*(1), 297–344.

Malik, W., Gul, S., & Qureshi, G. M. (2025). Regulating artificial intelligence: Challenges for data protection and privacy in developing nations. *Journal of Social Signs Review, 3*(05), 95–108.

Oyetunji, S. A. (2024). Investigating data protection compliance challenges. *International Journal of Innovative Science and Research Technology, 9*(8), 2131–2147.

Prasetyo, B., Handayani, I. G. A. K. R., & Sulistiyono, A. (2025). Data protection laws in Indonesia: Navigating privacy in the digital age. *Side: Scientific Development Journal, 2*(1), 9–16.

Puaschunder, J. M. (2022). Behavioral international law: Law-in-books vs. law-in-action resembling the neoclassical economics vs. behavioral economics debate. In *Proceedings of the 28th International RAIS Conference on Social Sciences and Humanities* (pp. 1–9).

Razi, F., & Markus, D. P. (2024). Implementation and challenges of the personal data protection law in Indonesia. *Jurnal Indonesia Sosial Teknologi, 5*(12).

Rusydi, M. T. (2024). Evaluating global cybersecurity laws: Effectiveness of legal frameworks and enforcement mechanisms in the digital age. *Walisongo Law Review (Walrev), 6*(1), 71–83.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7–34.

Sumkoski, G., Kocherbaeva, A., & Alapaeva, A. (2025). Regulatory management: Weaknesses and potential for improvement. *Upravlencheskie Nauki, 15*(4), 78–93.

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review, 14*, 175.

Wacks, R. (2021). *Understanding jurisprudence: An introduction to legal theory*. Oxford University Press.