Journal of Cyber Law
and Information Security
Volume 3, Number 2, 2024

Regulatory Implementation and Compliance Challenges in Indonesia's Cybersecurity Governance

Dhaniswara K. Harjono[1]

[1] Universitas Kristen Indonesia, Jakarta, Indonesia

Abstract

Cybersecurity governance in Indonesia faces persistent challenges arising from gaps in regulatory implementation and weak compliance among regulated actors. Although legal frameworks provide a formal basis for governing digital activities, their effectiveness is limited by inconsistent operationalization and insufficient adherence to regulatory requirements. This study examines the effectiveness of policy implementation and the factors influencing compliance in Indonesia's cybersecurity governance. Using a normative juridical method combined with systematic and sociological approaches, the research analyzes the interaction between implementation processes, enforcement mechanisms, and compliance behavior. The findings indicate that institutional limitations, weak enforcement credibility, and complex regulatory requirements contribute to inconsistent implementation and low compliance levels. These conditions reduce the effectiveness of cybersecurity regulation and create a gap between legal provisions and governance outcomes. The study concludes that strengthening implementation processes and improving compliance mechanisms are essential for achieving effective and reliable cybersecurity governance in Indonesia.

Article history:
Received: September 2, 2024
Revised: October 9, 2024
Accepted: November 8, 2024
Published: December 30, 2024

Keywords:
compliance behavior,
cybersecurity governance,
policy implementation,
regulatory compliance,
regulatory effectiveness,
state capacity.

Identifier:
Zera Open
Page: 165-182
https://zeraopen.com/journal/jclis

*Corresponding author:
(Dhaniswara K. Harjono)

1. Introduction

The increasing dependence on digital technologies has intensified the importance of effective cybersecurity governance, requiring not only comprehensive legal frameworks but also consistent implementation and compliance across institutions. While regulatory systems establish formal rules and obligations, their effectiveness ultimately depends on how these rules are operationalized in practice. Policy implementation plays a critical role in translating legal provisions into actionable outcomes, particularly in complex governance environments. Hill and Hupe (2021) emphasize that implementation processes determine whether policy objectives can be achieved within administrative systems. Similarly, Lapuente and Van de Walle (2020) highlight that governance performance is closely linked to the quality of public service delivery, which depends on effective implementation. These perspectives suggest that the success of cybersecurity governance is contingent on the ability of institutions to implement regulatory frameworks effectively.

In addition to implementation challenges, compliance represents a central issue in determining the effectiveness of cybersecurity governance. Compliance refers to the extent to which regulated actors adhere to legal and regulatory requirements, which is influenced by both institutional and behavioral factors. Ishwardat et al. (2024) emphasize that compliance is shaped by organizational behavior, incentives, and regulatory environments. Taing and Chang (2021) further demonstrate that compliance intentions are influenced by factors such as perceived norms, attitudes, and enforcement expectations. These findings indicate that compliance is not automatic but requires appropriate governance mechanisms to

ensure adherence. When compliance is weak, regulatory frameworks fail to produce intended outcomes. Consequently, understanding compliance dynamics is essential for evaluating cybersecurity governance effectiveness.

The relationship between enforcement and compliance further highlights the complexity of governance systems, where regulatory effectiveness depends on both institutional capacity and behavioral responses. Enforcement mechanisms are designed to ensure compliance by monitoring behavior and applying sanctions when necessary. Baldwin et al. (2021) argue that effective regulation requires enforcement strategies that balance deterrence and compliance incentives. Andarge and Lichtenberg (2020) further highlight that enforcement credibility is essential for maintaining regulatory effectiveness. However, when enforcement is inconsistent or limited, compliance levels tend to decline. This creates a situation in which regulatory frameworks exist but are not effectively followed. As a result, enforcement and compliance must be analyzed together to understand governance outcomes.

The challenges of implementation and compliance are particularly pronounced in the context of cybersecurity governance, where rapid technological change and complex risks require coordinated institutional responses. Cybersecurity governance involves multiple actors, including regulatory agencies, law enforcement bodies, and private sector entities, each with distinct roles and responsibilities. Savaş and Karataş (2022) highlight that cybersecurity governance requires the integration of legal, technical, and organizational dimensions. Wang et al. (2024) further demonstrate that cybersecurity compliance frameworks are complex and require alignment between regulatory requirements and organizational practices. These

conditions increase the difficulty of ensuring consistent implementation and compliance. Consequently, cybersecurity governance systems face unique challenges that go beyond traditional regulatory issues.

In Indonesia, cybersecurity governance is supported by legal frameworks such as Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi and Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, which provide a formal basis for regulating digital activities. However, existing studies indicate that there are significant gaps between regulatory provisions and their practical implementation. Simbolon and Juwono (2022) highlight that Indonesia's data protection framework still faces challenges in aligning with international standards and ensuring effective implementation. Yulianto (2021) further emphasizes that cybersecurity policies in Indonesia encounter difficulties in operational execution due to institutional and regulatory constraints. These findings suggest that the effectiveness of cybersecurity governance is limited by both implementation and compliance challenges. As a result, regulatory frameworks are not fully operationalized in practice.

Based on these considerations, this study aims to analyze the effectiveness of regulatory implementation and compliance in Indonesia's cybersecurity governance and to identify the factors that influence compliance with legal frameworks. Using a normative juridical method combined with systematic and sociological approaches, the research examines how implementation processes, enforcement mechanisms, and compliance behavior interact within governance systems. The analysis focuses on identifying gaps between legal provisions and practical outcomes, as well as the

underlying causes of compliance challenges. By integrating implementation and compliance perspectives, the study provides a more comprehensive understanding of cybersecurity governance effectiveness. Furthermore, it offers insights into how governance systems can be improved through better implementation strategies and enhanced compliance mechanisms. Through this approach, the study contributes to the development of more effective and operational cybersecurity governance in Indonesia.

2. Literature Review

Policy implementation is a central component of governance systems, determining whether legal frameworks can be translated into effective regulatory outcomes. It involves the processes through which policies are operationalized within administrative structures and implemented by institutions. Hill and Hupe (2021) emphasize that implementation is not a linear process but is shaped by institutional arrangements, administrative capacity, and contextual factors. Lapuente and Van de Walle (2020) further highlight that the quality of public service delivery is closely linked to the effectiveness of policy implementation. These perspectives indicate that implementation gaps often arise from institutional limitations rather than deficiencies in legal design. As a result, regulatory frameworks may exist formally but fail to produce intended outcomes in practice. This suggests that understanding implementation processes is essential for evaluating governance effectiveness.

Compliance theory provides a framework for understanding how regulated actors respond to legal and regulatory requirements within governance systems. Compliance is influenced by a combination of behavioral, organizational, and institutional factors that shape decision-making processes. Orozco (2019) conceptualizes compliance as a systemic phenomenon influenced by legal structures, incentives, and enforcement mechanisms. Michael et al. (2021) further argue that compliance behavior is shaped by regulatory environments and the perceived costs and benefits of adherence. These perspectives indicate that compliance is not merely a legal obligation but a strategic response to governance conditions. When regulatory systems fail to create appropriate incentives or deterrents, compliance levels tend to decline. Consequently, compliance theory highlights the importance of aligning regulatory frameworks with behavioral dynamics.

The determinants of compliance within governance systems are multifaceted, encompassing institutional capacity, enforcement mechanisms, and behavioral factors. Ishwardat et al. (2024) emphasize that compliance is influenced by organizational culture, regulatory pressure, and ethical considerations. Dunbar et al. (2021) further demonstrate that compliance is affected by factors such as resource availability, monitoring systems, and enforcement credibility. These findings suggest that compliance is shaped by both internal organizational factors and external regulatory environments. When institutions lack the capacity to monitor and enforce regulations, compliance becomes inconsistent. As a result, regulatory systems fail to achieve predictable and reliable outcomes. This highlights the need to address both institutional and behavioral dimensions of compliance.

The relationship between enforcement and compliance is critical for understanding regulatory effectiveness, as enforcement mechanisms directly influence compliance behavior. Enforcement ensures that legal norms are followed by monitoring activities and applying sanctions for non-compliance. Baldwin et al. (2021) emphasize that effective regulation requires a balance between deterrence and cooperative approaches to compliance. Andarge and Lichtenberg (2020) further highlight that enforcement credibility is essential for maintaining compliance within regulatory systems. When enforcement is weak or inconsistent, regulated actors may perceive non-compliance as low-risk. This reduces the effectiveness of regulatory frameworks and undermines governance outcomes. Therefore, enforcement and compliance must be analyzed as interconnected elements of governance systems.

In the context of cybersecurity governance, implementation and compliance challenges are amplified by the complexity of digital environments and the involvement of multiple actors. Cybersecurity governance requires coordination between regulatory authorities, enforcement agencies, and private sector organizations, each with distinct roles and responsibilities. Wang et al. (2024) highlight that cybersecurity compliance frameworks are complex and require alignment between regulatory requirements and organizational practices. Cochran (2024) further emphasizes that legal compliance in cybersecurity involves navigating multiple regulatory requirements and operational constraints. Savaş and Karataş (2022) also note that cybersecurity governance depends on the integration of legal, technical, and organizational dimensions. These perspectives indicate that

cybersecurity governance faces unique implementation and compliance challenges that require specialized approaches.

3. Methods

This study employs a normative juridical research method combined with systematic and sociological approaches to analyze the effectiveness of regulatory implementation and compliance in Indonesia's cybersecurity governance. The normative juridical approach is used to examine legal frameworks governing cybersecurity, including the structure of regulatory obligations, enforcement provisions, and institutional responsibilities. This allows for the identification of how legal norms are formally designed and how implementation is expected to occur within governance systems. However, as implementation theory suggests, the existence of legal provisions does not guarantee effective operationalization in practice. Hill and Hupe (2021) emphasize that implementation outcomes are shaped by institutional arrangements and administrative processes. Therefore, this study extends beyond doctrinal analysis to evaluate how implementation is carried out within institutional contexts.

The systematic approach is applied to analyze the relationships between implementation processes, enforcement mechanisms, and compliance behavior within Indonesia's cybersecurity governance system. This involves examining how institutional capacity, coordination practices, and enforcement strategies influence the effectiveness of regulatory implementation. Lapuente and Van de Walle (2020) highlight that governance performance is closely linked to the quality of

implementation and public service delivery. In addition, a sociological approach is used to assess compliance behavior, focusing on how regulated actors respond to legal requirements and enforcement practices. Ishwardat et al. (2024) emphasize that compliance is influenced by behavioral and organizational factors, including incentives and regulatory pressure. By integrating these approaches, the study captures both the formal design and practical operation of governance systems. This enables a comprehensive analysis of the factors that shape implementation effectiveness and compliance outcomes in cybersecurity governance.

4. Results

4.1. Effectiveness of Regulatory Implementation

The findings indicate that the implementation of cybersecurity regulations in Indonesia is characterized by significant gaps between formal legal provisions and their practical execution. Although regulatory frameworks establish clear obligations and institutional responsibilities, their operationalization remains inconsistent across governance structures. Hill and Hupe (2021) emphasize that policy implementation is influenced by institutional arrangements and administrative processes, which determine whether policy objectives can be achieved. Lapuente and Van de Walle (2020) further highlight that variations in implementation quality directly affect governance performance and service delivery outcomes. In Indonesia, these challenges are reflected in uneven enforcement practices and limited institutional coordination. As a result, regulatory implementation becomes fragmented and

inconsistent. This indicates that implementation effectiveness is constrained by structural and administrative limitations.

A key factor contributing to weak implementation is the presence of institutional limitations that hinder the execution of regulatory frameworks. These limitations include insufficient administrative capacity, lack of technical expertise, and organizational inefficiencies within institutions responsible for cybersecurity governance. Yulianto (2021) highlights that cybersecurity policy implementation in Indonesia faces challenges related to institutional coordination and resource constraints. Saleh and Winata (2023) further emphasize that national cybersecurity strategies encounter difficulties in translating policy objectives into operational practices. These constraints reduce the ability of institutions to implement regulations effectively and consistently. As a result, implementation processes are often incomplete or delayed. Consequently, regulatory frameworks fail to achieve their intended impact in practice.

The effectiveness of implementation is also influenced by the design and application of enforcement mechanisms within governance systems. Enforcement mechanisms are intended to ensure that regulatory requirements are followed by monitoring compliance and applying sanctions when necessary. Baldwin et al. (2021) emphasize that effective regulation requires enforcement strategies that balance deterrence and compliance incentives. Andarge and Lichtenberg (2020) further highlight that enforcement credibility is essential for maintaining regulatory effectiveness. However, in Indonesia, enforcement practices are often inconsistent and limited in scope. This reduces the perceived risk of non-compliance among

regulated actors. As a result, implementation processes are weakened by insufficient enforcement support.

The interaction between institutional limitations and weak enforcement mechanisms results in ineffective implementation outcomes, where legal frameworks are not fully operationalized. Simbolon and Juwono (2022) highlight that Indonesia's data protection policies face challenges in aligning regulatory provisions with practical implementation. Savaş and Karataş (2022) further emphasize that cybersecurity governance requires effective integration of legal and institutional processes to ensure implementation success. In the absence of such integration, implementation gaps persist and undermine regulatory effectiveness. This creates a disconnect between policy objectives and governance outcomes. Consequently, implementation challenges represent a critical limitation in cybersecurity governance. These findings demonstrate that improving implementation requires addressing both institutional and enforcement constraints.

4.1. Compliance Challenges in Cybersecurity Governance

The findings further indicate that compliance with cybersecurity regulations in Indonesia is influenced by a combination of behavioral, institutional, and regulatory factors. Compliance behavior is shaped by how regulated actors perceive legal obligations, enforcement risks, and organizational incentives. Taing and Chang (2021) demonstrate that compliance intentions are influenced by attitudes, social norms, and perceived behavioral control. Ishwardat et al. (2024) further emphasize that organizational behavior and regulatory environments play a significant role in shaping compliance outcomes. In Indonesia, compliance levels are affected by

limited awareness of regulatory requirements and weak enforcement credibility. These factors reduce the motivation of organizations to adhere to cybersecurity regulations. As a result, compliance remains inconsistent across sectors.

Institutional barriers also play a significant role in limiting compliance, particularly in relation to monitoring, supervision, and enforcement practices. Dunbar et al. (2021) highlight that compliance is influenced by the availability of resources, monitoring systems, and enforcement mechanisms. Michael et al. (2021) further argue that regulatory environments shape compliance behavior by influencing the perceived costs and benefits of adherence. In Indonesia, limited monitoring capacity and inconsistent enforcement reduce the effectiveness of compliance mechanisms. This creates an environment in which non-compliance is not consistently detected or sanctioned. As a result, regulatory frameworks fail to produce predictable compliance outcomes. Consequently, institutional limitations reinforce compliance challenges.

The complexity of cybersecurity governance further complicates compliance due to the need to align regulatory requirements with organizational practices and technological capabilities. Wang et al. (2024) highlight that cybersecurity compliance frameworks require coordination between regulatory standards and operational processes within organizations. Cochran (2024) further emphasizes that legal compliance in cybersecurity involves navigating multiple regulatory requirements and technical constraints. In Indonesia, organizations often face difficulties in understanding and implementing complex regulatory requirements. This increases the likelihood of non-compliance, particularly among smaller organizations with

limited resources. As a result, compliance challenges are exacerbated by the complexity of regulatory frameworks. Therefore, simplifying and aligning regulatory requirements is essential for improving compliance.

Finally, the persistence of compliance challenges reflects a broader governance issue in which regulatory systems fail to create sufficient incentives and deterrents for adherence. Orozco (2019) conceptualizes compliance as a systemic phenomenon influenced by the interaction between legal structures, enforcement mechanisms, and behavioral factors. Simbolon and Juwono (2022) further highlight that gaps between legal provisions and practical implementation contribute to weak compliance outcomes in Indonesia. These findings indicate that compliance challenges are not isolated but are embedded within governance systems. As a result, improving compliance requires a comprehensive approach that addresses both institutional and behavioral dimensions. Without such reforms, cybersecurity governance will continue to face significant limitations. Consequently, compliance challenges must be recognized as a central issue in regulatory effectiveness.

5. Discussion

The findings of this study demonstrate that the effectiveness of cybersecurity governance in Indonesia is fundamentally constrained by the interaction between weak regulatory implementation and inconsistent compliance behavior. These challenges are not independent but mutually reinforcing, creating a governance environment in which legal frameworks fail to produce intended outcomes. Implementation gaps reduce the consistency of regulatory application, while weak

compliance further undermines the effectiveness of enforcement mechanisms. As a result, governance systems operate below their potential, with limited ability to address complex cybersecurity risks. This indicates that the presence of legal frameworks alone is insufficient to ensure effective governance. Therefore, the effectiveness of cybersecurity regulation depends on the alignment between implementation processes and compliance behavior.

The analysis further highlights that improving governance effectiveness requires strengthening both institutional capacity and behavioral compliance mechanisms within regulatory systems. Effective implementation depends on the ability of institutions to operationalize legal frameworks through consistent enforcement, monitoring, and coordination. At the same time, compliance behavior is influenced by incentives, awareness, and the perceived credibility of enforcement mechanisms. When enforcement is inconsistent, regulated actors may perceive non-compliance as low-risk, reducing their motivation to adhere to regulations. This creates a cycle in which weak implementation leads to low compliance, and low compliance further weakens regulatory effectiveness. Consequently, addressing governance challenges requires a balanced approach that integrates institutional and behavioral dimensions.

From a broader governance perspective, the findings suggest that cybersecurity regulation must evolve toward more adaptive and responsive systems that can address both implementation and compliance challenges. This involves improving administrative capacity, enhancing coordination among institutions, and developing regulatory strategies that encourage compliance. Simplifying regulatory

requirements and providing clearer guidance to regulated actors can also improve compliance outcomes. In addition, strengthening enforcement mechanisms and ensuring their consistent application is essential for maintaining regulatory credibility. Without these changes, governance systems will continue to face limitations in achieving effective regulatory outcomes. Therefore, the future of cybersecurity governance in Indonesia depends on the ability to integrate implementation and compliance strategies within a cohesive regulatory framework.

6. Conclusion

This study concludes that the effectiveness of cybersecurity governance in Indonesia is significantly constrained by gaps in regulatory implementation and persistent challenges in achieving compliance among regulated actors. Although legal frameworks provide a formal structure for governing digital activities, their practical impact is limited by inconsistencies in implementation and weak adherence to regulatory requirements. This indicates that the core issue lies not in the existence of regulation, but in the inability of governance systems to operationalize and enforce these frameworks effectively. As a result, a disconnect emerges between legal provisions and actual governance outcomes. This disconnect reflects systemic weaknesses in both institutional processes and compliance behavior. Therefore, improving cybersecurity governance requires a focus on strengthening implementation and compliance mechanisms.

The findings further demonstrate that effective governance depends on the alignment between institutional capacity, enforcement strategies, and behavioral

compliance dynamics. Implementation processes must be supported by adequate resources, clear institutional mandates, and consistent enforcement practices to ensure that regulatory frameworks are applied effectively. At the same time, compliance behavior must be encouraged through appropriate incentives, awareness, and credible enforcement mechanisms. When these elements are aligned, governance systems are more likely to produce consistent and reliable outcomes. Conversely, misalignment between implementation and compliance leads to ineffective regulation and persistent governance challenges. Consequently, addressing these issues requires a comprehensive approach that integrates institutional and behavioral perspectives.

Finally, this study emphasizes that advancing cybersecurity governance in Indonesia requires sustained efforts to enhance both regulatory implementation and compliance within a cohesive governance framework. Strengthening administrative capacity, improving coordination among institutions, and ensuring consistent enforcement are essential for effective implementation. In addition, developing strategies that promote compliance, such as simplifying regulatory requirements and increasing awareness among regulated actors, can improve adherence to legal frameworks. These reforms would enable governance systems to respond more effectively to evolving cybersecurity challenges and ensure the consistent application of regulations. Therefore, the future of cybersecurity governance in Indonesia depends on the successful integration of implementation and compliance strategies to achieve effective and resilient regulatory systems.

References

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

Baldwin, R., Cave, M., & Lodge, M. (2021). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford University Press.

Cochran, K. A. (2024). Legal and compliance considerations in cybersecurity. In *Cybersecurity Essentials: Practical Tools for Today's Digital Defenders* (pp. 431–463). Apress.

Dunbar, P., Browne, J. P., & O'Connor, L. (2021). Determinants of regulatory compliance in health and social care services: a systematic review protocol. *HRB Open Research, 4*, 13.

Hill, M., & Hupe, P. (2021). *Implementing public policy: An introduction to the study of operational governance*. Sage.

Ishwardat, S., van Steenbergen, E., Coffeng, T., & Ellemers, N. (2024). Stimulating regulatory compliance and ethical behavior of organizations: A review. *Business Ethics and Leadership, 8*(3), 151–172.

Lapuente, V., & Van de Walle, S. (2020). The effects of new public management on the quality of public services. *Governance, 33*(3), 461–475.

Michael, B., Falzon, J., & Shamdasani, A. (2021). A theory of financial services competition, compliance and regulation. *Journal of Modelling in Management, 16*(1), 377–412.

Orozco, D. (2019). A systems theory of compliance law. *University of Pennsylvania Journal of Business Law, 22*, 244.

Saleh, A. I., & Winata, M. D. (2023). Indonesia's cyber security strategy: Problems and challenges. In *Proceedings of the International Joint Conference on Arts and Humanities 2023* (pp. 1675–1696). Atlantis Press.

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

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi), 11*(2), 178–190.

Taing, H. B., & Chang, Y. (2021). Determinants of tax compliance intention: Focus on the theory of planned behavior. *International Journal of Public Administration, 44*(1), 62–73.

Wang, W., Sadjadi, S. M., & Rishe, N. (2024). A survey of major cybersecurity compliance frameworks. In *2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity)* (pp. 23–34). IEEE.

Yulianto, A. (2021). Cybersecurity policy and its implementation in Indonesia. *Law Research Review Quarterly, 7*(1), 69–82.