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

Enforcement Capacity and Institutional Constraints in Indonesia's Cybersecurity Governance: Implications for Regulatory Effectiveness

Fendy Prasetyawan [1]

[1] Universitas Kadiri, Kediri, Indonesia

Abstract

Article history:
Received: August 23, 2025
Revised: September 14, 2025
Accepted: November 04, 2025
Published: December 30, 2025

Keywords:
Cybersecurity Governance, Enforcement Capacity, Enforcement Mechanisms, Institutional Constraints, Regulatory Enforcement, State Capacity.

Identifier:
Zera Open
Page: 160-178
https://zeraopen.com/journal/jclis

The effectiveness of cybersecurity governance depends not only on the existence of legal frameworks but also on the capacity of institutions to enforce them. This study examines how enforcement capacity influences cybersecurity governance in Indonesia and analyzes the institutional constraints that limit the operationalization of cyber law enforcement. Using a normative juridical method combined with systematic and sociological approaches, the research evaluates the relationship between institutional capacity, enforcement mechanisms, and regulatory outcomes. The findings indicate that despite the presence of comprehensive legal frameworks, enforcement remains ineffective due to limited resources, lack of technical expertise, weak enforcement mechanisms, and insufficient coordination among institutions. These constraints result in inconsistent application of legal norms and reduce the deterrent effect of regulation. The study concludes that strengthening enforcement capacity, improving institutional coordination, and enhancing operational mechanisms are essential to ensuring effective cybersecurity governance in Indonesia.

*Corresponding author:
(Fendy Prasetyawan)

1. Introduction

The increasing reliance on digital technologies has intensified the need for effective cybersecurity governance, placing enforcement at the center of regulatory performance. While legal frameworks establish rules and obligations, their effectiveness ultimately depends on the capacity of institutions to enforce them in practice. In complex governance systems, enforcement is not merely a legal function but a product of institutional capability, including resources, expertise, and organizational structure. Chowdhury (2022) emphasizes that state capacity plays a decisive role in determining whether regulations can be effectively implemented and enforced. Similarly, Geddes (2023) argues that institutional capacity constraints often limit the ability of governments to translate regulatory objectives into operational outcomes. This suggests that the effectiveness of cybersecurity governance is fundamentally linked to enforcement capacity rather than legal design alone.

The role of enforcement capacity becomes particularly significant in regulatory environments where multiple actors are involved in implementing and monitoring compliance. Effective enforcement requires not only formal authority but also the availability of institutional resources and the ability to coordinate enforcement actions across agencies. Andarge and Lichtenberg (2020) highlight that regulatory effectiveness depends on the credibility and consistency of enforcement, which are directly influenced by institutional capacity. O'Reilly and Murphy (2022) further demonstrate that variations in state capacity significantly affect the performance of regulatory systems. When enforcement capacity is limited, institutions struggle to monitor compliance, investigate violations, and apply

sanctions effectively. This results in a gap between legal provisions and their practical implementation. Consequently, enforcement capacity emerges as a critical determinant of regulatory effectiveness.

In addition to capacity constraints, the complexity of enforcement mechanisms further influences the effectiveness of cybersecurity governance. Enforcement involves a combination of administrative, regulatory, and legal processes that must operate cohesively to ensure compliance. Brummer et al. (2022) argue that modern regulatory systems increasingly rely on enforcement-driven approaches, where agencies use sanctions and oversight mechanisms to achieve policy objectives. Pojanowski (2020) further highlights that administrative law frameworks define how enforcement authority is structured and exercised within governance systems. However, the effectiveness of these mechanisms depends on their operational clarity and institutional support. When enforcement systems are poorly designed or inadequately resourced, they fail to function effectively. This indicates that enforcement effectiveness is shaped by both institutional capacity and the design of enforcement mechanisms.

The challenges of enforcement capacity are particularly evident in the context of cybersecurity, where rapid technological change and complex threats require specialized expertise and coordinated institutional responses. Cybersecurity enforcement involves not only traditional law enforcement agencies but also regulatory bodies and technical institutions, creating a multi-dimensional enforcement environment. Moloney et al. (2022) highlight that law enforcement agencies often face limitations in capacity and capability when addressing

cybercrime, particularly in terms of technical expertise and resources. Goldstein et al. (2020) further demonstrate that enforcement effectiveness is closely linked to broader governance performance, including the quality of public services. These findings suggest that cybersecurity enforcement requires a higher level of institutional capacity compared to traditional regulatory domains. As a result, capacity limitations become more pronounced and have greater implications for governance effectiveness. This highlights the need to examine enforcement capacity within the specific context of cybersecurity.

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, as well as institutional arrangements involving multiple agencies. These frameworks provide a formal basis for regulating digital activities and enforcing compliance. However, existing studies indicate that enforcement capacity remains limited due to institutional constraints and resource challenges. Razi and Markus (2024) highlight that enforcement mechanisms for data protection in Indonesia are still developing and lack sufficient operational capacity. Syailendra et al. (2024) further emphasize that institutional limitations hinder the effective implementation of cybersecurity regulations. These conditions suggest that enforcement challenges are not solely related to legal provisions but are deeply rooted in institutional capacity. Consequently, the effectiveness of cybersecurity governance in Indonesia cannot be fully understood without examining enforcement capacity.

Based on these considerations, this study aims to analyze how enforcement capacity affects the effectiveness of cybersecurity governance in Indonesia and to examine the institutional constraints that limit the operationalization of cyber law enforcement. Using a normative juridical method combined with systematic and sociological approaches, the study evaluates the relationship between institutional capacity, enforcement mechanisms, and regulatory outcomes. The analysis focuses on identifying how limitations in resources, authority, and coordination influence enforcement performance. By shifting the focus from legal frameworks to enforcement capacity, this research provides a deeper understanding of the structural factors underlying regulatory ineffectiveness. Furthermore, it offers insights into how strengthening institutional capacity can improve the performance of cybersecurity governance. Through this approach, the study contributes to the development of more effective and operationally capable regulatory systems in Indonesia.

2. Literature Review

Enforcement capacity is a fundamental component of regulatory governance, determining whether legal frameworks can be effectively implemented in practice. It encompasses the availability of institutional resources, administrative capability, and organizational structures necessary to monitor compliance and sanction violations. Chowdhury (2022) emphasizes that state capacity is a critical determinant of regulatory effectiveness, as weak capacity limits the ability of institutions to enforce legal norms. Geddes (2023) further argues that building effective governance

systems requires not only formal authority but also sustained investment in institutional capability. These perspectives indicate that enforcement capacity is not an auxiliary element but a central factor shaping governance outcomes. Without adequate capacity, legal frameworks remain largely symbolic and fail to achieve their intended objectives.

The effectiveness of enforcement is also influenced by the design and operation of administrative enforcement mechanisms within regulatory systems. Enforcement mechanisms include monitoring systems, sanctioning procedures, and oversight processes that enable institutions to ensure compliance. Brummer et al. (2022) highlight that modern regulatory approaches increasingly rely on enforcement as a primary tool for achieving policy goals, particularly in complex regulatory environments. Pojanowski (2020) further explains that administrative law frameworks define the scope and limits of enforcement authority, shaping how regulatory agencies exercise their powers. However, the effectiveness of these mechanisms depends on their operational clarity and institutional support. When enforcement systems are fragmented or inadequately structured, they fail to function effectively. This suggests that enforcement mechanisms must be both well-designed and supported by sufficient institutional capacity.

Institutional constraints play a significant role in limiting the effectiveness of enforcement within governance systems. These constraints include insufficient resources, lack of technical expertise, and organizational inefficiencies that hinder the ability of institutions to perform enforcement functions. O'Reilly and Murphy (2022) demonstrate that variations in state capacity directly affect the performance

of public sector institutions, including their ability to enforce regulations. Andarge and Lichtenberg (2020) further highlight that enforcement credibility is weakened when institutions lack the capacity to consistently apply legal norms. Such constraints create a situation in which enforcement becomes selective or inconsistent, reducing its effectiveness. As a result, regulatory systems fail to produce predictable and reliable outcomes. This indicates that institutional capacity is a key determinant of enforcement performance.

In addition to capacity limitations, the availability and effectiveness of enforcement tools, such as sanctions and incentives, significantly influence compliance behavior and regulatory outcomes. Enforcement tools are designed to create incentives for compliance and deterrence against violations, thereby enhancing the effectiveness of legal frameworks. Ertas (2025) emphasizes that the strategic use of sanctions and incentives is essential for managing behavior within public sector governance systems. Similarly, Isaeva et al. (2025) demonstrate that enforcement mechanisms combining sanctions and training can improve compliance outcomes in organizational contexts. However, the effectiveness of these tools depends on their consistent application and institutional support. When enforcement tools are weak or inconsistently applied, their deterrent effect is reduced. This highlights the importance of integrating enforcement tools within a broader framework of institutional capacity.

The specific context of cybersecurity introduces additional challenges for enforcement capacity due to the complexity and technical nature of digital threats. Cybersecurity enforcement requires specialized knowledge, advanced technological

capabilities, and coordinated action among multiple institutions. Moloney et al. (2022) highlight that law enforcement agencies often lack the necessary capacity and expertise to effectively address cybercrime. Goldstein et al. (2020) further demonstrate that enforcement effectiveness is closely linked to broader governance capacity, including the quality of public sector services. These challenges are particularly pronounced in developing countries, where institutional capacity is often limited. As a result, cybersecurity governance faces unique enforcement constraints that go beyond traditional regulatory challenges. This indicates that strengthening enforcement capacity is essential for addressing cybersecurity risks effectively.

Overall, the literature suggests that enforcement capacity, institutional constraints, and enforcement mechanisms are interconnected elements that determine the effectiveness of regulatory governance. Capacity limitations weaken enforcement mechanisms, while ineffective enforcement tools reduce compliance and regulatory impact. This relationship highlights the need to analyze enforcement as a systemic issue rather than an isolated function. The theoretical and empirical insights reviewed in this section provide a foundation for examining how enforcement capacity affects cybersecurity governance in Indonesia. They also support the argument that improving regulatory effectiveness requires strengthening institutional capacity and refining enforcement mechanisms. Therefore, this study builds on these perspectives to analyze the role of enforcement capacity in shaping cybersecurity governance outcomes.

3. Methods

This study employs a normative juridical research method combined with systematic and sociological approaches to analyze the role of enforcement capacity in cybersecurity governance in Indonesia. The normative juridical approach is used to examine legal frameworks governing enforcement, including the distribution of authority, sanctioning mechanisms, and institutional mandates within cybersecurity regulation. This enables the identification of how enforcement is formally structured within legal instruments and how responsibilities are assigned to different institutions. However, as administrative law scholarship emphasizes, the existence of enforcement provisions does not guarantee their effective implementation in practice. Pojanowski (2020) highlights that the effectiveness of administrative law depends on how enforcement authority is exercised within institutional contexts. Therefore, this study extends beyond doctrinal analysis to evaluate how enforcement capacity affects the operationalization of legal frameworks.

The systematic approach is applied to examine the interrelationship between institutional capacity, enforcement mechanisms, and regulatory outcomes within Indonesia's cybersecurity governance system. This involves analyzing how resources, expertise, and organizational structures influence the ability of institutions to perform enforcement functions. O'Reilly and Murphy (2022) emphasize that variations in institutional capacity significantly affect governance performance, particularly in regulatory enforcement. In addition, a sociological approach is employed to assess how enforcement operates in practice, focusing on institutional behavior, coordination patterns, and the application of sanctions. Andarge and

Lichtenberg (2020) highlight that enforcement effectiveness depends on the consistency and credibility of institutional actions, which are shaped by capacity and organizational dynamics. By integrating these approaches, the study captures both the formal structure and practical operation of enforcement systems. This enables a comprehensive analysis of how institutional constraints limit the effectiveness of cybersecurity governance in Indonesia.

4. Results

4.1. Enforcement Capacity Limitations in Cybersecurity Governance

The findings indicate that enforcement capacity in Indonesia's cybersecurity governance is constrained by limitations in institutional resources, expertise, and organizational capability. Although legal frameworks establish enforcement obligations, the ability of institutions to operationalize these provisions remains limited. Chowdhury (2022) emphasizes that state capacity is a determining factor in regulatory performance, particularly in the implementation and enforcement of legal norms. Geddes (2023) further highlights that institutional development is often uneven, resulting in gaps between regulatory expectations and actual enforcement capacity. In the Indonesian context, these limitations are reflected in the insufficient availability of specialized personnel and technical resources required for cybersecurity enforcement. As a result, institutions face difficulties in monitoring compliance and responding effectively to violations. This indicates that enforcement capacity limitations are a fundamental constraint on governance effectiveness.

A key dimension of enforcement capacity limitation is the lack of adequate resources and technical capability to address the complexity of cybersecurity threats. Effective enforcement in the digital domain requires advanced technological infrastructure and specialized expertise, which are often lacking in regulatory institutions. O'Reilly and Murphy (2022) demonstrate that variations in institutional capacity significantly influence the ability of public sector organizations to perform regulatory functions. Similarly, Moloney et al. (2022) highlight that law enforcement agencies frequently lack the necessary skills and tools to effectively investigate and address cybercrime. These capacity gaps reduce the ability of institutions to detect violations and enforce compliance consistently. As a result, enforcement becomes reactive rather than proactive. Consequently, the overall effectiveness of cybersecurity governance is weakened.

In addition to resource constraints, the effectiveness of enforcement is influenced by the structure and operation of enforcement mechanisms within governance systems. Enforcement mechanisms are intended to ensure compliance through monitoring, investigation, and sanctioning processes. Brummer et al. (2022) argue that modern regulatory systems rely heavily on enforcement as a tool for achieving policy objectives, particularly in complex regulatory environments. However, Rosenbloom (2022) emphasizes that administrative enforcement requires well-defined procedures and institutional clarity to function effectively. In Indonesia, enforcement mechanisms are often characterized by procedural ambiguity and limited operational coordination. This reduces the ability of institutions to apply

enforcement measures consistently and effectively. As a result, enforcement mechanisms fail to fully support regulatory objectives.

The combined effect of limited capacity and weak enforcement mechanisms results in ineffective enforcement outcomes, where legal frameworks are not adequately implemented. Andarge and Lichtenberg (2020) highlight that enforcement effectiveness depends on the consistency and credibility of regulatory actions, which are undermined when capacity is insufficient. Goldstein et al. (2020) further demonstrate that weak enforcement negatively affects governance outcomes by reducing the quality of public services. In Indonesia, these conditions contribute to persistent cybersecurity risks, as institutions are unable to enforce regulations effectively. This creates a gap between legal provisions and their practical implementation. Consequently, enforcement capacity limitations directly undermine the effectiveness of cybersecurity governance. These findings confirm that strengthening enforcement capacity is essential for improving regulatory performance.

4.1. Institutional Constraints on Enforcement Effectiveness

The findings further indicate that institutional constraints significantly limit the effectiveness of enforcement within Indonesia's cybersecurity governance system. These constraints include organizational inefficiencies, lack of coordination, and unclear institutional mandates that hinder enforcement operations. Sumkoski et al. (2025) emphasize that regulatory systems characterized by structural weaknesses and fragmented management are less capable of enforcing legal norms effectively. Pojanowski (2020) further highlights that administrative law frameworks require

clear allocation of authority to ensure effective enforcement. In the absence of such clarity, institutions may struggle to perform their enforcement roles effectively. This leads to inconsistencies in enforcement practices and reduces accountability. As a result, institutional constraints become a major barrier to effective cybersecurity governance.

Another critical constraint is the limited availability and effectiveness of enforcement tools, including sanctions and monitoring mechanisms. Enforcement tools are essential for ensuring compliance and deterring violations, but their impact depends on how they are applied within governance systems. Ertas (2025) emphasizes that sanctions and incentives must be strategically designed and consistently implemented to influence behavior effectively. Similarly, Isaeva et al. (2025) demonstrate that enforcement mechanisms combining sanctions and institutional support can improve compliance outcomes. However, in Indonesia, enforcement tools are often underutilized or inconsistently applied, reducing their effectiveness. This weakens the deterrent effect of regulatory frameworks and limits their ability to shape behavior. Consequently, enforcement tools fail to achieve their intended purpose within cybersecurity governance.

Institutional constraints also manifest in the form of weak coordination and limited integration among enforcement actors. Effective enforcement in cybersecurity governance requires collaboration between regulatory agencies, law enforcement bodies, and technical institutions. Winship (2020) highlights that enforcement networks are essential for addressing complex regulatory challenges that involve multiple actors. However, in practice, coordination among institutions

is often limited, resulting in fragmented enforcement efforts. Moloney et al. (2022) further emphasize that lack of coordination reduces the effectiveness of law enforcement responses to cybercrime. This leads to gaps in enforcement coverage and inconsistencies in regulatory application. Therefore, coordination failure reinforces institutional constraints on enforcement.

The persistence of these institutional constraints results in systemic enforcement failure, where regulatory frameworks are unable to achieve their intended objectives. Razi and Markus (2024) highlight that enforcement mechanisms in Indonesia's data protection framework remain underdeveloped and lack operational effectiveness. Syailendra et al. (2024) further emphasize that institutional limitations hinder the implementation of cybersecurity regulations. These findings indicate that enforcement challenges are deeply rooted in structural and institutional factors rather than legal deficiencies. As a result, improving enforcement effectiveness requires addressing these underlying constraints. Without such reforms, cybersecurity governance will continue to face significant limitations. Consequently, institutional constraints must be recognized as a central issue in the effectiveness of cyber law enforcement.

5. Discussion

The findings of this study demonstrate that the effectiveness of cybersecurity governance in Indonesia is fundamentally constrained by limitations in enforcement capacity rather than the absence of legal frameworks. Although regulatory systems provide formal mechanisms for enforcement, their practical operation is limited by

insufficient institutional resources, technical expertise, and organizational capability. This indicates that enforcement is not merely a legal function but a capacity-driven process that depends on the ability of institutions to operationalize regulatory provisions. As a result, the gap between legal frameworks and governance outcomes emerges from structural limitations within enforcement systems. This transforms enforcement into a reactive and inconsistent process rather than a proactive and reliable mechanism. Consequently, cybersecurity governance fails to achieve its intended objectives due to capacity constraints.

The interaction between enforcement capacity and institutional constraints further reveals that governance effectiveness depends on the alignment between resources, authority, and operational mechanisms. When institutions lack sufficient capacity and face structural limitations, enforcement becomes fragmented and inconsistent. This reduces the credibility of regulatory systems and weakens their ability to influence behavior. In such conditions, enforcement tools such as sanctions and monitoring mechanisms are applied unevenly, diminishing their deterrent effect. Moreover, limited coordination among enforcement actors exacerbates these challenges by preventing the development of cohesive enforcement strategies. This suggests that enforcement effectiveness requires not only adequate capacity but also integrated institutional arrangements. Therefore, improving enforcement requires both strengthening institutional capacity and addressing structural constraints.

From a broader governance perspective, the findings highlight the need to shift from a formalistic approach to enforcement toward a capacity-oriented model that emphasizes institutional capability and operational effectiveness. Strengthening

cybersecurity governance requires investments in resources, expertise, and technological infrastructure to enhance enforcement capacity. In addition, reforms aimed at improving coordination and clarifying institutional mandates are essential for ensuring consistent enforcement. A more integrated and capacity-driven approach would enable institutions to implement legal frameworks more effectively and respond to evolving cybersecurity challenges. Without such reforms, enforcement systems will continue to operate below their potential and fail to achieve regulatory objectives. Therefore, the improvement of cybersecurity governance in Indonesia depends on the transformation of enforcement systems into more capable and coordinated institutional frameworks.

6. Conclusion

This study concludes that the effectiveness of cybersecurity governance in Indonesia is primarily constrained by limitations in enforcement capacity rather than deficiencies in legal frameworks. Although existing regulations provide a formal basis for enforcement, their practical impact remains limited due to insufficient institutional resources, lack of technical expertise, and weak organizational capability. This indicates that the success of regulatory systems depends not only on legal provisions but also on the ability of institutions to operationalize enforcement mechanisms effectively. As a result, a gap persists between regulatory intent and actual governance outcomes. This gap reflects structural weaknesses in enforcement systems rather than shortcomings in legal design. Therefore, strengthening

enforcement capacity is essential for improving the effectiveness of cybersecurity governance.

The findings further demonstrate that institutional constraints, including unclear authority, limited coordination, and weak enforcement tools, significantly undermine enforcement effectiveness. When enforcement systems lack clarity and coherence, institutions are unable to apply legal norms consistently and effectively. This reduces the credibility of regulatory frameworks and limits their ability to influence behavior. In such conditions, enforcement becomes fragmented and reactive, failing to provide adequate deterrence against violations. Addressing these challenges requires a comprehensive approach that enhances institutional capacity, improves coordination, and strengthens enforcement mechanisms. Without such reforms, enforcement systems will continue to operate below their intended capacity. Consequently, institutional constraints must be addressed as a central issue in cybersecurity governance.

Finally, this study emphasizes that improving cybersecurity governance in Indonesia requires a shift toward a capacity-oriented enforcement model that prioritizes institutional capability and operational effectiveness. Strengthening enforcement capacity involves not only increasing resources but also developing expertise, improving organizational structures, and enhancing technological capabilities. In addition, establishing clear institutional mandates and coordinated enforcement strategies is essential for ensuring consistent regulatory application. Such reforms would enable governance systems to function as cohesive and effective enforcement frameworks. By aligning legal frameworks with institutional capacity,

Indonesia can improve the effectiveness of its cybersecurity governance. Therefore, the future of cyber law enforcement depends on the ability to transform enforcement systems into more capable and integrated structures.

References

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

Brummer, C., Yadav, Y., & Zaring, D. (2022). Regulation by enforcement. *Southern California Law Review, 96*, 1297.

Chowdhury, A. (2022). Regulation and state capacity. *Rationality and Society, 34*(4), 446–468.

Ertas, N. (2025). Sanctions and incentives in public ethics management. In *Public Sector Ethics* (pp. 72–91).

Geddes, B. (2023). *Politician's dilemma: Building state capacity in Latin America* (Vol. 25). University of California Press.

Goldstein, R., Sances, M. W., & You, H. Y. (2020). Exploitative revenues, law enforcement, and the quality of government service. *Urban Affairs Review, 56*(1), 5–31.

Isaeva, E., Seki, M., & Kakinaka, M. (2025). Information system security policy noncompliance: Effects of sanctions and training in public organizations. *Pacific Asia Journal of the Association for Information Systems, 17*(4), 2.

Moloney, C. J., Unnithan, N. P., & Zhang, W. (2022). Assessing law enforcement's cybercrime capacity and capability. *FBI Law Enforcement Bulletin.*

O'Reilly, C., & Murphy, R. H. (2022). An index measuring state capacity, 1789–2018. *Economica, 89*(355), 713–745.

Pojanowski, J. A. (2020). Neoclassical administrative law. *Harvard Law Review, 133*(3), 852–919.

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

Rosenbloom, D. H. (2022). *Administrative law for public managers*. Routledge.

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.

Winship, V. (2020). Enforcement networks. *Yale Journal on Regulation, 37*, 274.