Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 18 (01), 2026
pp. 19 - 41

Cyber security Governance in Public Institutions: A Legal Risk Assessment Model for Indonesia's Digital Transformation

Bagus Arwani[1], Prasetijo Rijadi[2], Jonaedi Efendi[3]

[1]baguspunkman@.gmail.com

Afiliasi Faculty Of Law, Universitas Bhayangkara Surabaya

*Corresponding Author: **Bagus Arwani**

Email: baguspunkman@.gmail.com

ABSTRACT

Indonesia's rapid digital transformation has expanded the role of public institutions as custodians of critical data and providers of essential electronic services. However, this transition has not been matched by a coherent and enforceable cyber security governance framework. Existing regulations—dispersed across the ITE Law, PDP Law, PP 71/2019, and sectoral instruments—remain fragmented, inconsistent, and limited in binding force. Institutional mandates are similarly diffuse, with the National Cyber and Encryption Agency (BSSN), Kominfo, OJK, BI, and sectoral ministries exercising overlapping authorities. These doctrinal and structural weaknesses leave Indonesia vulnerable to escalating cyber threats, including ransomware attacks, data breaches, and systemic disruptions to public services. This article develops a Legal Risk Assessment Model (LRAM) tailored to Indonesia's public institutions, integrating normative legal research and comparative analysis. Drawing on best practices from Estonia, Singapore, and the United Kingdom—jurisdictions with advanced public-sector cyber governance—the model proposes four interrelated components: (1) a unified statutory framework through a dedicated Cybersecurity Act; (2) a centralized national authority with clear enforcement powers; (3) mandatory, standardized risk assessment and incident-reporting obligations; and (4) institutional oversight mechanisms ensuring accountability and transparency. The proposed model reconceptualizes cyber security not merely as a technical function but as a legal and administrative governance obligation. The study concludes that adopting the LRAM would significantly strengthen Indonesia's cyber resilience, harmonize public-sector security standards, enhance public trust, and support sustainable digital transformation. The model offers a reform pathway that aligns national regulatory structures with global norms while remaining sensitive to Indonesia's institutional context.

Keywords: Comparative Law, Cyber Security, Digital Transformation, Governance, Legal Risk Assessment, Public Institutions

Received: 20 November 2025 **Revised:** 27 December 2025 **Accepted:** 06 January 2026

INTRODUCTION

Digital transformation has become a defining pillar of Indonesia's contemporary governance agenda. Over the past decade, the Indonesian government has undertaken substantial efforts to digitize administrative processes, expand electronic public services, integrate national data systems, and modernize the technological architecture underpinning state operations. Anchored in policy initiatives such as the Sistem Pemerintahan Berbasis Elektronik (SPBE), the Online Single Submission (OSS) platform, electronic population administration, and national data interoperability frameworks, Indonesia seeks to establish a public sector capable of delivering services that are more efficient, transparent, and responsive. This rapid digitalization, however, has also intensified the exposure of public institutions to increasingly sophisticated cybersecurity threats that challenge administrative continuity, public trust, and national security.

Cyberattacks targeting public institutions in Indonesia have escalated sharply in both scale and severity. Recent breaches—such as large-scale leaks of population data, ransomware attacks on government networks, disruptions to electronic public services, and attempted intrusions into critical infrastructure—have revealed the systemic vulnerabilities of Indonesia's cybersecurity governance ecosystem. Many attacks stem from long-standing weaknesses including outdated systems, inconsistent risk-management practices, fragmented institutional mandates, and the absence of legally enforceable cybersecurity standards across government bodies. These vulnerabilities expose crucial state assets to manipulation, sabotage, and exploitation, raising concerns regarding institutional resilience in the face of evolving cyber threats. International analyses consistently position Indonesia as a country undergoing rapid digital expansion but lacking adequate cybersecurity governance structures to match this growth.[1]

At the heart of Indonesia's challenge is a fragmented legal landscape. The current cybersecurity regulatory framework is distributed across multiple statutes and sectoral instruments, including the Electronic Information and Transactions Law (ITE Law), the Personal Data Protection Law (PDP Law), Presidential Regulation No. 53/2017 establishing the National Cyber and Encryption Agency (BSSN), as well as various ministerial regulations on critical information infrastructure. Although these instruments demonstrate Indonesia's recognition of cybersecurity's importance, they collectively fail to provide a coherent or unified governance model. Scholars note that Indonesia's cybersecurity laws remain reactive and technologically oriented rather than preventive, governance-based, or institutionally integrated.[2]

[1] International Telecommunication Union Development Sector, *Global Cybersecurity Index 2020*, n.d.
[2] Awaludin Marwan, Diana Odier-Contreras Garduño, and Fiammetta Bonfigli, "Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia," *BESTUUR* 10, no. 1 (August 6, 2022): 22, https://doi.org/10.20961/bestuur.v10i1.59143.

Another structural weakness lies in institutional fragmentation. BSSN, while formally designated as the national cybersecurity authority, lacks comprehensive statutory powers comparable to those held by cybersecurity agencies in leading jurisdictions. Sectoral regulators—including Kominfo, OJK, Bank Indonesia, and ministries overseeing critical infrastructures—retain overlapping supervisory roles, creating duplication, inconsistencies, and gaps in enforcement. Public institutions are left with considerable discretion regarding cybersecurity risk management, leading to wide disparities in preparedness between central government ministries, regional governments, and state-owned enterprises. Many agencies continue to operate without risk registers, incident-response protocols, or regular cyber auditing processes.[3]

This gap between digital expansion and governance capacity is not unique to Indonesia; many emerging economies face similar challenges. However, comparative evidence demonstrates that countries with advanced digital governance models have achieved resilience through coherent regulatory frameworks, centralized institutions, and mandatory risk-based standards. Estonia, Singapore, and the United Kingdom exemplify three distinct yet equally successful approaches to public-sector cybersecurity governance. Their experiences offer valuable insights for Indonesia's reform pathway.

Estonia's model is globally recognized as the most integrated and comprehensive. Following the 2007 nationwide cyberattacks, Estonia embedded cybersecurity deep within its constitutional and administrative architecture, establishing the Estonian Information System Authority (RIA), a national incident reporting obligation, and the X-Road interoperability layer that ensures secure data exchange across government systems.[4] Estonia's success illustrates the importance of national coherence, legal clarity, and digitally embedded security mechanisms.

Singapore adopts a centralized, enforcement-driven model anchored in the Cybersecurity Act 2018, granting the Cyber Security Agency (CSA) strong regulatory authority over critical information infrastructure, mandatory audits, compulsory incident reporting, and cybersecurity directives.[5] Singapore's hybrid of preventive regulation and authoritative oversight has consistently positioned the country among the highest tiers of global cybersecurity governance rankings.[6]

The United Kingdom presents a mature and risk-based governance model that blends legal obligations with institutional guidance. The establishment of the National Cyber Security Centre (NCSC) in 2016 consolidated cybersecurity expertise, providing public institutions with technical, legal, and procedural frameworks. Combined with the NIS

---

[3] OECD, *OECD Digital Government Studies*, *OECD E-Government Studies*, 2020, https://www.oecd.org/en/publications/oecd-digital-government-studies_24131962.html.

[4] Eneken Tikk and Anna-Maria Taliharm, *International Cyber Security Legal & Policy Proceedings*, 2010, https://ccdcoe.org/uploads/2010/01/LP_Proceedings_2010-2.pdf.

[5] E. Gorian, "Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection," in *Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and Production*, 2020, 1–9, https://doi.org/10.1007/978-3-030-15577-3_1.

[6] OECD, *OECD Digital Government Studies*.

Regulations and the UK's whole-of-government risk management approach, this model promotes both compliance and adaptability.[7] The UK's reliance on layered governance—statutory rules, specialized agencies, and institutional autonomy—demonstrates a flexible yet robust structure for managing public-sector cyber risks.

Comparative studies show that all three jurisdictions share core governance features absent in Indonesia:

1. Sector-specific legal mandates governing cybersecurity in public institutions;
2. A centralized national cybersecurity authority with clear enforcement powers;
3. Mandatory risk assessment and incident reporting; and
4. Strong oversight mechanisms, including judicial and administrative accountability.[8]

This gap gives rise to a crucial research problem: Indonesia lacks a legally grounded, institutionally coherent cybersecurity governance model for public institutions. Existing academic literature on Indonesian cybersecurity remains heavily technical or policy-oriented, with limited engagement from legal scholars in developing holistic frameworks grounded in administrative law, regulatory theory, and comparative legal insights.[9] As a result, Indonesia's legal scholarship has yet to articulate a comprehensive model for cybersecurity governance capable of supporting state resilience in the digital era.

This article addresses that gap by proposing a Legal Risk Assessment Model for Indonesia's public-sector cybersecurity governance. Developed through normative legal research and comparative analysis, the model integrates doctrinal clarity, institutional design principles, and risk management frameworks adapted from leading cybersecurity jurisdictions. The objective is not to transplant foreign systems wholesale but to identify normative and structural elements compatible with Indonesia's constitutional framework, administrative law principles, and digital transformation agenda.

This study argues that Indonesia must transition from a fragmented, reactive cybersecurity framework toward an integrated, statute-based governance system emphasizing centralized authority, legal compliance, and standardized risk management. Only through such transformation can Indonesia safeguard critical information assets, ensure service continuity, and reinforce public trust in an increasingly digital state. The proposed model aims to support that transition by offering legally grounded, structurally coherent, and contextually appropriate solutions for Indonesia's public-sector cybersecurity governance.

---

[7] National Cyber Security Office, "NCSC Annual Review 2022 ," NCSC.GOV.UK, accessed November 18, 2025, https://www.ncsc.gov.uk/collection/annual-review-2022.

[8] ENISA, "National Cybersecurity Strategies Guidelines & Tools," ENISA, 2021, https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/national-cybersecurity.

[9] Mohammad Fadil Imran, Hendra Gunawan, and Dwi Asmoro, "Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty," *Jurnal Manajemen Pelayanan Publik* 8, no. 2 (June 1, 2024): 275–90, https://doi.org/10.24198/jmpp.v8i2.52212.

RESEARCH METHODOLOGY

This study employs a normative legal research methodology combined with comparative legal analysis to examine and evaluate cybersecurity governance frameworks applicable to public institutions. The normative approach is used to analyze the coherence, adequacy, and conceptual structure of Indonesia's cybersecurity laws, institutional arrangements, and regulatory instruments, while the comparative method draws from governance models in Estonia, Singapore, and the United Kingdom to identify doctrinal principles and institutional mechanisms that may guide Indonesia's legal reform. Normative legal research, which focuses on legal norms, statutory frameworks, judicial reasoning, and conceptual structures, is applied here to Indonesian cybersecurity laws—including the ITE Law, the Personal Data Protection Law, Presidential Regulation No. 53/2017 on BSSN, and various sectoral rules governing critical information infrastructure—and examines their coherence, hierarchical structure, enforceability, and doctrinal clarity.[10] This approach also reveals legal gaps and structural inconsistencies, such as the absence of a unified statutory definition of cybersecurity governance responsibilities, which creates fragmented implementation across institutions; additionally, the normative analysis considers the connection between cybersecurity obligations and administrative law principles like accountability, due process, proportionality, and institutional clarity.[11] At the same time, the comparative legal method is employed because cybersecurity governance reflects diverse global regulatory models. Through a functional comparison, the study evaluates how Estonia, Singapore, and the United Kingdom address similar governance challenges such as securing digital public-sector infrastructure, managing cybersecurity risks, enforcing compliance, and maintaining institutional accountability.[12] The comparison examines statutory definitions of obligations, institutional governance structures (RIA in Estonia, CSA in Singapore, NCSC in the UK), incident reporting mandates, critical information infrastructure regulations, enforcement mechanisms, interagency coordination, and risk assessment frameworks, not to transplant foreign models but to extract governance principles compatible with Indonesia's legal and administrative context.[13]

This research draws upon three categories of legal materials. Primary sources include statutory texts, regulations, national strategies, constitutional provisions, and official government documents from Indonesia (ITE Law, PDP Law, Presidential Regulation No. 53/2017), Estonia (Cybersecurity Act 2018 and X-Road regulatory framework), Singapore (Cybersecurity Act 2018 and subsidiary regulations), and the United Kingdom (NIS Regulations 2018, Computer Misuse Act 1990, NCSC Guidelines), as well as OECD and ENISA frameworks treated as primary-soft law for comparative purposes.[14]

---

[10] Dr. Johnny Ibrahim, *Teori & Metodologi Penelitian Hukum Normatif* (Bayu Media, 2013).
[11] Satjipto Rahardjo, *Ilmu Hukum*, 8th ed. (Bandung: PT Citra Aditya Bakti, 2014).
[12] Konrad Zweigert and Hein Kotz, *Introduction to Comparative Law* (New York: Oxford University Press, 1998).
[13] Pierre Legrand, "The Impossibility of 'Legal Transplants,'" *Maastricht Journal of European and Comparative Law* 4, no. 2 (June 1, 1997): 111–24, https://doi.org/10.1177/1023263X9700400202.
[14] Gorian, "Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection."

Secondary sources consist of legal commentaries, monographs, academic books, and articles from leading journals such as Computer Law & Security Review, Government Information Quarterly, Journal of Cyber Policy, and International Journal of Public Administration in the Digital Age, which supply doctrinal interpretation and theoretical insights relevant to cybersecurity governance.[15] Tertiary sources include reports, policy analyses, and benchmarking tools from the OECD, ENISA, the ITU Global Cybersecurity Index, the UK's NCSC annual reports, and Singapore's CSA publications, providing cross-jurisdictional indicators of cybersecurity maturity and institutional performance.[16]

To analyze Indonesia's cybersecurity governance model systematically, the study applies an integrated analytical framework combining grammatical-textual interpretation, systematic interpretation, teleological interpretation, institutional analysis, and risk governance evaluation. Grammatical interpretation is used to determine statutory intent and definitional precision concerning terms like "electronic systems," "critical information infrastructure," "personal data," and "cyber incident."[17] Systematic interpretation evaluates the coherence among various regulatory layers—constitutional mandates, statutory laws, presidential regulations, and sectoral guidelines—and assesses whether they form a unified governance regime or remain fragmented.[18] Teleological interpretation examines whether cybersecurity regulations achieve their intended objectives such as national security protection, service continuity, public-data safeguarding, and enhancement of administrative trust within digital governance.[19] Institutional analysis evaluates the authority, coordination capacity, enforcement mechanisms, administrative accountability, and reporting structures of Indonesian public institutions, drawing lessons from the institutional architectures of Estonia, Singapore, and the UK.^11 Because cybersecurity governance is fundamentally risk-based, the study also examines how legal frameworks address risk identification, risk assessment, risk mitigation, incident response, and post-incident accountability, and whether Indonesia's system provides standardized governance tools or leaves risk management overly discretionary.[20]

The jurisdictions selected—Estonia, Singapore, and the United Kingdom—are justified based on their demonstrable strengths. Estonia is widely recognized as one of the world's most advanced digital states, integrating cybersecurity into its constitutional doctrine, administrative systems, and national resilience planning.[21] Singapore provides a leading

---

[15] Jacqueline Lipton, *Rethinking Cyberlaw* (Edward Elgar Publishing, 2015), https://doi.org/10.4337/9781781002186.

[16] OECD, "OECD Public Governance Reviews: Estonia and Finland," in *OECD Public Governance Reviews*, OECD Public Governance Reviews (OECD, 2015), https://doi.org/10.1787/9789264229334-EN.

[17] Karen Renaud et al., "Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious?," *Computers & Security* 78 (September 2018): 198–211, https://doi.org/10.1016/j.cose.2018.06.006.

[18] Imran, Gunawan, and Asmoro, "Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty."

[19] Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review* 113, no. 2 (December 1999): 501, https://doi.org/10.2307/1342331.

[20] National Cyber Security Office, "NCSC Annual Review 2022 ."

[21] e-Estonia, "X-Road: The Backbone of Estonia's Interoperable Digital State," Tallin, 2022, https://e-estonia.com/solutions/interoperability-services/x-road/.

Southeast Asian model with strong centralization, strict enforcement, and sophisticated regulatory design relevant to Indonesia's administrative context.[22] The United Kingdom offers a mature hybrid system that balances statutory obligations with expert institutional guidance and risk-management frameworks, providing insights into moderately centralized but highly capable governance structures.[23] This study acknowledges several limitations, including its focus solely on public-institution cybersecurity (excluding defense and full private-sector arrangements), its reliance on document-based analysis rather than empirical fieldwork, comparative constraints arising from contextual differences, and the inherent dynamism of cybersecurity law, which evolves faster than academic publications. Nonetheless, the normative-comparative methodology remains the most appropriate for constructing a legally grounded cybersecurity governance model tailored to Indonesia's institutional needs.

RESULT AND DISCUSSION

Cybersecurity Legal Frameworks in Indonesia, Estonia, Singapore, and the United Kingdom

Cybersecurity governance is shaped at the intersection of statutory regulation, institutional design, administrative practice, and national strategic priorities. Public institutions, as custodians of critical state functions and sensitive population data, constitute essential components of a country's digital security landscape. Therefore, a robust cybersecurity governance framework must provide clear legal mandates, coherent institutional structures, and enforceable obligations for risk assessment, incident reporting, and security controls. This section analyzes the legal frameworks governing cybersecurity in Indonesia and compares them with the more advanced models of Estonia, Singapore, and the United Kingdom. Through this comparison, key normative, structural, and operational dimensions of cybersecurity governance are identified.

1. Indonesia's Cybersecurity Legal Framework

Indonesia's cybersecurity regulation is rooted in a fragmented landscape composed of several statutes, presidential regulations, and sectoral rules. The Electronic Information and Transactions Law (ITE Law) and its amendments serve as the foundational law governing electronic systems and digital interactions. However, the ITE Law focuses primarily on regulating electronic transactions, cybercrime offenses, and intermediary liability rather than establishing comprehensive cybersecurity governance for public institutions.[24]

The Personal Data Protection Law (PDP Law) 2022 introduces obligations relating to data security, breach notification, and administrative sanctions. While significant, the PDP Law remains centered on information privacy rather than holistic cybersecurity

[22] Cyber Security Agency of Singapore, "Singapore Cyber Landscape 2022" (Singapore, 2023), https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2022/.
[23] UK Cabinet Office, "National Cyber Strategy 2022 Pioneering a Cyber Future with the Whole of the UK," 2022.
[24] Ahmad M Ramli et al., *Hukum Telematika*, Kedua (Tangerang Selatan: Universitas Terbuka, 2020).

governance. Moreover, its enforcement authority is still in transition, leaving regulatory gaps concerning institutional compliance and risk management practices.[25]

Indonesia created the National Cyber and Encryption Agency (BSSN) through Presidential Regulation No. 53/2017, later strengthened by Perpres No. 133/2017. BSSN is formally designated as the national cybersecurity authority responsible for coordinating cyber defense, incident response, and national resilience. However, the absence of a dedicated Cybersecurity Act limits BSSN's statutory authority, restricting its ability to impose mandatory compliance standards, conduct audits, or enforce penalties against public institutions that fail to meet cybersecurity requirements.[26]

Sectoral regulators—such as Kominfo, OJK, BI, and the Ministry of Energy—continue to issue their own cybersecurity regulations for their respective critical infrastructure domains. This creates a decentralized regulatory ecosystem in which cybersecurity responsibilities vary widely across agencies, leading to inconsistencies, duplication, and gaps in oversight.[27]

Furthermore, although Indonesia's Government Regulation No. 71/2019 (PP 71/2019) mandates security standards for electronic systems classified as "strategic," "high," or "low" risk, public institutions seldom comply due to the absence of auditing mechanisms and legally binding penalties. Consequently, cybersecurity standards are often treated as recommendations rather than enforceable obligations.[28] This fragmented legal landscape reflects Indonesia's struggle to transition from technical cybersecurity provisions to a governance-based regulatory architecture.

2. Estonia's Cybersecurity Legal Framework

Estonia is globally recognized as a pioneer in cybersecurity governance due to its integrated digital state infrastructure and well-established national strategies. The Cybersecurity Act (2018) serves as Estonia's principal legal framework, requiring both public and private institutions to implement risk management systems, conduct regular audits, and report incidents to the Estonian Information System Authority (RIA).[29]

A defining feature of Estonia's model is the X-Road interoperability system, a secure data exchange platform that enforces standardized encryption, digital signatures, and access control across all government agencies. This ensures security-by-design at the architectural level rather than relying solely on institutional compliance.[30] Estonia mandates comprehensive cybersecurity obligations for public institutions, including:

---

[25] DLA, "Data Protection Laws in Indonesia," 2023, https://www.dlapiperdataprotection.com/?t=law&c=ID.

[26] Damar Apri Sudarmadi and Arthur Josias Simon Runturambi, "Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber Di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional* 2, no. 2 (December 25, 2019), https://doi.org/10.7454/jkskn.v2i2.10028.

[27] Imran, Gunawan, and Asmoro, "Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty."

[28] Annual Cyber Security, "Estonian Information System Authority," *Estonian Information System Authority: Annual Cyber Security Assessment*, 2019.

[29] Damjan Štrucl, "Comparative Study on the Cyber Defence of NATO Member States," *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, 2021, www.ccdcoe.org.

[30] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011).

a. Continuous risk assessment
b. Mandatory incident reporting
c. Compliance with baseline security standards
d. Annual security audits conducted by certified assessors
e. Institutional-level cybersecurity coordinators

These requirements are legally enforceable, and RIA holds authority to issue binding orders and impose corrective measures.[31] Estonia's approach is reinforced by national resilience strategies established after the 2007 cyberattacks, integrating cybersecurity into its constitutional doctrine and national defense structures. The country's State Information System Authority Act and Emergency Act further emphasize cybersecurity as a core public function under administrative law and national security law.[32] Estonia's system exemplifies legal clarity, technological integration, and centralized cybersecurity governance—features still absent in Indonesia.

3. Singapore's Cybersecurity Legal Framework

Singapore maintains one of the most centralized and enforcement-oriented cybersecurity governance systems in the world. The Cybersecurity Act 2018 provides a strong statutory foundation, granting comprehensive regulatory powers to the Cyber Security Agency (CSA).^10 The Act establishes:

a. Legal definitions of cybersecurity incidents
b. Mandatory incident reporting for public institutions and critical infrastructure
c. Licensing frameworks for cybersecurity service providers
d. Government authority to issue enforcement directions and conduct investigations
e. Strong audit obligations for owners of critical information infrastructure (CII)

Public institutions in Singapore are required to comply with Government Instruction Manuals (IM8) and the Public Sector Governance Framework, which outline standardized security measures for data handling, network configuration, cloud usage, and access control. These standards are legally binding for all ministries and statutory boards.[33] Singapore's cybersecurity governance is supported by:

a. A national Cybersecurity Strategy (2021) emphasizing risk-based regulation
b. A centralized incident-response system integrated with national defense
c. Regular stress-testing and cybersecurity exercises (e.g., Cyber Star series)
d. Strong legal penalties for non-compliance

Singapore's success lies in its capacity to combine centralized statutory authority, mandatory compliance, and strategic foresight, placing it far ahead of Indonesia's fragmented model.

4. United Kingdom's Cybersecurity Legal Framework

The United Kingdom employs a hybrid model that balances statutory mandates, institutional guidance, and sectoral autonomy. The primary regulatory instruments

[31] Gorian, "Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection."
[32] Cyber Security Agency of Singapore, *The Singapore Cybersecurity Strategy*, 2021, https://ccdcoe.org/uploads/2018/10/Singapore_Cybersecurity_Strategy_2021.pdf.
[33] OECD, *OECD Digital Government Studies*.

include the Network and Information Systems (NIS) Regulations 2018, which implement the EU NIS Directive until 2020 and remain in force post-Brexit with national modifications.[34] The NIS Regulations impose:

a. Mandatory cybersecurity standards for operators of essential services
b. Incident reporting obligations
c. Competent authority oversight (e.g., Department for Health, Ofcom, Energy regulators)
d. Significant administrative penalties for non-compliance
e. Complementing the NIS regime is the National Cyber Security Centre (NCSC), established in 2016 under GCHQ. NCSC functions as the UK's technical authority, offering:
f. Risk-assessment frameworks (e.g., Cyber Assessment Framework – CAF)
g. Guidance for public agencies
h. Threat intelligence services
i. Incident response coordination

The UK's National Cyber Strategy (2022) emphasizes whole-of-government risk governance, integrating cyber planning across ministries and public-sector bodies.[35] UK public institutions are required to follow best-practice standards such as:

a. Cyber Essentials
b. ISO/IEC 27001
c. Government Security Classifications Policy

Unlike Singapore, the UK does not centralize all cybersecurity authority under a single agency. Instead, it relies on a layered governance model combining statutory obligations, specialized regulators, and centralized technical guidance from NCSC.[36]

5. Comparative Findings

Table 1 Comparative Overview of Cybersecurity Governance Frameworks

Aspect	**Estonia**	**Singapore**	**United Kingdom**	**Indonesia**
Legal Coherence	Possesses a comprehensive and integrated Cybersecurity Act.	Has the Cybersecurity Act 2018 with clear regulatory scope.	Operates under the NIS Regulations and coherent supporting legislation.	Lacks a dedicated Cybersecurity Act; legal framework remains fragmented and weakly enforceable.

[34] "The NIS Regulations 2018," GOV.UK, January 4, 2023, https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018.
[35] UK Cabinet Office, "National Cyber Strategy 2022 Pioneering a Cyber Future with the Whole of the UK."
[36] National Cyber Security Centre, "Cyber Assessment Framework ," NCSC.GOV.UK, 2021, https://www.ncsc.gov.uk/collection/cyber-assessment-framework.

Aspect	Estonia	Singapore	United Kingdom	Indonesia
Institutional Authority	RIA holds statutory oversight and enforcement powers.	CSA has strong statutory authority for audits, investigations, and enforcement.	NCSC provides unified guidance; enforcement authority is distributed across sectoral regulators.	BSSN lacks binding enforcement authority under the current legal framework.
Mandatory Risk Management	Requires risk assessments, audits, and mandatory incident reporting.	Imposes strict risk management and auditing obligations for CII operators.	NIS Regulations mandate compliance with standardized risk-management requirements.	Risk-management obligations remain declaratory rather than enforceable.
Incident Reporting Systems	Mandatory incident reporting with statutory penalties for non-compliance.	Mandatory reporting overseen by CSA with enforcement mechanisms.	Incident reporting required under NIS, supervised by competent authorities.	No unified mandatory incident reporting system for public institutions.
Administrative Accountability	Cybersecurity embedded within administrative law and national accountability structures.	Strong administrative mechanisms for oversight of cybersecurity negligence.	Accountability enforced through risk standards, regulatory compliance, and sectoral evaluation.	No established judicial doctrines or administrative accountability mechanisms addressing cybersecurity negligence.

Source: Author's Analysis

These differences indicate that Indonesia must evolve toward a coherent, enforceable, and institutionally integrated cybersecurity governance model to support its digital transformation.

Doctrinal and Institutional Weaknesses in Indonesia's Cybersecurity Governance

Despite Indonesia's rapid digital transformation, its cybersecurity governance remains constrained by foundational weaknesses at the doctrinal, institutional, and operational levels. These systemic deficiencies not only undermine national cybersecurity resilience but also impede the ability of public institutions to manage cyber risks effectively. This section examines key doctrinal and institutional flaws in Indonesia's current cybersecurity framework, illustrating how regulatory fragmentation, ambiguous legal norms, and weak institutional authority collectively hinder the formation of a coherent public-sector cybersecurity governance model.

1. Doctrinal Weaknesses in Indonesia's Cybersecurity Regulation

Doctrinal weaknesses reflect inconsistencies and gaps in the legal principles underlying Indonesia's cybersecurity framework. These weaknesses stem from fragmented legislation, unclear definitions, overlapping mandates, and the absence of enforceable standards.

a. Fragmented and Overlapping Cybersecurity Legislation

Indonesia's cybersecurity regulation lacks a unified statutory foundation. Instead of a dedicated Cybersecurity Act, cybersecurity-related provisions are dispersed across various laws, including the ITE Law, PDP Law, Perpres 53/2017on BSSN, PP 71/2019, and numerous sectoral regulations. This fragmentation creates doctrinal inconsistencies that complicate regulatory interpretation and implementation.

For example, the ITE Law contains provisions on electronic system reliability but does not articulate a comprehensive cybersecurity governance structure for public institutions.[37] Similarly, the PDP Law mandates security measures for personal data controllers but does not establish standardized cybersecurity obligations beyond data protection.[38] As a result, cybersecurity responsibilities across government institutions are ambiguous and lack uniformity.

Comparative jurisdictions illustrate the importance of doctrinal consolidation. Estonia's Cybersecurity **Act 2018**, Singapore's Cybersecurity Act, and the UK's NIS Regulations provide unified legal frameworks that articulate state responsibilities, institutional authority, and enforceable obligations. Indonesia lacks such doctrinal coherence.[39]

b. Absence of Clear Legal Definitions and Taxonomy

Indonesian law lacks clear definitions for key cybersecurity concepts, including:

1) "Cybersecurity Incident"
2) "critical Information Infrastructure"
3) "Cyber Risk"
4) "Security Baseline"
5) "National Cyber Resilience"
6) "Government information system security"

[37] Ramli et al., *Hukum Telematika*.
[38] DLA, "Data Protection Laws in Indonesia."
[39] Annual Cyber Security, "Estonian Information System Authority."

PP 71/2019 introduces classifications for electronic systems but does not provide detailed risk taxonomies or criteria for identifying critical systems.^4 This doctrinal ambiguity results in inconsistent interpretations across ministries and regional governments. In contrast, Singapore defines CII sectors clearly, and Estonia's cyber law provides specific definitions for incident severity levels, reporting thresholds, and system criticality.[40]

c. Weak Legal Obligations for Risk Management and Auditing

Indonesian public institutions are not legally bound to conduct:

1) Periodic cybersecurity audits
2) Risk assessments
3) Penetration tests
4) Incident simulations
5) Vulnerability assessments

Existing guidelines from Kominfo and BSSN remain largely advisory rather than mandatory. Without statutory force, most agencies treat cybersecurity assessments as optional.[41] By contrast, Estonia requires annual audits for public institutions, Singapore mandates CII audits every two years, and the UK enforces risk assessment obligations under NIS Regulations.[42]

d. Lack of Mandatory Incident Reporting

Indonesia lacks a nationwide, legally binding incident-reporting obligation for public institutions. Current systems rely on voluntary reporting to BSSN, and many agencies choose not to report cybersecurity incidents to avoid reputational risks or administrative scrutiny. This undermines national situational awareness and cripples coordinated response efforts.[43] Comparatively:

1) Estonia imposes strict reporting deadlines to RIA.
2) Singapore mandates immediate reporting for CII sectors.
3) The UK requires timely reporting to competent authorities under NIS.
4) The absence of a statutory incident reporting duty represents a major doctrinal gap in Indonesia's cybersecurity framework.

e. Inadequate Legal Accountability Mechanisms

Indonesian administrative law lacks clear doctrines addressing cybersecurity negligence in public institutions. There is no judicial precedent or administrative regulation defining liability for:

1) Failure to implement cybersecurity measures.
2) Negligence leading to data breaches.
3) Inadequate incident response.
4) Systemic non-compliance with security standards.

---

[40] OECD, *OECD Digital Government Studies*.
[41] Gorian, "Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection."
[42] Sudarmadi and Runturambi, "Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber Di Indonesia."
[43] Štrucl, "Comparative Study on the Cyber Defence of NATO Member States."

In contrast, Singapore's Cybersecurity Act provides for fines and enforcement actions for institutional negligence, and the UK's NIS Regulations impose penalties for failure to mitigate risks or report incidents.[44]

Indonesia's inability to assign legal accountability prevents the establishment of a governance culture that prioritizes cybersecurity.

2. Institutional Weaknesses in Indonesia's Cybersecurity Governance

Institutional weaknesses constitute a central challenge to Indonesia's cybersecurity resilience. These include limited statutory authority, overlapping mandates, weak coordination, limited oversight, and uneven institutional capacity.

a. Limited Statutory Authority of BSSN

Although BSSN is designated as Indonesia's national cybersecurity authority, it lacks strong statutory foundations. BSSN was created through a presidential regulation, not a dedicated law. Consequently, its authority is weaker than comparable agencies in advanced jurisdictions. BSSN cannot:

1) Issue binding cybersecurity directives.
2) Enforce mandatory audits.
3) Impose administrative sanctions.
4) Coordinate interagency compliance effectively.

In contrast:

1) Singapore's CSA is empowered by statute to conduct audits and issue binding directions.
2) Estonia's RIA holds legal authority to enforce compliance.
3) The UK relies on competent authorities with statutory power under the NIS regime.[45]
4) Without legislative empowerment, BSSN functions more as a coordinating body than an enforcement agency.

b. Overlapping Institutional Mandates and Regulatory Duplication

Multiple Indonesian institutions hold partial cybersecurity mandates, including:

1) BSSN (national cybersecurity coordination).
2) Kominfo (telecommunications and data governance.
3) OJK (financial sector cybersecurity).
4) BI (payment systems security).
5) Ministry of Defense (cyber defense).
6) Ministry of Home Affairs (regional cyber governance).

This overlapping jurisdiction results in:

1) Conflicting standards.
2) Duplicated reporting procedures.
3) Unclear institutional leadership.
4) Inconsistent enforcement.

[44] ENISA, "National Cybersecurity Strategies Guidelines & Tools."
[45] "The NIS Regulations 2018."

OECD's Digital Government Review notes that Indonesia's multiplicity of cybersecurity actors reduces policy coherence and limits strategic direction.[46]

c. Weak Cybersecurity Culture in Public Institutions

Many Indonesian public institutions lack internal cybersecurity governance structures, such as:

1) Chief Information Security Officers (cisos).
2) Cybersecurity committees.
3) SOC (Security Operation Center) teams.
4) Incident-response teams.
5) Enterprise risk management integration.

By contrast, Estonia requires each agency to appoint a security coordinator, Singapore mandates cybersecurity managers for CII owners, and UK public bodies are expected to follow NCSC governance structures.[47]

d. Insufficient Cyber Workforce and Institutional Capacity

Indonesia faces a significant shortage of cybersecurity professionals in the public sector. International analyses estimate that Indonesia lacks more than 150,000 skilled cybersecurity workers, affecting both national and regional governments.[48] Many agencies rely on general IT staff without specialized cybersecurity expertise, leading to misconfigurations, weak monitoring, and slow incident response.

e. Inadequate Funding and Resource Allocation

Cybersecurity budgets in many Indonesian public institutions are:

1) Not standardized.
2) Not risk-based.
3) Insufficient for modern infrastructure.
4) Allocated mainly for hardware procurement rather than governance, training, or auditing.

OECD findings indicate that Indonesia's digital spending is disproportionately directed toward technology acquisition rather than security lifecycle governance.[49]

f. Limited Coordination at National and Subnational Levels

Indonesia's decentralized governance structure complicates national cybersecurity coordination. Regional governments operate independently in allocating digital resources, managing IT systems, and responding to cyber incidents. This decentralization slows coordinated response efforts and creates vulnerabilities in critical digital services, such as population administration and health information systems.[50]

g. Lack of Independent Oversight and Accountability Mechanisms

Indonesia lacks an independent supervisory authority for cybersecurity comparable to:

1) Estonia's RIA.

---

[46] Cyber Security Agency of Singapore, "Singapore Cyber Landscape 2022."
[47] OECD, *OECD Digital Government Studies*.
[48] National Cyber Security Centre, "Cyber Security Governance," NCSC.GOV.UK, 2021, https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance.
[49] ISC2, "Cybersecurity Workforce Study," ISC2, 2022, https://www.isc2.org/research.
[50] OECD, "Government at a Glance Southeast Asia 2019," *Government at a Glance Southeast Asia 2019* (OECD, September 10, 2019), https://doi.org/10.1787/9789264305915-EN.

2) Singapore's CSA.
3) UK's competent authorities under NIS.

Current oversight mechanisms rely heavily on internal reporting, which is prone to bureaucratic bias, underreporting, and weak enforcement.

3. Implications of Doctrinal and Institutional Weaknesses

The combination of doctrinal incoherence and institutional fragility creates systemic vulnerabilities, such as:

a. Inconsistent preparedness across institutions.
b. Inability to detect and respond to cyber threats promptly.
c. Poor coordination during cyber incidents.
d. Lack of nationwide threat intelligence.
e. Absence of legal accountability for cybersecurity failures.
f. Erosion of public trust.

Moreover, Indonesia's digital transformation efforts—SPBE integration, digital ID expansion, national data governance initiatives—are at risk without strong cybersecurity governance foundations.

Development of the Legal Risk Assessment Model for Indonesia's Public Institutions

The assessment of Indonesia's cybersecurity framework reveals foundational weaknesses that cannot be resolved through incremental regulatory adjustments alone. Instead, the country requires the construction of a holistic governance model grounded in legal clarity, institutional authority, and standardized risk management. Drawing upon comparative insights from Estonia, Singapore, and the United Kingdom, this section develops a legal risk assessment model tailored specifically for Indonesia's public institutions. The model rests on the premise that cybersecurity in the public sector must be treated as a matter of administrative governance and legal responsibility rather than merely a technical or operational function.

At the conceptual level, the model recognizes that Indonesia's fragmented regulatory system—comprising the ITE Law, PDP Law, PP 71/2019, and an array of ministerial regulations—does not provide a coherent basis for cybersecurity governance. In contrast, countries such as Estonia and Singapore employ comprehensive statutes that clearly articulate institutional obligations, enforcement powers, and sectoral responsibilities. Indonesia must therefore begin by establishing a unifying legal foundation through a comprehensive Cybersecurity Act. Such an Act would consolidate dispersed provisions, provide clear statutory definitions, and introduce binding obligations for public-sector cybersecurity. Comparative experience demonstrates that regulatory consolidation strengthens compliance and enhances national cyber resilience, as seen in Estonia's Cybersecurity Act 2018 and Singapore's Cybersecurity Act.[51]

[51] OECD, *OECD Digital Government Studies*.

Central to the proposed model is the restructuring of institutional authority. Indonesia's National Cyber and Encryption Agency (BSSN) presently operates through a presidential regulation rather than statutory mandate, limiting its capacity to enforce compliance. A Cybersecurity Act should elevate BSSN into a national authority equipped with robust regulatory and supervisory powers. This includes the authority to issue binding security directives, conduct mandatory audits, coordinate national incident response, and impose sanctions for institutional negligence. Singapore's Cyber Security Agency and Estonia's Information System Authority provide compelling examples of how statutory empowerment enables a central authority to lead national cybersecurity governance effectively.[52] Strengthening BSSN would also resolve institutional overlaps that currently exist between Kominfo, OJK, BI, and other sectoral regulators by establishing a clear hierarchy of authority.

The model further emphasizes the need to institutionalize cybersecurity risk assessment within the bureaucratic fabric of public governance. Indonesia currently lacks legally mandated requirements for risk identification, documentation, or mitigation. Public institutions operate without standardized risk registers, cybersecurity audits, or vulnerability assessments, leading to substantial asymmetries in preparedness. By contrast, Estonia mandates periodic audits for all public institutions, the UK requires risk governance under the NIS Regulations, and Singapore enforces stringent audit obligations for critical information infrastructure owners.[53] Through a dedicated Cybersecurity Act, Indonesia can institutionalize annual risk assessments, external audits, penetration testing, and ongoing vulnerability management as mandatory governance practices for all ministries, regional authorities, and state institutions.

A critical deficiency in Indonesia's present system lies in the absence of mandatory incident reporting. Cyber incidents are frequently underreported, leaving national authorities with limited situational awareness. This prevents coordinated national responses and weakens resilience. A risk assessment model must therefore incorporate a unified and legally binding incident-reporting system. Public institutions should be obliged to report cybersecurity incidents—ranging from data breaches to system outages and malware intrusions—to the national authority within specified timelines. International models require reporting within strict deadlines, such as Singapore's immediate reporting rule for critical sectors and the UK's 72-hour reporting mandate under the NIS regime.[54] Indonesia's model should follow this trend to enhance national visibility and accelerate crisis coordination.

Effective cybersecurity governance also requires attention to supply-chain vulnerabilities. Indonesia increasingly relies on third-party vendors for cloud infrastructure, software platforms, and data management services. Many major incidents in the public sector emerge from weaknesses in outsourced systems, misconfigurations,

[52] Gorian, "Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection."
[53] Annual Cyber Security, "Estonian Information System Authority."
[54] "The NIS Regulations 2018."

or insufficient vendor oversight. The proposed model includes a legal requirement for supply-chain risk assessments, contractual cybersecurity clauses, and national guidelines for external vendor compliance. The UK's National Cyber Security Centre emphasizes supply-chain risk as one of the most significant systemic threats facing government institutions.[55] Indonesia's legal model must formally integrate vendor governance into public-sector cybersecurity.

Another essential component of the proposed model is the establishment of oversight mechanisms that ensure accountability and transparency. Indonesia currently lacks independent supervisory structures for cybersecurity, and administrative law does not explicitly address institutional negligence in digital governance. The Legal Risk Assessment Model recommends a combination of internal and external oversight mechanisms, including periodic performance evaluations, inter-ministerial monitoring, and the publication of anonymized cybersecurity audit results. Comparative experience demonstrates that transparency fosters public trust and incentivizes better compliance among agencies. Estonia's reporting practices and the UK's annual cybersecurity reviews represent best-practice benchmarks in this regard.[56]

Judicial and administrative remedies also constitute an indispensable element of the model. Indonesian courts should be empowered to review cybersecurity-related administrative decisions, adjudicate cases of institutional negligence, and enforce legal consequences for non-compliance. The absence of judicial doctrine on cybersecurity governance is one of Indonesia's most significant doctrinal gaps. Legal scholarship notes that without enforceable accountability structures, public institutions have little incentive to comply with governance-based cybersecurity norms.[57] The model urges the development of legal provisions enabling courts to play an active role in upholding administrative accountability in the digital sector.

Collectively, these components—statutory coherence, centralized authority, risk assessment obligations, mandatory reporting, supply-chain governance, and oversight mechanisms—form a unified Legal Risk Assessment Model for Indonesia's public institutions. Rather than focusing solely on technological measures, the model conceptualizes cybersecurity as a field of administrative governance rooted in legal duties, institutional structures, and risk management processes. It operationalizes cybersecurity as a continuous cycle of risk identification, assessment, mitigation, monitoring, and accountability.

This holistic approach offers several advantages. First, it enhances national resilience by ensuring that public institutions maintain consistent and enforceable standards. Second, it reduces regulatory fragmentation through legislative consolidation and strengthened institutional authority. Third, it improves public trust by fostering transparency and

[55] National Cyber Security Centre, "Supply Chain Security Guidance," NCSC.GOV.UK, 2021, https://www.ncsc.gov.uk/collection/supply-chain-security.
[56] UK Cabinet Office, "National Cyber Strategy 2022 Pioneering a Cyber Future with the Whole of the UK."
[57] Imran, Gunawan, and Asmoro, "Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty."

accountability, particularly in cases of data breaches and service disruptions. Fourth, it aligns Indonesia with global best practices, improving the country's standing in international cybersecurity indices and strengthening the credibility of its digital governance initiatives.

Ultimately, the Legal Risk Assessment Model acknowledges that Indonesia's digital transformation cannot advance sustainably without the parallel maturation of its cybersecurity governance framework. As public services migrate into digital environments, the integrity of those environments becomes synonymous with the integrity of the state itself. Through a legally grounded and institutionally robust risk governance model, Indonesia can safeguard its digital future while strengthening the foundations of public administration.

CONCLUSION

Indonesia's accelerating transition toward digital governance has placed cybersecurity at the forefront of national administrative reform. Public institutions now oversee vast databases, interconnected platforms, and critical digital infrastructures that underpin essential state functions. Yet the analysis conducted throughout this study makes clear that Indonesia's cybersecurity governance framework remains fundamentally incomplete. Fragmented legal mandates, unclear institutional responsibilities, inconsistent implementation, and the absence of standardized risk-management procedures collectively weaken the country's resilience against increasingly sophisticated cyber threats. These structural weaknesses not only jeopardize the continuity and reliability of public services but also erode public confidence in the state's ability to safeguard digital systems and personal data.

Comparative examination of Estonia, Singapore, and the United Kingdom demonstrates that strong cybersecurity governance is inseparable from legal coherence, institutional authority, and enforceable accountability. These jurisdictions show that effective public-sector cybersecurity is not built merely through technological sophistication but through the systematic alignment of law, governance, and risk management. Estonia exemplifies the power of integrated legislation and architectural security-by-design; Singapore shows the importance of centralized oversight and strict statutory compliance; while the UK illustrates the strength of a flexible but institutionalized risk-based ecosystem. Together, these cases illuminate the deficiencies within Indonesia's framework and the urgent need for a structured legal response.

Drawing from these insights, this article proposes the Legal Risk Assessment Model (LRAM) as a comprehensive governance architecture tailored to Indonesia's administrative landscape. The model emphasizes the need for a unified Cybersecurity Act that consolidates dispersed regulations into a coherent statutory framework. It calls for the empowerment of BSSN as a national authority with regulatory and enforcement capacities, ensuring consistent oversight across ministries, regional governments, and state institutions. It also embeds cybersecurity into the legal obligations of public bodies by mandating risk assessments, independent audits, incident reporting, and supply-chain

security measures. Furthermore, the model integrates oversight and accountability mechanisms that involve both administrative and judicial review, thereby reinforcing a culture of responsibility and transparency within the public sector.

These reforms are not merely technical adjustments; they constitute a shift toward a governance paradigm in which cybersecurity is understood as an essential component of administrative law and public accountability. By institutionalizing risk governance, Indonesia can move from reactive cybersecurity practices toward a proactive, coordinated, and legally enforceable system. Such a transformation is indispensable for supporting the country's long-term digital ambitions, including nationwide SPBE integration, data interoperability, and the expansion of secure digital public services.

In practical terms, Indonesia must prioritize the drafting of a comprehensive Cybersecurity Act that clarifies institutional mandates, sets minimum security standards, and formalizes risk-management obligations. The government must also strengthen BSSN's legal authority and streamline interagency coordination to eliminate overlapping jurisdictions. Public institutions should adopt standardized risk registers, conduct mandatory audits, and report incidents promptly to the national authority. Parallel to these measures, Indonesia must invest in human resource development by training cybersecurity professionals and establishing structured cybersecurity governance units within all ministries and regional governments. Transparency—through the publication of audit summaries, incident reports, and budget allocations—is also essential for enhancing public trust and ensuring accountability.

The path toward strong cybersecurity governance is complex, requiring sustained political commitment, legal precision, institutional reform, and cultural change within the public sector. Nevertheless, the benefits of adopting the Legal Risk Assessment Model are substantial. A coherent governance system will provide greater protection for national data assets, improve service reliability, enhance Indonesia's position in international cybersecurity rankings, and build public confidence in the state's digital transformation. Most importantly, it will establish cybersecurity as an integral component of sound public administration and national resilience.

SUGGESTION

Indonesia stands at a critical juncture. As digital transformation accelerates, cybersecurity must evolve from a peripheral technical consideration into a core pillar of governance and public trust. Through the implementation of a unified legal framework, empowered institutions, and standardized risk-management practices, Indonesia can strengthen its ability to navigate the complex cyber landscape of the future. The Legal Risk Assessment Model offered in this article provides a structured path toward this objective. Its adoption will help ensure that Indonesia's digital transformation is not only ambitious, but secure, sustainable, and resilient.

REFERENCES

1. Annual Cyber Security. "Estonian Information System Authority." Estonian Information System Authority: Annual Cyber Security Assessment, 2019.
2. Cyber Security Agency of Singapore. "Singapore Cyber Landscape 2022." Singapore, 2023. https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2022/.
3. ———. The Singapore Cybersecurity Strategy, 2021. https://ccdcoe.org/uploads/2018/10/Singapore_Cybersecurity_Strategy_2021.pdf.
4. Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security." Journal of Cyber Warfare and Terrorism 1, no. 1 (2011).
5. DLA. "Data Protection Laws in Indonesia," 2023. https://www.dlapiperdataprotection.com/?t=law&c=ID.
6. e-Estonia. "X-Road: The Backbone of Estonia's Interoperable Digital State." Tallin, 2022. https://e-estonia.com/solutions/interoperability-services/x-road/.
7. ENISA. "National Cybersecurity Strategies Guidelines & Tools." ENISA, 2021. https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/national-cybersecurity.
8. Gorian, E. "Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection." In Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and Production, 1–9, 2020. https://doi.org/10.1007/978-3-030-15577-3_1.
9. Ibrahim, Dr. Johnny. Teori & Metodologi Penelitian Hukum Normatif. Bayu Media, 2013.
10. Imran, Mohammad Fadil, Hendra Gunawan, and Dwi Asmoro. "Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty." Jurnal Manajemen Pelayanan Publik 8, no. 2 (June 1, 2024): 275–90. https://doi.org/10.24198/jmpp.v8i2.52212.
11. International Telecommunication Union Development Sector. Global Cybersecurity Index 2020, n.d.
12. ISC2. "Cybersecurity Workforce Study." ISC2, 2022. https://www.isc2.org/research.
13. Legrand, Pierre. "The Impossibility of 'Legal Transplants.'" Maastricht Journal of European and Comparative Law 4, no. 2 (June 1, 1997): 111–24. https://doi.org/10.1177/1023263X9700400202.
14. Lessig, Lawrence. "The Law of the Horse: What Cyberlaw Might Teach." Harvard Law Review 113, no. 2 (December 1999): 501. https://doi.org/10.2307/1342331.
15. Lipton, Jacqueline. Rethinking Cyberlaw. Edward Elgar Publishing, 2015. https://doi.org/10.4337/9781781002186.
16. Marwan, Awaludin, Diana Odier-Contreras Garduño, and Fiammetta Bonfigli.

"Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia." BESTUUR 10, no. 1 (August 6, 2022): 22. https://doi.org/10.20961/bestuur.v10i1.59143.
17. National Cyber Security Centre. "Cyber Assessment Framework ." NCSC.GOV.UK, 2021. https://www.ncsc.gov.uk/collection/cyber-assessment-framework.
18. ———. "Cyber Security Governance." NCSC.GOV.UK, 2021. https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance.
19. ———. "Supply Chain Security Guidance." NCSC.GOV.UK, 2021. https://www.ncsc.gov.uk/collection/supply-chain-security.
20. National Cyber Security Office. "NCSC Annual Review 2022 ." NCSC.GOV.UK. Accessed November 18, 2025. https://www.ncsc.gov.uk/collection/annual-review-2022.
21. OECD. "Government at a Glance Southeast Asia 2019." Government at a Glance Southeast Asia 2019. OECD, September 10, 2019. https://doi.org/10.1787/9789264305915-EN.
22. ———. OECD Digital Government Studies. OECD E-Government Studies, 2020. https://www.oecd.org/en/publications/oecd-digital-government-studies_24131962.html.
23. ———. "OECD Public Governance Reviews: Estonia and Finland." In OECD Public Governance Reviews. OECD Public Governance Reviews. OECD, 2015. https://doi.org/10.1787/9789264229334-EN.
24. Rahardjo, Satjipto. Ilmu Hukum. 8th ed. Bandung: PT Citra Aditya Bakti, 2014.
25. Ramli, Ahmad M, Tasya Safiranita Ramli, Ferry Gunawan, Brilianing Pratiwi, Haryati, and Aris Suryana. Hukum Telematika. Kedua. Tangerang Selatan: Universitas Terbuka, 2020.
26. Renaud, Karen, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. "Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious?" Computers & Security 78 (September 2018): 198–211. https://doi.org/10.1016/j.cose.2018.06.006.
27. Štrucl, Damjan. "Comparative Study on the Cyber Defence of NATO Member States." NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2021. www.ccdcoe.org.
28. Sudarmadi, Damar Apri, and Arthur Josias Simon Runturambi. "Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber Di Indonesia." Jurnal Kajian Stratejik Ketahanan Nasional 2, no. 2 (December 25, 2019). https://doi.org/10.7454/jkskn.v2i2.10028.
29. "The NIS Regulations 2018." GOV.UK, January 4, 2023. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018.
30. Tikk, Eneken, and Anna-Maria Taliharm. International Cyber Security Legal & Policy Proceedings, 2010. https://ccdcoe.org/uploads/2010/01/LP_Proceedings_2010-2.pdf.

31. UK Cabinet Office. “National Cyber Strategy 2022 Pioneering a Cyber Future with the Whole of the UK,” 2022.
32. Zweigert, Konrad, and Hein Kotz. Introduction to Comparative Law. New York: Oxford University Press, 1998.