Jurnal Teknik Informatika dan Teknologi Informasi
Volume. 5 Nomor. 3 Desember 2025
E-ISSN .: 2827-9387, P-ISSN .: 2827-9379, Hal 434-450
DOI: https://doi.org/10.55606/jutiti.v5i3.6379
Tersedia: https://journalshub.org/index.php/jutiti

Comprehensive Cybersecurity Framework for Digital Governance: Threat Assessment, Risk Mitigation, and Regulatory Compliance in Indonesia

Wildan Maulana Assani Mualim[1*], Fitri Yul Dewi Marta[2], Ira Meiyenti[3]
[1-3] Fakultas Manajemen Pemerintahan, Institut Pemerintahan Dalam Negeri, Indonesia
Email : 35.0809@praja.ipdn.ac.id [1], fitri.yul@ipdn.ac.id [2] , irameiyenti@ipdn.ac.id [3]*

**Penulis Korespondensi: 35.0809@praja.ipdn.ac.id [1]*

Abstract*. Digital transformation of government administration brings significant benefits in improving public service efficiency and citizen access to information. However, digitalization also opens opportunities for increasingly complex and organized cyber threats. This journal explores a comprehensive cybersecurity framework for digital governance through an extensive literature review that includes threat assessment, risk mitigation strategies, and regulatory compliance analysis. This research analyzes international frameworks (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019), Indonesian national standards (Law No. 1 of 2024 on Information and Electronic Transactions, SPBE, BSSN), and best practices in incident response and Zero Trust Architecture. Results demonstrate that government cybersecurity requires a holistic approach integrating technical aspects, policy, human resources, and governance. This journal recommends implementing a comprehensive cybersecurity framework, enhancing human capital capacity, adopting cutting-edge technology, and fostering inter-institutional coordination to build sustainable cybersecurity resilience for government entities.*

Keywords*: Digital Transformation; Government Cybersecurity; Information Security Framework; Regulatory Compliance; Risk Mitigation.*

Abstrak. Transformasi digital dalam administrasi pemerintahan memberikan manfaat signifikan dalam meningkatkan efisiensi layanan publik dan akses masyarakat terhadap informasi. Namun, digitalisasi juga membuka peluang munculnya ancaman siber yang semakin kompleks dan terorganisasi. Jurnal ini mengkaji kerangka kerja keamanan siber yang komprehensif untuk tata kelola digital melalui tinjauan literatur yang luas, mencakup penilaian ancaman, strategi mitigasi risiko, dan analisis kepatuhan regulasi. Penelitian ini menganalisis berbagai kerangka kerja internasional (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019), standar nasional Indonesia (Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, SPBE, BSSN), serta praktik terbaik dalam respons insiden dan Arsitektur Zero Trust. Hasil penelitian menunjukkan bahwa keamanan siber pemerintah membutuhkan pendekatan holistik yang mengintegrasikan aspek teknis, kebijakan, sumber daya manusia, dan tata kelola. Jurnal ini merekomendasikan penerapan kerangka keamanan siber yang komprehensif, peningkatan kapasitas sumber daya manusia, adopsi teknologi mutakhir, serta penguatan koordinasi antar lembaga untuk membangun ketahanan keamanan siber yang berkelanjutan bagi entitas pemerintah.

Kata kunci: Keamanan Siber Pemerintah; Kepatuhan Regulasi; Kerangka Keamanan Informasi; Mitigasi Risiko; Transformasi Digital.

1. INTRODUCTION

The digital era has fundamentally transformed how government agencies function in serving society. The Electronic Government System (Sistem Pemerintahan Berbasis Elektronik or SPBE), regulated under Presidential Regulation No. 95 of 2018, serves as the backbone of modern public administration transformation in Indonesia (Peraturan Presiden Nomor 95 Tahun 2018, 2018). Electronic public services such as e-budgeting, e-office systems, and online service portals have facilitated millions of digital transactions daily.

Naskah Masuk: 17 September 2025; Revisi: 21 Oktober 2025; Diterima: 28 November 2025; Terbit: 11 Desember 2025

However, behind the opportunities brought by digital transformation lies an increasingly concerning cybersecurity risk. Cyber threats against government infrastructure no longer originate solely from ordinary criminals but from organized Advanced Persistent Threat (APT) groups sponsored by nation-states with high technical capabilities. In 2024, cybersecurity incidents in the Asia Pacific region reached unprecedented levels, with government institutions facing sophisticated multi-vector attacks combining spear-phishing, malware deployment, and supply chain compromise techniques. A significant incident reflecting these vulnerabilities is the ransomware attack on the National Data Center (PDN) in June 2024. Based on analysis by the National Cyber and Cryptography Agency (Badan Siber dan Sandi Negara or BSSN), the attack using LockBit 3.0 ransomware on June 20, 2024, paralyzed at least 210 central and local government institutions, with particular impact on immigration services at international airports (Tempo.co, 2024). This incident underscores the urgent need to strengthen the cybersecurity framework for government entities comprehensively and integrally.

Given these escalating challenges, a critical inquiry emerges regarding the adequacy of existing cybersecurity frameworks and regulatory mechanisms in anticipating increasingly complex threats targeting Indonesia's digital government infrastructure. This study therefore examines whether current national regulations and institutional safeguards are sufficient to respond to rapid threat evolution and explores how they can be aligned with globally recognized standards. Specifically, it seeks to determine the extent to which frameworks such as ISO/IEC 27001:2022, NIST CSF 2.0, and COBIT 2019 can be integrated with Indonesia's regulatory instruments—including the Electronic Information and Transactions Law, SPBE policies, and BSSN guidelines—to construct a coherent and comprehensive cybersecurity governance model. Furthermore, this research aims to identify effective mitigation strategies suited to various types of cyber threats, particularly those targeting strategic governmental sectors, and to formulate governance approaches that promote accountability, transparency, and alignment with good governance principles.

Within this context, the research addresses several key questions: (1) whether existing frameworks and regulations adequately anticipate evolving cyber threats; (2) how international and national standards can be consolidated into a unified cybersecurity framework; (3) which mitigation strategies are most effective for government-sector cyber risks; and (4) how accountable and transparent cybersecurity governance can be realized. Correspondingly, the study aims to analyze threat categories targeting digital government systems, evaluate the relevance of international and national frameworks for the Indonesian context, develop an

integrated cybersecurity model, and propose strategic roadmaps for sustainable implementation across short-, medium-, and long-term horizons.

2. LITERATURE REVIEW

Cyber Threat Landscape Against Digital Government

Major Categories of Cyber Threats

Cyber threats against government can be classified into several major categories. Recent systematization of cybersecurity regulations, standards and guidelines demonstrates the complexity of implementing comprehensive security frameworks across organizational contexts (Carello et al., 2023).

a. Advanced Persistent Threat (APT)

APT represents the most serious threat to government sectors. APT groups are state-sponsored cyber actors possessing high technical capabilities, unlimited financial resources, and long-term objectives to gain access to government systems and critical infrastructure. These groups employ sophisticated multi-stage deployment strategies utilizing publicly available tools combined with custom malware for reconnaissance, lateral movement, and data exfiltration. APT activities targeting government sectors in Southeast Asia have increased significantly during 2024-2025, with documented campaigns demonstrating advanced technical capabilities and strategic coordination.

Recent threat analysis reveals that government institutions face coordinated attacks combining multiple vectors: spear-phishing with targeted malware payloads, credential harvesting through phishing portals, exploitation of unpatched systems, and insider threat enablement through compromised legitimate accounts. The technical sophistication of these attacks includes memory-resident malware, fileless execution techniques, geofenced payload delivery, and advanced evasion mechanisms designed to bypass traditional endpoint detection and response systems.

b. Ransomware

Ransomware remains a pervasive threat to critical government infrastructure. The June 2024 PDN incident demonstrated the systemic impact of ransomware that could simultaneously paralyze hundreds of government institutions (Tempo.co, 2024). Recent cyber threat analysis indicates that ransomware-related attacks in the Asia Pacific region have intensified, with criminal operators employing dwell time techniques (prolonged presence in target systems for reconnaissance), sophisticated persistence methods, and

exfiltration-based extortion (threatening sensitive data publication in addition to encryption).

Active ransomware variants targeting public sectors use legitimate tools (Living off the Land Binaries), exploitation of stale credentials from previous phishing campaigns, and strategic delays between initial access and encryption to deepen penetration and maximize operational impact. Critical infrastructure paralysis has direct consequences for citizen services, data confidentiality, and organizational continuity.

c. Phishing and Social Engineering

Phishing remains the primary attack vector for breaching government cybersecurity through sophisticated social engineering campaigns. Contemporary techniques include spear-phishing with customized payloads targeting specific roles and responsibilities, malicious Office documents with macro-based payload delivery, and communication platform weaponization where legitimate applications are leveraged to distribute malware links in trusted contexts.

Impact of Threats on Public Services

Cyber attacks against government have cascading impacts that extend across multiple organizational and societal dimensions. Research demonstrates that cybersecurity failures can simultaneously disrupt critical service delivery, compromise citizen privacy, create financial losses, erode public trust, and impact national security (Savaş & Karataş, 2022). These impacts include:

a. Disruption of Critical Services: Paralysis of essential public services such as immigration, health, and population administration affecting government continuity and public welfare.
b. Data Breaches and Privacy Violations: Leakage of citizen personal data including identity numbers, addresses, and financial information creating identity theft and financial fraud risks.
c. Financial Losses: System recovery costs, ransomware demands, and long-term economic productivity losses affecting resource allocation.
d. Erosion of Public Trust: Decreased public confidence in government digital capabilities, hindering further e-services adoption and digital transformation progress.
e. National Security Impact: System compromise providing foreign actors access for intelligence gathering or critical infrastructure sabotage.

International Cybersecurity Frameworks

NIST Cybersecurity Framework 2.0

NIST released Cybersecurity Framework (CSF) 2.0 on February 26, 2024, representing significant evolution from previous versions (National Institute of Standards and Technology, 2024). CSF 2.0 organizes cybersecurity activities into six integrated primary functions with explicit governance as central organizing principle.

GOVERN (GV): The core function providing strategic direction and oversight of cybersecurity implementation. GOVERN comprises six principal categories reflecting holistic governance aspects:

a. Organizational Context (GV.OC): Understanding organizational mission, strategic objectives, and internal/external environment affecting cybersecurity risk decisions.
b. Risk Management Strategy (GV.RM): Establishing risk management objectives aligned with stakeholders, defining risk appetite and tolerance.
c. Roles, Responsibilities, and Authorities (GV.RR): Establishing organizational leadership accountability for cyber risks across all organizational units.
d. Policy (GV.PO): Developing comprehensive cybersecurity policies based on organizational context, security strategy, and priorities.
e. Oversight (GV.OV): Conducting periodic reviews of cybersecurity risk management outcomes and adjusting organizational strategy accordingly.
f. Cybersecurity Supply Chain Risk Management (GV.SC): Managing supply chain risks through vendor assessment, contract security requirements, and incident response coordination.

IDENTIFY (ID): Understanding organizational cybersecurity risks through asset identification, supplier identification, external dependencies, and risk assessment.

PROTECT (PR): Implementing safeguards preventing or minimizing cyber event impacts through access controls, data protection, asset management, and security program maintenance.

DETECT (DE): Identifying and analyzing cyber events to determine cybersecurity incidents through anomaly detection and continuous monitoring.

RESPOND (RS): Taking actions against detected cybersecurity incidents to stop attacks, restore operations, and minimize impact.

RECOVER (RC): Restoring systems and data to normal conditions following incidents, including post-incident analysis and improvement programs.

Significance of NIST CSF 2.0: This framework provides flexible guidance for implementation across government levels with different risk profiles. Strong GOVERN functions address governance oversight needs in complex centralized SPBE ecosystems (National Institute of Standards and Technology, 2024). Explicit Supply Chain Risk Management integration directly addresses documented weaknesses in vendor software security management.

ISO/IEC 27001:2022 Information Security Management System

ISO/IEC 27001:2022 is an international standard regulating Information Security Management System (ISMS) (International Organization for Standardization, 2022). This standard provides comprehensive framework for identifying, managing, and reducing information security risks through Plan-Do-Check-Act methodology.

The standard organizes security controls into 14 principal domains covering organizational information security, personnel security, asset management, access control, cryptography, supplier relationships, physical security, operations, communications, system acquisition, supplier relationships, incident management, business continuity, and compliance. ISO 27001 implementation in Indonesian government sectors has shown positive results in several ministries. However, this standard became mandatory SNI (National Standard) for SPBE since 2024 under BSSN Regulation No. 7 of 2024, indicating government commitment to certified international standardization (Badan Siber dan Sandi Negara, 2024).

COBIT 2019 for Information Security and IT Governance

COBIT 2019 provides enterprise IT governance guidance for organizations with heterogeneous contexts and resource constraints (ISACA, 2019). COBIT 2019 introduces Design Factors concept enabling organizations to design IT governance systems customized to organizational strategy, risk profiles, threat landscape, compliance requirements, and organizational complexity.

Key advantages over previous versions include Design Factors flexibility for realistic maturity roadmaps, COBIT Performance Management with CMMI-based 0-5 capability assessment, Focus Areas for selective topic adoption, and open-source continuous updates. For SPBE sector, COBIT 2019 provides integrated processes with clear linkage to business objectives and stakeholder value (ISACA, 2020).

National Indonesian Cybersecurity Regulations

Law No. 1 of 2024 on Information and Electronic Transactions

Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law 1/2024) constitutes the foundation of Indonesian cybersecurity law (Undang-Undang Nomor 1 Tahun 2024, 2024). ITE Law 1/2024 regulates electronic transactions, illegal content distribution, data theft, system hacking, and citizen privacy protection with cybersecurity crime handling standards adapted to rapid field developments.

BSSN Authority Clarification: According to Article 43 of ITE Law 1/2024 and BSSN Regulation No. 6 of 2021, criminal investigation authority remains with Civil Servant Officials (PPNS) in Ministry of Communication and Digital Affairs plus Indonesian National Police (Badan Siber dan Sandi Negara, 2021). BSSN holds strategic role providing technical investigation support through digital forensics, expert testimony, post-incident security audits, and threat intelligence sharing.

Administrative Sanctions and Enforcement Mechanisms: Article 16B of ITE Law 1/2024 introduces tiered administrative sanctions against Electronic System Operators violating security obligations, including written warnings, administrative fines, temporary service suspension, and permanent access termination. This mechanism provides government executive authority to disable digital services deemed non-compliant with minimum security standards (Undang-Undang Nomor 1 Tahun 2024, 2024).

Electronic Government System (SPBE)

SPBE, regulated under Presidential Regulation No. 95 of 2018, utilizes information and communication technology for government data management and services (Peraturan Presiden Nomor 95 Tahun 2018, 2018). Research on cybersecurity challenges in remote work environments highlights that Presidential Regulation No. 21 of 2023 granting Indonesian civil servants location flexibility creates cybersecurity challenges requiring comprehensive framework development (Asyrofi & Nugraha, 2025).

SPBE security standards reference SNI ISO/IEC 27001:2022 for strategic electronic system operators. BSSN Regulation No. 8 of 2024 mandates periodic security audits, audit result documentation, and accredited auditors holding international certifications (Badan Siber dan Sandi Negara, 2024).

National Cyber and Cryptography Agency (BSSN) Governance Framework

BSSN holds strategic responsibility in national cybersecurity ecosystem through multiple regulatory instruments. BSSN Regulation No. 1 of 2024 (Cyber Incident Management) regulates national cyber incident response coordination including 24/7 Cyber Incident Response Team (TTIS) operations, incident reporting protocols, severity classification, and law enforcement coordination (Badan Siber dan Sandi Negara, 2024).

Cybersecurity Risk Management

Risk Identification and Assessment

Cybersecurity risk management requires systematic and structured processes. Systematization of cybersecurity regulations demonstrates that comprehensive frameworks must address multiple dimensions: asset identification, threat assessment, vulnerability analysis, and risk calculation using Likelihood × Impact matrices (Carello et al., 2023).

Risk Mitigation Strategies

Table 1. Risk mitigation strategies mapped to cyber threat types

Threat Type	Key Risk	Mitigation Strategy	Supporting Technology	Priority
Advanced Persistent Threat (APT)	State-sponsored actors, prolonged dwell time, data exfiltration	Zero Trust Architecture, credential protection, lateral movement detection	EDR/XDR, network segmentation, IAM, behavioral analytics	CRITICAL
Ransomware	Service paralysis, data encryption, business continuity disruption	Backup & Disaster Recovery (3-2-1 rule), immutable backups, PAM	EDR solutions, network isolation, backup systems, DLP	CRITICAL
Phishing & Social Engineering	Initial breach, credential compromise, malware distribution	Security awareness training, email filtering (SPF/DKIM/DMARC), MFA	Email security gateway, SIEM, user behavior analytics, MFA	HIGH
Supply Chain Compromise	Widespread impact through trusted providers, difficult detection	Vendor assessment & audit, SBOM requirement, code signing verification	Supply chain visibility tools, SBOM analysis, artifact scanning	HIGH
Insider Threats	Legitimate credential usage, difficult detection, data exfiltration	Least privilege enforcement, PAM, user behavior monitoring	PAM solution, UEBA, DLP, activity monitoring	MEDIUM-HIGH

Distributed Denial of Service (DDoS)	Service unavailability, citizen access disruption	DDoS mitigation service, traffic filtering, rate limiting, CDN	CDN services, DDoS mitigation appliances, traffic analysis	MEDIUM

Risk mitigation strategies encompass four fundamental approaches: risk avoidance (avoiding unacceptable activities), risk reduction (applying technical controls), risk transfer (through insurance or outsourcing), and risk acceptance (with contingency plans).

Contemporary Cybersecurity Technologies

Zero Trust Architecture (ZTA)

Zero Trust Architecture rests on fundamental principle "Never Trust, Always Verify" assuming continuous verification of every access regardless of source. ZTA encompasses continuous verification based on identity and device posture, least privilege access limiting to minimum required permissions, assumption of breach building defense assuming perimeter compromise, and micro-segmentation dividing networks into independently protected zones.

PDN Case Study Implications: June 2024 PDN incident confirmed inadequate ZTA implementation where Windows Defender disabling failed to trigger immediate alerts, malicious activity continued undetected for hours, and lateral movement proceeded unchallenged (Tempo.co, 2024). With proper ZTA implementation, such attacks would trigger immediate alerts, block suspicious access, and prevent lateral movement through network segmentation.

Backup and Disaster Recovery

Periodic data backup provides critical control for ransomware resilience and business continuity. Best practices include 3-2-1 backup rule (3 copies using 2 media types with 1 offsite location), immutable backups preventing malware modification, and regular restoration testing ensuring recovery capability. PDN investigation revealed several tenants lacked backup data separation from primary systems, violating fundamental backup principles (Tempo.co, 2024).

Cybersecurity Governance and Human Capital Development

Good cybersecurity governance requires implementing five integrated principles addressing accountability through clear expectations, transparency through stakeholder information access, rule of law through consistent enforcement, democratic control through parliamentary oversight, and effectiveness through achieving security objectives (Savaş & Karataş, 2022). Research demonstrates that governance frameworks remain inadequately established globally with persistent struggles between organizational solutions and comprehensive governance models.

Human capital development constitutes a critical enabler of cybersecurity resilience. Indonesia's cybersecurity maturity depends substantially on strengthening cybersecurity competencies across government institutions. The Indonesia-Australia Cyber Policy Dialogue (2018-2020) demonstrates the importance of international cooperation in capacity building, with BSSN playing a central role in identifying and developing cybersecurity expertise among government personnel (Shiddique & Juned, 2023). Effective human capital development requires comprehensive training programs, clear career pathways, and sustained investment in professional development across all government levels.

3. METHODS

This research employed systematic literature review methodology following established research practices. Sources were collected from peer-reviewed academic journals indexed in SINTA, Scopus, and academic databases (emphasizing 2023-2025 publications), official Indonesian government publications, international organization publications, and threat intelligence reports from trusted security vendors and research organizations.

Sources were analyzed according to comprehensive cybersecurity framework incorporating technical, organizational, human, and legal/regulatory dimensions. Best international practices were integrated with Indonesian national regulations through mapping and gap analysis, emphasizing Indonesian SPBE-specific context. Findings were validated through cross-referencing with minimum 15+ primary sources, with particular attention to cyber security incident data verification, framework specifications validation, latest regulation confirmation, and threat intelligence corroboration.

4. RESULTS AND DISCUSSION

Threat Assessment Against Indonesian Digital Government

Threat landscape analysis reveals significant patterns. Multi-vector attack approaches combine spear-phishing, malware deployment, and supply chain compromise. Geopolitical motivation drives APT activities with strategic intelligence gathering objectives (Carello et al., 2023). Supply chain vulnerabilities in IT vendor software and services provide attackers widespread impact potential through compromised upstream providers (Tempo.co, 2024).

Gap Analysis Between International Frameworks and National Regulations

International framework adoption remains early-stage with significant inter-agency variations. Many SPBE institutions have not achieved maturity level 3+ in NIST CSF implementation. Centralized coordination lacks for threat intelligence sharing and incident

response. Resource constraints and skills shortages create implementation bottlenecks (Asyrofi & Nugraha, 2025). Security audits often focus on compliance checklists rather than operational effectiveness (Carello et al., 2023).

Comprehensive Cybersecurity Framework Recommendations

Comprehensive Indonesian government cybersecurity framework based on 5 integrated pillars addresses technical controls, governance and policies, organizational structure and coordination, human capital development, and incident response and crisis management. Research demonstrates that such integrated approaches combining technology, human resources, governance, and transparent communication allow public administration to transform cybersecurity from challenge into strategic advantage (Savaş & Karataş, 2022).

Pillar 1: Technical Security

Technical foundation must include implementing NIST CSF 2.0 as cybersecurity organizing structure (National Institute of Standards and Technology, 2024), adopting ISO/IEC 27001:2022 for establishing comprehensive ISMS (International Organization for Standardization, 2022), implementing Zero Trust Architecture on critical systems, modern endpoint protection and threat detection, regular vulnerability assessments, and secure backup and disaster recovery procedures.

Pillar 2: Governance and Policies

Governance framework must include clear cybersecurity strategy aligned with national digital transformation objectives, comprehensive cybersecurity policies covering access control and incident response, regular policy review and update, and board oversight with measurable cybersecurity KPIs.

Pillar 3: Organizational Structure and Coordination

Organizational structure must include establishing Chief Information Security Officer (CISO) role with C-level reporting, forming Cybersecurity Steering Committee with cross-unit representation, intelligence sharing through Information Sharing and Analysis Centers (ISACs), and formal BSSN coordination (Badan Siber dan Sandi Negara, 2024).

Pillar 4: Human Capital Development

Cybersecurity workforce development requires strategic investment in training, professional development, and capacity building across all government sectors. Indonesia has recognized the critical importance of human capital through international partnerships and BSSN initiatives, particularly through the Indonesia-Australia Cyber Policy Dialogue which provided direct knowledge transfer and practical training in cybersecurity competencies (Shiddique & Juned, 2023). Effective human capital initiatives must include comprehensive

cybersecurity awareness training tailored to different roles, specialized training for IT security professionals, phishing simulation exercises, career development paths, and certification programs support. Organizational readiness for cybersecurity maturity depends substantially on the quality and depth of human resource capabilities.

Pillar 5: Incident Response and Crisis Management

Incident response capability must include comprehensive Incident Response Plans with clear roles and responsibilities (Badan Siber dan Sandi Negara, 2024), regular tabletop exercises, 24/7 Security Operations Center (SOC) operations, law enforcement coordination protocols, and post-incident analysis programs.

Discussion

Implementation Challenges

Comprehensive framework implementation faces substantial challenges. Legacy systems modernization difficulty, budget constraints, skills shortage, complex change management, and vendor lock-in situations limit implementation progress. These obstacles particularly impact developing economies with limited cybersecurity infrastructure investment (Asyrofi & Nugraha, 2025). Human capital development challenges require sustained commitment to workforce training and professional development (Shiddique & Juned, 2023).

Emerging Technologies and Opportunities

Emerging technologies offer cybersecurity posture enhancement opportunities including Artificial Intelligence and Machine Learning for threat detection automation, Quantum Computing era preparation, Blockchain for critical infrastructure security, and Cloud Computing with security provisions (Carello et al., 2023).

Best Practices from Other Jurisdictions

Victoria, Australia demonstrates centralized 24/7 incident response service accessibility. New Zealand emphasizes structured incident categorization for proportionate response. United Kingdom provides government-wide cyber governance standard mapped to NIST CSF, offering valuable adaptation opportunities for Indonesian context (Savaş & Karataş, 2022). International cooperation models like the Indonesia-Australia Cyber Policy Dialogue demonstrate effective approaches to knowledge transfer and capacity building (Shiddique & Juned, 2023).

5. CONCLUSION AND RECOMMENDATIONS

Conclusion

Comprehensive cybersecurity framework for Indonesian digital government requires consolidating five fundamental dimensions. Cybersecurity governance integration with digital transformation strategy is not merely technical imperative but central vector of state responsibility (Savaş & Karataş, 2022). These dimensions include technical controls implementing international frameworks (National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022; ISACA, 2019), regulatory compliance to ITE Law 1/2024 (Undang-Undang Nomor 1 Tahun 2024, 2024), organizational excellence with strong governance structures (Badan Siber dan Sandi Negara, 2024), human capital continuous investment (Shiddique & Juned, 2023), and incident readiness with comprehensive response plans.

Implementing this framework will enhance Indonesian government cybersecurity resilience, protect sensitive citizen information, ensure public service continuity, and build public confidence in government digital transformation. Significant obstacles in resource constraints, skills shortages, and legacy system modernization require inter-ministerial coordination and sustained political leadership commitment for successful implementation (Asyrofi & Nugraha, 2025; Carello et al., 2023).

Recommendations

Table 2: Implementation Roadmap For Comprehensive Cybersecurity Framework

Timeframe	Initiative	Responsible Entity	Estimated Budget	Success Metrics	Key Dependencies
Short-term (1-2 Years)	Develop Comprehensive Cybersecurity Strategy	Ministry of Communication & Digital Affairs + BSSN	Rp 5-10B	Strategy document published, stakeholder alignment achieved	Political commitment, inter-agency coordination
Short-term (1-2 Years)	Cybersecurity Maturity Assessment (NIST CSF 2.0)	Each government agency + BSSN	Rp 2-5B	100% critical agencies assessed, baseline maturity documented	Assessment tool availability, trained assessors
Short-term (1-2 Years)	Establish/Strengthen CISO Role	All major government agencies	Rp 1-3B	CISO positions established, charter defined	Budget allocation, qualified personnel
Short-term (1-2 Years)	Mandatory Cybersecurity	BSSN + HR departments	Rp 3-8B	80%+ employee training	Training content development,

	Awareness Training			completion rate	delivery infrastructure
Short-term (1-2 Years)	Develop Incident Response Plans	Each agency CISO teams	Rp 2-4B	IRP documentation complete, roles assigned	Templates provided, BSSN coordination
Medium-term (2-5 Years)	Implement NIST CSF 2.0 & ISO 27001:2022	All critical systems operators	Rp 15-30B	70%+ of critical systems compliant	Budget availability, vendor support, skill development
Medium-term (2-5 Years)	Centralized Security Operations Center (SOC)	BSSN	Rp 20-50B	24/7 SOC operational, incident response time <1 hour	Infrastructure investment, staffing, tool procurement
Medium-term (2-5 Years)	Specialized Cybersecurity Workforce Development	Ministry of Education + Universities + BSSN	Rp 25-40B	500+ certified cybersecurity professionals trained	International partnerships, curriculum development
Medium-term (2-5 Years)	Implement Zero Trust Architecture	Critical systems operators	Rp 30-60B	Mission-critical systems protected by ZTA	Technology investment, change management
Medium-term (2-5 Years)	Strengthen BSSN Information Sharing	BSSN + all agencies	Rp 5-10B	Real-time threat intelligence sharing platform operational	Information sharing agreements, system integration
Long-term (5+ Years)	Industry-leading Cybersecurity Maturity (Level 4-5)	All government organizations	Rp 50-100B+/year	Critical infrastructure at maturity level 4+	Continuous funding, sustained leadership commitment
Long-term (5+ Years)	Indigenous Cybersecurity Vendor Ecosystem	Ministry of Industry + BSSN	Rp 40-80B	3-5 local vendors delivering critical security solutions	Government support programs, R&D investment
Long-term (5+ Years)	Regional Cybersecurity Leadership Role	BSSN + Ministry of Foreign Affairs	Rp 10-20B	Best practices shared with neighboring countries	International cooperation agreements
Long-term (5+ Years)	Continuous Adaptation to Emerging Threats	All agencies + BSSN	Rp 15-30B/year	Response time to emerging threats <48 hours	Threat intelligence infrastructure, skilled workforce

Short-term Recommendations (1-2 Years)

a) Develop Comprehensive Cybersecurity Strategy for entire government sector aligned with national digital transformation roadmap
b) Conduct Cybersecurity Maturity Assessments using NIST CSF 2.0 framework (National Institute of Standards and Technology, 2024)
c) Establish or Strengthen CISO Role in major government agencies with clear charter and adequate resources
d) Implement Mandatory Cybersecurity Awareness Training for all government employees (Shiddique & Juned, 2023)
e) Develop Incident Response Plans for critical government services (Badan Siber dan Sandi Negara, 2024)

Medium-term Recommendations (2-5 Years)

a) Implement NIST CSF 2.0 and ISO/IEC 27001:2022 Standards across critical government systems (National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022)
b) Establish Centralized Security Operations Center (SOC) under BSSN for national-level monitoring (Badan Siber dan Sandi Negara, 2024)
c) Develop Specialized Cybersecurity Workforce through university and international partnerships (Shiddique & Juned, 2023)
d) Implement Zero Trust Architecture on critical government systems
e) Strengthen BSSN Coordination through regular information sharing

Long-term Recommendations (5+ Years)

a) Achieve Industry-leading Cybersecurity Maturity Levels on critical government infrastructure (ISACA, 2019)
b) Develop Indigenous Cybersecurity Vendor Ecosystem through government support
c) Establish Indonesia as Regional Cybersecurity Leader sharing best practices with neighboring countries
d) Continuous Adaptation to emerging threats and technologies (Carello et al., 2023)

REFERENCES

Asyrofi, M. F., & Nugraha, I. G. D. (2025). Cybersecurity of work from anywhere model for government: A systematic literature review. *International Journal of Electrical, Computer and Biomedical Engineering*, 3(1), 124. https://doi.org/10.62146/ijecbe.v3i1.113

Badan Siber dan Sandi Negara. (2021). *Peraturan BSSN Nomor 6 Tahun 2021 tentang Pengawasan Keamanan Informasi Penyelenggara Sistem Elektronik Strategis*. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2024). *Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber*. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2024). *Peraturan BSSN Nomor 7 Tahun 2024 tentang Penilaian Kesesuaian Teknologi Informasi*. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2024). *Peraturan BSSN Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE)*. Jakarta: BSSN.

Carello, M. P., Marchetti Spaccamela, A., Querzoni, L., & Angelini, M. (2023). A systematization of cybersecurity regulations, standards and guidelines for the healthcare sector. In *Proceedings of IEEE ISI 2023: 20th Annual IEEE International Conference on Intelligence and Security Informatics* (pp. 1-6). IEEE. https://doi.org/10.1109/ISI58743.2023.10297246

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. Information security management systems. Requirements*. Geneva: ISO/IEC.

ISACA. (2019). *COBIT 2019 - Governance and management of enterprise IT: Framework and objectives*. Rolling Meadows: ISACA.

ISACA. (2020). *COBIT 2019 and COBIT 5 comparison*. Industry News Report. Retrieved from https://www.isaca.org

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework 2.0* (Publication CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 192.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, 3(1), 7-34. https://doi.org/10.1365/s43439-021-00045-4

Shiddique, M. R., & Juned, M. (2023). Human capital development for cybersecurity: Examining BSSN's contributions in the Indonesia-Australia cyber policy dialogue (2018-2020). *Journal of Government and Development*, 6(4), 215-224. https://doi.org/10.31014/aior.1991.06.04.457

Tempo.co. (2024, June 25). PDNS lumpuh karena serangan ransomware, data terdampak tidak bisa dipulihkan. Retrieved from https://www.tempo.co/hukum/pdns-lumpuh-karena-serangan-ransomware-data-terdampak-tidak-bisa-dipulihkan--45597

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024.