Vifada Management and Social Sciences, E-ISSN 2987-1999

Designing a Security Profile Using the NIST Cybersecurity Framework for General Elections in Indonesia

Muhammad Hibban Mikhail [(1*)] *Sinung Suakanto* [(2)] *Basuki Rahmad*[(3)]

[(1,2,3)] *Master of Information Systems Study Program, Faculty of Industrial Engineering, Telkom University*

Received: 2026, 04,15 **Accepted**: 2026, 06,08
Available online: 2026, 06,30

*Corresponding author.
E-mail addresses: hbnmichael@student.telkomuniversity.ac.id

KEYWORDS

Keywords:
election cybersecurity; NIST CSF 2.0; e-voting; VVPAT; election information systems; cyber threats; electoral governance

Conflict of Interest Statement:
The author(s) declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

ABSTRACT

This study aims to design a comprehensive cybersecurity profile for Indonesia's electoral digital ecosystem using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0. The research focuses on identifying vulnerabilities in election information systems, formulating mitigation controls, and strengthening the supervisory role of the Election Supervisory Agency (Bawaslu) toward the General Election Commission (KPU). This study employed a qualitative descriptive-diagnostic approach. Data were collected through qualitative observations, historical cyber incident reports, regulations, cybersecurity documents, and academic literature related to election governance and digital security in Indonesia. Data analysis followed five implementation phases of NIST CSF 2.0: prioritize and scope, orient, create current profile, conduct risk assessment, and create target profile. The findings indicate that Indonesia's election information systems remain vulnerable to data breaches, access control weaknesses, insider threats, infrastructure failures, and disinformation attacks. The study proposes a dual-recording e-voting architecture integrated with Voter Verifiable Paper Audit Trail (VVPAT) to improve transparency, auditability, and election integrity. The findings imply that election cybersecurity governance requires integrated institutional oversight, technical mitigation, and forensic audit mechanisms to maintain democratic legitimacy and public trust.

Introduction

The success of a general election is measured not merely by the level of public participation, but also by the quality, integrity, and transparency of its administration. A democratic election serves as a central mechanism for legitimizing leadership transitions and forming legislative representation through the direct delegation of voting mandates by the people. The conduct of general elections in the Republic of Indonesia is not merely a periodic administrative routine, but a constitutional mandate precisely regulated under Article 22E of the 1945 Constitution of the Republic of Indonesia. This constitutional provision requires the rotation of power to be conducted according to the principles of direct, general, free, confidential, honest, and fair elections. Although high public participation reflects mature political awareness, without guarantees of honest and fair administration, such participation cannot ensure the formation of a government with strong legitimacy (Tampubolon et al., 2021).

Indonesia's vast sociogeographic conditions have driven the electoral administration system to undergo structural evolution, with the transition toward information technology-based services being the most prominent change. The adoption of technology is motivated by the urgent need to streamline bureaucracy, accelerate the aggregation of vote counts that traditionally takes weeks, and reduce the likelihood of human error in data recapitulation. The literature on election technology also indicates that automation can improve speed, accuracy, auditability, accessibility, and cost efficiency in managing electoral processes (Chaudary, 2022). On the other hand, this modernization of electoral

infrastructure creates a paradoxical challenge. The extensive use of hardware, software, and cloud computing infrastructure introduces new vulnerabilities that may be exploited by cyber threat actors, making digital security an issue that cannot be overlooked in election administration (Afiansyah & Amiruddin, 2019).

Various electoral information subsystems in Indonesia have demonstrated operational vulnerabilities and exposure to cyberattacks during previous election periods. These incidents not only threaten the security and privacy of citizens' data, but also erode public trust in the integrity of democratic institutions (Vincent et al., 2021). Previous academic studies have examined the influence of online vote-counting systems on public trust, finding that electronic information transparency has a significant positive correlation with public perceptions of electoral integrity (Tampubolon et al., 2021). A similar pattern is observed globally. International IDEA emphasizes that cyber threats can affect the entire electoral cycle, both through attacks on election technology and through disinformation targeting public perceptions of electoral integrity. Even countries that do not use e-voting remain exposed to risk because the entire election process depends on information and communication technology infrastructure (Staak & Wolf, 2019).

IFES emphasizes that the growing integration of digital technology into voter registration, result transmission, and result aggregation has generated various policies, principles, and practices for responding to cyber threats that could undermine electoral integrity (IFES, 2023). According to a more recent IFES report, the most critical vulnerabilities lie in voter registration databases, tabulation systems, and result transmission processes, while weak cyber hygiene, fragmented third-party procurement, and ad hoc coordination among stakeholders further increase these risks (Chaudary, 2022). The cross-actor nature of these threats requires interagency collaboration because risk management, incident response, and the protection of election technology involve election management bodies (EMBs), cybersecurity agencies, technology providers, political parties, the media, and civil society (Staak & Wolf, 2019).

Secure and reliable electoral information systems are essential to ensure that election results are valid, accurate, and legally accountable. In the global cybersecurity context, protecting the digital domain is no longer viewed solely as an information technology function, but as a crucial element of national resilience strategy. This view is consistent with the strategic guidelines of the Ministry of Defense of the Republic of Indonesia, which position cyber defense as a vital layer in safeguarding non-military sovereignty. Information technology security governance approaches that adopt international standards have also proven effective in mapping and mitigating risks across various government institutions (Khatami & Rahayu, 2024).

Although previous studies have made significant contributions to understanding the technical and social dimensions of electoral information-system security, several gaps remain inadequately addressed. Most existing studies focus on public trust or post-incident evaluation without offering a structured governance framework based on international standards that can be directly applied to Indonesia's electoral ecosystem. Furthermore, the asymmetric oversight mechanism exercised by the Election Supervisory Body (Bawaslu) over the security governance implemented by the General Election Commission (KPU) has not received sufficient academic attention, even though this oversight dimension is essential to building an accountable electoral system.

Based on these gaps, this study poses the following main question: how can a comprehensive security profile be designed for Indonesia's electoral ecosystem to systematically mitigate cyber-threat risks? This study aims to design a security profile for Indonesia's electoral digital infrastructure using version 2.0 of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), focusing on vulnerability identification, the formulation of technical mitigation controls, and the strengthening of Bawaslu's oversight of KPU governance (National Institute of Standards and Technology, 2024). This framework was selected because it is flexible, risk-based, and aligned with the election infrastructure profile published in NISTIR 8310. The novelty of this study lies in integrating an institutional oversight perspective into the design of an electoral cybersecurity profile, an approach that has not previously been examined in an integrated manner in either national or international academic literature.

Literature Review

General elections are the most fundamental constitutional instrument for realizing popular sovereignty. Conceptually, electoral systems worldwide can be classified into three main categories. The first is the plurality/majority system, which is based on vote dominance and includes First Past the Post (FPTP), the Two-Round System (TRS), Alternative Vote (AV), and Block Vote (BV). The second is proportional representation, which allocates seats proportionally according to each party's vote share through closed-list, open-list, or Single Transferable Vote (STV) formats. The third is the mixed system, such as Mixed Member Proportional (MMP) and the Parallel System, which structurally combines the two preceding approaches. Each system has different implications for representation, accountability, and vulnerability to manipulation (Afiansyah & Amiruddin, 2019).

The legal framework for election administration in Indonesia is based on Law of the Republic of Indonesia Number 7 of 2017 concerning General Elections and is implemented by three independent institutions that provide mutual checks and balances. The General Election Commission (KPU) serves as the executive authority responsible for planning, implementing, and managing all stages of the election, from logistics management to the determination of official results. The Election Supervisory Body (Bawaslu) holds the mandate to supervise elections and enforce electoral regulations, including investigating alleged violations and safeguarding the integrity of each stage (Sumardi, 2024). The Election Organizer Ethics Council (DKPP) functions as an ethics adjudication body that receives complaints and imposes sanctions for violations of the organizers' code of ethics, thereby helping to ensure the impartiality of the democratic process.

The adoption of technology in elections has become the subject of extensive debate between bureaucratic efficiency and concerns about computational transparency. Estonia implements remote internet voting (i-Voting) with public-key authentication through smart identity cards (Berenjestanaki et al., 2024). Brazil uses Direct Recording Electronic (DRE) machines that are completely isolated from networks to mitigate the risk of remote attacks (Khatami & Rahayu, 2024). India requires electronic voting machines to be paired with a Voter Verifiable Paper Audit Trail (VVPAT) as physically verifiable evidence of each vote (Berenjestanaki et al., 2024). Germany and the Netherlands followed a different path, returning decisively to paper ballots because of hacking vulnerabilities and the principle that public transparency should not require specialized computing expertise (Fitzpatrick & Jöst, 2022). These differences among countries demonstrate that no universal solution exists for securing election technology.

The development of electronic voting technology in Indonesia began with a series of comprehensive studies initiated in 2010 by the Agency for the Assessment and Application of Technology (BPPT), which has since been integrated into the National Research and Innovation Agency (BRIN). A strategic partnership with PT Industri Telekomunikasi Indonesia (PT INTI) produced a device ecosystem that has been implemented in more than 2,000 village head elections across 28 regencies in Indonesia. The system can address duplicate entries in the Permanent Voter List (DPT) through the integration of smart-card readers and fingerprint biometric scanners. Expanding this platform to national general elections, however, requires a defense and information-security architecture based on significantly higher standards.

Cybersecurity in the modern context has evolved beyond the traditional information-security paradigm. The International Telecommunication Union (ITU) defines it as the collection of tools, policies, security concepts, risk-management guidelines, training, and technologies used to protect cyberspace and all organizational assets against unauthorized access, use, disruption, or modification (Wamala, 2011). The central objective of this effort is to preserve the information-security triad of confidentiality, integrity, and availability (National Institute of Standards and Technology, 2024). In the electoral context, the risk-management paradigm requires much stricter tolerance thresholds than those applied in the corporate sector, because failure to respond to an intrusion may distort the public mandate, undermine public trust, and unlawfully alter election results (Vincent et al., 2021).

The analytical instrument selected for this study is version 2.0 of the NIST Cybersecurity Framework (CSF). Architecturally, the framework divides the protection cycle into six interrelated functions: Govern (strategic governance and supply-chain risk management), Identify (asset understanding and vulnerability assessment), Protect (implementation of authentication, encryption,

and access-management controls), Detect (continuous monitoring to identify anomalies in real time), Respond (execution of containment measures and strategic communication during incidents), and Recover (restoration of normal operations and post-incident system rebuilding). These functions are contextualized by comparing the Current Profile (the factual security posture) with the Target Profile (the intended ideal condition) to produce a measurable improvement action plan (National Institute of Standards and Technology, 2024).

Research Design and Methodology

This study employs a qualitative approach using descriptive-diagnostic analysis. This design was selected because it is consistent with the primary objective of systematically mapping the security posture of electoral digital infrastructure and formulating mitigation recommendations based on empirical evidence, rather than producing statistical generalizations.

The research subject is Indonesia's election-administration information-technology ecosystem, which encompasses two principal institutional entities: KPU as the executive entity and Bawaslu as the audit and oversight entity. The analysis focuses on critical business processes that depend heavily on digital information systems, namely voter-data management, electoral-contestant registration, the logistics supply chain, and vote-count recapitulation.

Data were collected from two sources. Primary data were obtained through qualitative observations of information-security policy implementation at KPU and Bawaslu, with a focus on the effectiveness of interinstitutional oversight controls. Secondary data were collected through an extensive literature review covering historical election-incident reports, global cybersecurity white papers, KPU and Bawaslu regulations, and relevant reputable scientific journals.

Data analysis was conducted using an NIST CSF 2.0 implementation model adapted to electoral infrastructure through five structured phases. The first phase, Prioritize and Scope, established the boundaries of the analysis based on the core missions of KPU and Bawaslu as mandated by Law Number 7 of 2017. The second phase, Orient, involved inventorying technology assets, human resources, and network infrastructure, including mapping the threat landscape targeting Indonesia's electoral systems. The third phase, Create a Current Profile, evaluated the factual cybersecurity posture through historical observations of system failures and data-breach incidents mapped to NIST CSF categories and subcategories. The fourth phase, Conduct a Risk Assessment, measured the probability that identified vulnerabilities would be exploited and assessed their systemic impact on the confidentiality, integrity, and availability of election data. The fifth phase developed a Target Profile containing realistic and measurable security recommendations based on the preceding risk assessment. The alignment between this layered analytical method and the research question supports the scientific replicability and verification of the findings (National Institute of Standards and Technology, 2014).

Findings and Discussion

Findings

Analysis of the Election-Administration Information-System Ecosystem

General elections in Indonesia operate through a highly complex set of distributed applications that were not all designed with synergistic capabilities. This ecosystem is managed by two institutions with mutually balancing functions: the General Election Commission (KPU), as the administrator controlling the primary operational infrastructure, and the Election Supervisory Body (Bawaslu), as the oversight institution managing independent monitoring and audit infrastructure (Sumardi, 2024).

The mapping of historical incidents and field observations identified vulnerabilities across various sectors of the election-technology ecosystem. The Voter Data Information System (Sidalih) is the principal population database and has been exposed to high-level data-exfiltration attacks (Khatami & Rahayu, 2024). Decision Number 4-PKE-DKPP/I/2024 confirmed that Sidalih experienced unauthorized access by a hacker using the alias 'Jimbo' in late 2023, who claimed to have stolen hundreds of millions of voter records. The hearing also disclosed the results of an Information

Technology Security Assessment (ITSA) conducted by BSSN, which identified Privilege Escalation and Possible Brute Force vulnerabilities that had not been fully mitigated before the incident occurred.

The Political Party Information System (Sipol) frequently faces the unauthorized appropriation of citizens' names, indicating weak input-validation controls, while its availability is questionable under peak loads (Khatami & Rahayu, 2024). The Candidacy Information System (Silon) exhibits not only technical vulnerabilities arising from high network dependency, but also managerial vulnerabilities, as KPU has previously closed Bawaslu's read-only monitoring access and thereby impeded its supervisory function (Wamala, 2011).

The Campaign and Campaign-Finance Information System (Sikadeka) has generated critical governance constraints. Bawaslu has complained that KPU restricted its access to Sikadeka, making it difficult to transparently monitor Campaign Fund Special Account (RKDK) transactions and Initial Campaign Fund Reports (LADK). These restrictions effectively weakened Bawaslu's supervisory authority and obstructed transparency and accountability in political financing (Sumardi, 2022).

The Recapitulation Information System (Sirekap), an optical character recognition (OCR) application, was proven to have failed to accurately convert C.Hasil form data in February 2024, as documented in Decision Number 53-PKE-DKPP/III/2024 (Hastuti et al., 2024). This failure produced numerical anomalies and substantial discrepancies from the physical data recorded in the field. KPU's systemic failure to implement anomaly-threshold logic, or sanity checks, before publication triggered a nationwide crisis of confidence and demonstrated the need to prevent operational failures from the earliest stages of system development (Afiansyah & Amiruddin, 2019).

Other systems, including the Logistics Information System (Silog), the KPU Member and Ad Hoc Body Information System (SIAKBA), the Ad Hoc Body Budget Accountability Information System (SITAB), the Online Voter List Check portal, and the full range of Bawaslu oversight systems (SIAPP, SIWASLIH, Siwaslu, Sigap Lapor, and RDKSPD), face similar challenges involving weak connectivity infrastructure, privacy-data vulnerabilities, and nationwide server failures under simultaneous access caused by inadequate architectural capacity planning (Afiansyah & Amiruddin, 2019).

Table 1 summarizes the systemic failures that have been exploited, based on the identified cybersecurity vulnerabilities within this ecosystem.

Table 1. Election-System Failures and Cybersecurity Vulnerabilities

System	Incident/Vulnerability	Evidence Source	Affected MOs
Sidalih	Exfiltration of hundreds of millions of voter records by a hacker using the alias 'Jimbo'; Privilege Escalation and Possible Brute Force vulnerabilities were identified but had not been mitigated before the incident occurred.	DKPP Decision No. 4-PKE-DKPP/I/2024; 2023 BSSN ITSA findings	MO-1, MO-6, MO-8
Sirekap	Failure of the OCR data-conversion system for C.Hasil forms (February 2024), which caused numerical anomalies and a nationwide crisis of public trust because sanity-check logic was absent.	DKPP Decision No. 53-PKE-DKPP/III/2024	MO-1, MO-7, MO-10
Sikadeka	KPU's restrictions on Bawaslu's access to RKDK and LADK data undermined the independent campaign-finance audit and oversight function.	Field evidence; Bawaslu reports	MO-6, MO-7
Silon	High network dependency; KPU previously closed Bawaslu's read-only access, thereby impeding oversight of the candidacy process.	Observations of the 2024 election administration	MO-2, MO-6
Sipol	The unauthorized appropriation of citizens' names indicates weak input validation; system availability is questionable under peak loads.	Internal incident reports	MO-2, MO-5
Silog	Slow data-update rates; KPU denied Bawaslu auditors access at critical distribution points.	Logistics-distribution observations	MO-6, MO-8

Online Voter List Check	Vulnerable to DDoS attacks that could disable voter-verification services on election day.	System-architecture analysis	MO-2, MO-9
Bawaslu Systems (SIAPP, SIWASLIH, Siwaslu, Sigap Lapor)	Vulnerability to nationwide server outages during simultaneous access because of inadequate architectural capacity planning.	Election-day observations	MO-2, MO-9

Source: DKPP Decision No. 4-PKE-DKPP/I/2024; DKPP Decision No. 53-PKE-DKPP/III/2024; field observations.

Mapping Cyber Threats to the Democratic Process

The mapping of attack vectors affecting the democratic process identified three main threat clusters. First, global threats include state-sponsored actors, such as foreign intelligence factions that design Advanced Persistent Threats for geopolitical purposes to influence election results or undermine trust in democracy; cybercriminals motivated by financial gain through ransomware deployment or voter-data exfiltration, as demonstrated in DKPP Decision Number 4-PKE-DKPP/I/2024; and hacktivists driven by ideological commitments or fanaticism toward particular candidates (Hastuti et al., 2024).

Second, disinformation threats and the misuse of artificial intelligence include narrative-manipulation campaigns designed to exploit social divisions so that the public perceives the election as fraudulent, as well as the use of deepfake technology to produce high-quality audiovisual manipulations portraying candidates or election officials as though they were tampering with ballots (Walker et al., 2024).

Third, technical attacks include Distributed Denial of Service (DDoS) attacks intended to disable public-service portals on election day; data theft through phishing or zero-day exploitation; the insertion of malware into vote-tabulation software; and insider threats from administrative personnel or third-party vendors who create backdoors for sabotage. Internal systemic negligence, as established in DKPP Decision Number 53-PKE-DKPP/III/2024, also constitutes a vulnerability that can readily be exploited to conduct disinformation campaigns (Berenjestanaki et al., 2024).

Electronic Voting Architecture Design

During the early stage of Indonesia's e-voting experiment, pioneered in Mendoyo Hamlet, Jembrana, in 2009, the architecture still used a pure Direct Recording Electronic (DRE), or paperless-voting, model. Data flowed linearly within the machine without a physical feedback mechanism, creating a black-box effect in which voters had to place complete trust in the software (Arinze & Nwajana, 2025).

Constitutional Court Decision Number 147/PUU-VII/2009 fundamentally changed the direction of this architecture. The Constitutional Court declared electronic voting constitutionally permissible subject to strict cumulative conditions, most importantly the guarantee of the direct, general, free, confidential, honest, and fair election principles. Technically, these conditions require system transparency and auditability through a Voter Verifiable Paper Audit Trail (VVPAT) (Arinze & Nwajana, 2025).

In response to these requirements, the Target Profile developed in this study proposes a dual-recording defense architecture comprising four principal mechanisms. First, credential authentication uses a Smart Card Reader as a session key to ensure that each voter can access the voting booth only once. Second, dual validation and confirmation are performed when the computer sends an instruction to the VVPAT thermal printer to print the voter's selection on a paper roll behind glass, giving the voter seven seconds to conduct visual verification. Third, the vote is executed and encrypted in tabulation memory, while the VVPAT paper is cut and deposited into a sealed steel audit box. Fourth, absolute isolation is implemented through an air-gapped configuration in which the terminal is completely disconnected from all communication networks during election day; an encrypted VPN channel is opened only after the polling station closes to transmit logs to the KPU server. This architecture positions the paper VVPAT as the highest form of legally recognized material evidence, which can be forensically recounted in the event of a cyber-related dispute.

Changes in Institutional Functions

The transition toward verified e-voting requires structural changes in the roles of election organizers. KPU's role shifts as the District Election Committee (PPK), which previously conducted manual mathematical recapitulation, becomes the custodian responsible for securing the VVPAT Ballot Box (KSV) and memory devices, while KPU headquarters operates the National Data Center and provides audit logs for adjudication.

Bawaslu gains analytical authority through read-only monitoring access to KPU's national server logs. Recommendations for a revote (PSU) are no longer based solely on disputes over manual C1 forms, but also on digital anomalies and VVPAT slips verified by Polling Station Supervisors. DKPP focuses its ethical sanctions on violations of digital procedures, such as failure to conduct mock polls, damage to VVPAT seals, manipulation of audit logs, or attempts to obstruct auditors' access to servers (Brady et al., 2024).

Changes in the Stages of Election Administration

The implementation of a verified e-voting system requires comprehensive adjustments to every stage of election administration. Program and Budget Planning must be reoriented from consumable logistics toward the procurement and calibration of Control Units (CUs), Balloting Units (BUs), VVPAT devices, E-Poll Books, data-center infrastructure, VPNs, and independent audit contracts with BSSN. The Regulatory Drafting stage should promote amendments to the Election Law so that VVPAT slips are legally recognized as primary evidence before the Constitutional Court.

On election day, a fundamental transition occurs from paper-based logistics management to verified digital workflow management and device-based supervision. The seven-member KPPS structure is retained, but its roles are redesigned as presented in Table 2.

Table 2. Adjustment of KPPS Member Roles in the VVPAT E-Voting System

KPPS Personnel	Traditional Role (Manual)	New Role Transformation (VVPAT E-Voting)
KPPS 1 (Chair)	Manually signs hundreds of ballot papers before they are issued to voters.	Supervisor and Adjudicator. Leads device Zero Report initialization and handles first-level adjudication when the on-screen selection does not match the VVPAT receipt.
KPPS 2	Administrator of the paper-based manual attendance list.	Biometric Authentication Officer. Operates the E-Poll Book and validates the electronic identity card and biometric data against the digital Permanent Voter List to prevent duplicate voting.
KPPS 3	Issues paper ballots to voters.	Activation Officer. Controls the Control Unit (CU) to activate the Balloting Unit in the voting booth and provides each voter with a single-use access Smart Card.
KPPS 4 & 5	Guards the voting booth and ballot box.	Digital Assistance and Education. Protects voting-booth confidentiality and educates vulnerable and elderly voters about the obligation to verify the receipt behind the VVPAT glass within seven seconds.
KPPS 6	Post-voting ink-marking officer.	Retains post-voting ink marking as a physical dual-control instrument.
KPPS 7	Secures the polling-station entrance.	Circulation Management (Crowd Control). Regulates one-way movement from the authentication point to the polling-station exit.

Source: Research design based on Constitutional Court Decision No. 147/PUU-VII/2009.

After the polling station closes, the KPPS Chair executes Close Poll. The Control Unit aggregates the data and prints a Digital C1 form. The VPN internet connection is then activated exclusively for result transmission. KPPS subsequently performs a manual physical count of the VVPAT slips and compares it directly with the Digital C1 as a polling-station-level local audit mechanism. The Constitutional Court recognizes the sealed VVPAT Ballot Box as the primary evidence in election-result

disputes (PHPU), thereby allowing Constitutional Court judges to conduct a material forensic recount in the courtroom.

Establishing Mission Objectives

A vital stage of the NIST CSF is the establishment of Mission Objectives (MOs) as reference points for risk mitigation and for safeguarding the confidentiality, integrity, and availability of electoral systems in accordance with the constitutional mandate. The ten Mission Objectives are: (MO-1) ensure the integrity of election results as a national democratic asset; (MO-2) ensure the reliability and availability of the e-voting system throughout the electoral cycle; (MO-3) establish e-voting cybersecurity as part of national security; (MO-4) control the risks of vote manipulation, system sabotage, and digital interference; (MO-5) ensure that all e-voting system assets are inventoried and protected; (MO-6) ensure that only authorized parties can access election systems and data; (MO-7) ensure that all voting and vote-counting transactions can be audited and verified; (MO-8) detect anomalies, attacks, and digital fraud early and in real time; (MO-9) ensure a rapid and coordinated response to incidents on election day; and (MO-10) ensure the recovery of election systems and results without loss of integrity or public trust.

Risk Assessment and Gap Analysis

This study conducted a risk assessment by comparing the organizers' current internal practices (Current Profile) with the intended mitigation practices (Target Profile). The gap analysis uses a risk-priority scale based on the impact on the ten established Mission Objectives. Table 3 defines the Current Priority scale used in the analysis, while Table 4 defines the Target Tier scale.

Table 3. Current Priority Scale

Current Priority	Description
1	Highest priority; the current condition presents a high risk to the integrity of election results, the reliability of the e-voting system, and public trust.
2	High priority; the current condition still contains gaps that could increase risk unless immediately strengthened.
3	Medium priority; the condition is relatively controlled but requires improvement for medium-term strengthening.
4	Low priority; the current condition does not indicate high urgency and can be improved at a later stage.

Source: Adapted from the NIST CSF 2.0 Implementation Tiers.

Table 4. Target Tier Scale

Target Tier	Description
4	Formal policies and procedures are updated regularly; controls and security awareness are implemented consistently using current technology.
3	Formal policies and/or procedures exist; controls have been implemented and cybersecurity awareness is present.
2	Formal policies and/or procedures exist, but implementation is not yet consistent.
1	No policies or procedures exist; controls and awareness are not implemented consistently; adequate technology is not used.

Source: Adapted from the NIST CSF 2.0 Implementation Tiers.

Table 5 presents a gap-analysis matrix identifying 41 security gaps together with recommendations for implementing the target mitigation practices. The CP column refers to Current Priority, while the TT column refers to Target Tier.

Table 5. Cybersecurity Gap Analysis of the E-Voting System Based on NIST CSF 2.0

NIST Subcategory	*Current Internal Practices*	CP	*Target Internal Practices*	TT
GV.OC-01	Cybersecurity is still viewed as an additional technical burden rather than a central pillar of electoral integrity. Leaders place greater emphasis on meeting physical-logistics schedules than on system resilience, so cyber risks are often compromised in order to meet plenary deadlines.	2	Establish cybersecurity as part of national security (MO-3). Internalize a risk-aware culture by requiring a cyber-impact assessment for every plenary policy that may affect vote integrity.	4

GV.OC-04	Sidalih and Sirekap are identified as critical systems, but system-capacity limitations are often not communicated honestly. This condition causes public trust to decline when disruptions are perceived as manipulation of election results.	1	Ensure system reliability throughout the electoral cycle (MO-2). Establish a real-time communication channel that publishes e-voting system-health indicators to preserve legitimacy and public trust.	4
GV.OC-05	KPU depends on external vendors, but third-party cyber-compliance audits are generally treated merely as an administrative formality at the initial tender stage, without continuous technical supervision throughout the contract period.	2	Ensure that all vendor assets are protected and controlled (MO-5). Require independent technical audits and penetration testing of vendors every three months to close opportunities for digital interference.	3
GV.RM-01	Risk objectives derived from legal policies are often established without comprehensively mapping their cyber impacts, causing risk mitigation to become misaligned with the dynamics of system-sabotage threats on election day.	2	Control the risks of vote manipulation and system sabotage (MO-4) by establishing formal risk thresholds jointly agreed upon by KPU and Bawaslu.	4
GV.RM-04	Tolerance limits for system-disruption duration are not clearly communicated to regional levels, causing procedural uncertainty and operator panic when technical problems occur.	2	Ensure system recovery without loss of public trust (MO-10). Establish risk-response options that prioritize restoring the integrity of vote data through transparent technical measures.	3
GV.RR-01	Leaders tend to delegate cybersecurity responsibility entirely to technical personnel. DKPP Decision No. 4/2024 records weaknesses in ethical accountability, as leaders did not promptly take corrective action after becoming aware of failures in data protection.	1	Leaders bear full legal and ethical responsibility for the integrity of votes as a national democratic asset (MO-1). Every cyber failure must be reported honestly and transparently.	4
GV.PO-01	Formal policies are available (ISO 27001), but administrative sanctions against internal personnel who violate security procedures are rarely enforced in practice.	2	Ensure that only authorized parties can access the system (MO-6) by automatically enforcing policies through technical mechanisms and reporting every violation to DKPP.	3
GV.OV-01	Cybersecurity-strategy evaluations are conducted very late, generally long after the election has concluded, so the results cannot be used for tactical improvements during ongoing stages.	3	Ensure system reliability throughout the electoral cycle (MO-2) through weekly reviews of the security strategy to adjust defensive direction based on the latest threat intelligence.	3
ID.AM-01	Central servers are well documented, but controls over officials' personal devices (BYOD) in regional areas that connect to the system network are very weak and are not included in the central monitoring inventory.	2	Ensure that all e-voting system assets are inventoried and protected (MO-5). Implement a unique digital identity for every physical device to prevent sabotage or device substitution.	3
ID.AM-02	The main applications are registered, but the versions of supporting open-source libraries and dependencies are rarely audited, leaving KPU vulnerable to supply-chain attacks.	2	Validate the integrity of all e-voting software components (MO-5). Ensure that no service or system operates without central authorization through dynamic software-list management.	3
ID.AM-03	Massive volumes of data were successfully extracted without triggering automated alerts because data-flow visualization and exfiltration monitoring at the central gateway were insufficient, as demonstrated in DKPP Decision No. 4/2024.	1	Detect every data-flow anomaly or instance of digital fraud early and in real time (MO-8) by automatically blocking any flow that deviates from official patterns.	4
ID.AM-05	Security efforts focus on KPU headquarters while neglecting critical points at the district level, where manual recapitulation data are primarily entered into electronic systems and the risk of manipulation is very high.	2	Ensure the integrity of election results (MO-1) by assigning the highest protection priority to voting-terminal infrastructure and vote-counting databases.	4
ID.AM-07	Metadata classifications are often mixed, making it difficult to apply automated access controls based on confidential/public data labels in the database and increasing the risk of unauthorized access to voter data.	1	Ensure that only authorized parties can access data (MO-6) through strict metadata management that separates vote data from voter data.	3
ID.RA-01	The 2023 BSSN ITSA findings identified a Privilege Escalation vulnerability in Sidalih, but remediation	1	Control the risk of vote manipulation (MO-4) by requiring critical	4

	was often postponed to preserve system availability, leaving the vulnerability exposed on election day.		vulnerabilities to be remediated within hours before the system is used to serve public data.	
ID.RA-03	KPU focuses excessively on external hackers while overlooking manipulation threats from internal accounts with administrative authority. Insider threats have not been mapped in depth in the official threat register.	1	Detect sabotage and digital-interference threats early (MO-4, MO-8) by recording the attack tactics of both foreign and internal actors to strengthen the detection of digital fraud.	4
ID.RA-04	Impact analysis is limited to the technical duration of system downtime. KPU does not yet have a methodology for calculating the delegitimizing effects of an election and the potential for social unrest resulting from the exploitation of cyber vulnerabilities in the recapitulation system.	2	Ensure system recovery without loss of public trust (MO-10) through impact assessments that integrate national-stability variables into evaluations of potential cyber failures.	4
ID.RA-05	Risk scoring remains manually qualitative, making cyber-mitigation budgeting imprecise. Risks with major consequences for vote integrity often receive the same resource allocation as administrative risks.	2	Protect the integrity of election results (MO-1) by using cyber-intelligence data to prioritize mitigation according to the probability of real attacks against democratic assets.	3
ID.RA-06	Critical-risk mitigation is often delayed by rigid procurement-budget bureaucracy, preventing a rapid risk response during quiet periods when new vulnerabilities are discovered.	2	Ensure system reliability throughout the electoral cycle (MO-2). Ensure that risk-response measures are transparently monitored by Bawaslu to maintain accountability for corrective actions.	3
ID.RA-09	Procurement focuses on price; the integrity of application code and vendor hardware is rarely subjected to in-depth forensic audits to confirm the absence of backdoors before distribution to regional areas.	3	Control the risks of sabotage and digital interference (MO-4) through cryptographic integrity checks on every e-voting device before use.	3
ID.IM-04	An incident-response plan is available at headquarters, but field operators often resort to trial and error when systems fail because no practical technical playbook is available, slowing recovery on election day.	1	Ensure a rapid and coordinated response (MO-9) by preparing tested tactical scenarios for every type of cyber disruption affecting regional voting terminals.	4
PR.AA-01	DKPP Decision No. 53/2024 revealed widespread account sharing among operators in order to meet data-entry targets, destroying individual accountability and complicating investigations into illegal vote-data entries.	1	Ensure that only authorized parties can access the system (MO-6) through unique biometric/NIK-based identities that make every vote-data entry individually accountable.	4
PR.AA-03	Authentication was initially weak; KPU required 2FA/MFA only reactively after the massive Sidalih data breach, rather than adopting it as a security-by-design standard from the outset.	1	Ensure that all transactions can be verified (MO-7) by requiring physical-token- or biometric-based MFA for every access to critical vote-counting functions.	4
PR.AA-05	Regional administrators are often granted excessive access rights for operational convenience. Separation of duties between data-entry operators and verifiers is frequently violated, creating opportunities for collusive vote manipulation.	1	Ensure that only authorized parties can enter the system (MO-6) by limiting regional-administrator privileges and enforcing separation of duties under Bawaslu's independent supervision.	4
PR.DS-01	DKPP decisions reveal that the Sidalih database was not fully encrypted or strongly masked, allowing hackers to read massive quantities of raw voter personal data after penetrating the network perimeter.	1	Ensure the integrity of election results (MO-1) by implementing strong database encryption (AES-256) for every vote-count result field.	4
PR.DS-02	HTTPS is used, but dedicated data-communication channels from polling stations often do not pass through a stable VPN, leaving data vulnerable to interception when cellular signals in remote areas are unstable.	1	Ensure that all voting transactions can be verified (MO-7) by protecting data transmission from voting devices to the central server with end-to-end encryption.	4
PR.DS-10	Servers do not use memory isolation; vote data being calculated in RAM can be manipulated through code-injection techniques at the application-runtime level without leaving traces in storage logs.	2	Control the risks of manipulation and sabotage (MO-4) by isolating vote-counting processes within secure hardware-based enclaves.	4
PR.DS-11	A Disaster Recovery Center (DRC) is operational, but backups are not protected by immutability	1	Ensure the recovery of election results without loss of integrity (MO-10) by	4

	technology, creating a risk that backup data could also be deleted or encrypted if attackers deploy ransomware in the primary infrastructure.		implementing immutable data backups (WORM) that are routinely validated.	
PR.PS-04	Applications generate activity logs, but these are not aggregated to the Security Information and Event Management (SIEM) monitoring center in real time, so suspicious administrator activity is often detected several days late.	1	Ensure that all voting transactions can be audited (MO-7) through secure log records for post-election forensic verification.	4
PR.PS-06	Sirekap development is subject to tight deadlines; code-security reviews (SAST/DAST) are often subordinated to the need for sudden feature releases, allowing critical vulnerabilities to reach production.	1	Ensure system reliability throughout the electoral cycle (MO-2) by integrating automated security scanning into every code-development cycle.	4
DE.CM-01	The Network Operations Center (NOC) focuses on service availability; Layer 7 application-traffic anomaly detection cannot yet automatically stop mass downloads by attackers whose access patterns resemble normal traffic.	1	Detect every anomaly and attack early and in real time (MO-8) through an artificial-intelligence-enhanced network-monitoring system that proactively identifies attack patterns.	4
DE.CM-03	Administrator logs are recorded, but behavioral-pattern analysis is not conducted routinely. Suspicious administrator activity outside official working hours is difficult to detect proactively before data damage occurs.	2	Control the risks of manipulation and internal digital interference (MO-4) by monitoring user behavior and instantly detecting deviations from assigned duties.	3
DE.CM-09	Runtime-level monitoring for fileless malware in server memory remains very limited. Traditional antivirus software cannot detect modern threats that operate directly in the RAM of election servers.	2	Detect digital fraud early (MO-8) by continuously monitoring the integrity of the e-voting application's runtime environment.	4
DE.AE-02	Cyber analysts frequently experience alert fatigue; genuine attacks are often missed among thousands of false-warning logs on election day, delaying understanding of the actual scope of an attack.	1	Ensure a coordinated and rapid response (MO-9) by analyzing anomalous events in depth to understand the context of an attack immediately.	4
DE.AE-03	Cyber-threat intelligence from BSSN is available, but correlation across sources (server logs, applications, and external intelligence) remains manual and slow when responding to coordinated threats.	2	Detect anomalies and digital fraud early (MO-8) by automatically correlating threat information from BSSN, BIN, and internal sources.	4
DE.AE-04	Determining whether a system disruption is caused by an organic traffic surge or a DDoS attack takes too long, impeding tactical decision-making for rapid recovery.	1	Understand estimated incident impacts to ensure a rapid response (MO-9) through immediate visualization of the scope of affected assets.	3
RC.RP-01	A disaster-recovery plan (DRP) is available, but failover to the DRC during a crisis still requires lengthy manual intervention, causing interruptions to public services that can fuel fraudulent-election narratives.	1	Execute recovery immediately to ensure a rapid response on election day (MO-9). The system switches to backup infrastructure without interrupting service to voters.	4
RC.RP-02	Infrastructure recovery is prioritized, but application repairs are often implemented hastily through hotfixes without renewed integrity testing, creating a risk that new vulnerabilities will be introduced into the restored system.	2	Ensure system recovery without loss of integrity (MO-10) by implementing validated corrective measures before deployment.	4
RC.RP-03	Operators often restore backup data immediately without hash verification, creating a risk that backups manipulated by attackers will also be restored to the central production system.	2	Ensure that voting transactions can be verified (MO-7) by cryptographically checking backup-data integrity before restoration.	4
RC.RP-05	Post-incident confirmation that conditions have returned to normal is often conducted without an in-depth database-reconciliation audit, creating public doubt about the accuracy of recovered data, as documented in DKPP Decision No. 53/2024.	2	Ensure the restoration of public trust (MO-10) through a transparent vote-data reconciliation audit accessible to Bawaslu.	4
RC.CO-03	Horizontal coordination with law-enforcement agencies is functioning, but technical coordination with regional offices to reduce public panic and information uncertainty is often delayed.	1	Communicate recovery progress intensively among KPU, Bawaslu, and BSSN to ensure a coordinated response (MO-9).	4
RC.CO-04	Notifications of cyber failures are not transparent and tend to be defensive. Fraud narratives on social media spread more rapidly than KPU's official	1	Ensure the restoration of public trust (MO-10) by providing honest, rapid, and	4

	clarifications, further delegitimizing the electoral process.	transparent recovery updates to all stakeholders.

Source: Research analysis based on NIST CSF 2.0; DKPP Decisions No. 4/2024 and No. 53/2024.

Discussion

The gap analysis reveals a pattern of systemic deficiencies in Indonesia's electoral cybersecurity ecosystem. Of the 41 NIST CSF 2.0 subcategories analyzed, most are assigned Current Priority levels 1 and 2, indicating critical conditions that require urgent attention. Most targets are set at Tier 4, indicating the need for comprehensive transformation that extends beyond technical measures to encompass governance and human-resource dimensions (National Institute of Standards and Technology, 2014).

The most critical findings occur in the Protect category. The widespread practice of account sharing among KPPS operators to meet recapitulation targets, as documented in DKPP Decision Number 53-PKE-DKPP/III/2024, fundamentally undermines the non-repudiation principle of information systems. When anomalous inputs occur, such as the manipulation of vote results, the system cannot identify the authentic responsible party. This condition directly contradicts Mission Objective MO-6, which underpins the legitimacy of election administration. The finding is consistent with Krivonosova and Iova (2021), who conclude that electoral cybersecurity failures generally originate in weaknesses in operational procedures and human accountability rather than solely in the sophistication of the technology used.

In the Governance and Risk Identification categories, the absence of continuous vendor audits and the postponement of patching to preserve system uptime have demonstrably created pathways for advanced threat actors. The fact that KPU's gateway monitoring failed to detect large-scale data exfiltration, as revealed in DKPP Decision Number 4-PKE-DKPP/I/2024, reinforces the finding of Shackelford et al. (2020) that election infrastructure not protected by behavioral-analytics-based intrusion-detection systems will remain vulnerable to exfiltration attacks that exploit legitimate access channels. This finding indicates that a Zero Trust Architecture (ZTA) should form the foundation of the security architecture for the next generation of election systems.

With respect to Incident Recovery, the absence of inclusive technical coordination with Bawaslu as an independent party creates room for public distrust during a crisis. This condition reinforces Norris's (2014) finding that electoral integrity is determined not only by the technical perfection of the system, but also by public perceptions of transparency and accountability throughout the process. In this context, the VVPAT architecture proposed in this study directly addresses the gap by providing physical material evidence that can be forensically audited, so that election-result disputes no longer depend solely on arguments regarding the integrity of server files.

The dual-recording architecture that positions VVPAT as primary evidence before the Constitutional Court constitutes an appropriate constitutional response to Constitutional Court Decision Number 147/PUU-VII/2009. This approach also aligns with international best practices recommended by the United States Election Assistance Commission (EAC) and the Council of Europe's Guidelines on E-Voting, which require a physical audit mechanism independent of the primary computing system (Annisa et al., 2020). This framework differs from the paperless DRE approach implemented in 2009, which has proven vulnerable to manipulation without an audit trail (Shackelford et al., 2020).

The redesign of the roles of the seven KPPS members, as presented in Table 3, demonstrates that the digitalization of voting does not entail reducing human resources, but rather upgrading qualifications and specializing functions. This is relevant to Kersting and Baldersheim's (2004) finding that the success of e-voting in various countries depends heavily on the preparedness of election personnel, not merely on the reliability of technological infrastructure.

Overall, the root causes of current weaknesses in Indonesia's electoral cybersecurity are not solely technological limitations; they also arise systemically from operational governance that frequently subordinates cybersecurity parameters to the pressure of meeting physical-logistics targets. Therefore, applying NIST CSF 2.0 as a standard for electoral cyber-risk management must be accompanied by organizational-culture reform and firm accountability mechanisms, as recommended in Table 6.

The gap analysis between historical vulnerabilities and ideal constitutional standards produced cybersecurity strategy recommendations intended to transform the conventional hybrid election system into a proactive, cross-sector defense. Table 7 summarizes the action plan based on the six NIST CSF 2.0 functions and identifies the institutional entities responsible for each action.

Table 6. Cybersecurity Strategy Recommendations by NIST CSF 2.0 Function

NIST CSF 2.0 Function	*Action Plan*	Institutional Entities
Govern	Ratify a KPU regulation requiring the provision of a read-only Application Programming Interface (API) for Bawaslu to access the server. Formalize supply-chain risk management for election-hardware vendors using factory-certified Hardware Security Modules.	General Election Commission, Election Supervisory Body, BSSN
Identify	Conduct an inventory of cryptographic systems. BSSN conducts red-team penetration testing to model Advanced Persistent Threat (APT) infiltration maneuvers against the Sidalih codebase, Control Units, and interface portals before election day.	KPU, BSSN, Independent IT Forensic Auditors
Protect	Require all e-voting terminals to remain computationally quarantined (air-gapped) while voting is in progress. Implement hardware-based Multi-Factor Authentication (MFA) controls for KPU administrator-level staff to mitigate insider threats.	Ministry of Communication and Informatics, BSSN, KPU, Directorate General of Population and Civil Registration
Detect	Operate a 24/7 Security Operations Center (SOC). Inject sanity-check logic into database gateways to immediately prevent the publication of arithmetic errors and detect anomalous server queries.	KPU IT Team, Bawaslu, BSSN
Respond	Formalize an incident-response protocol with emergency network isolation within less than 15 minutes. The Cyber Task Force acts rapidly to expose the dissemination of manipulated deepfakes that could trigger public distrust through forensic verification of digital logs.	Indonesian National Police Cyber Task Force, KPU, Bawaslu, Ministry of Communication and Informatics
Recover	Legally recognize the VVPAT Printed-Receipt Evidence Box as conclusive e-voting evidence before the Constitutional Court if the server is compromised by ransomware. Prepare immutable offline backups for computational data.	KPU, Constitutional Court, Bawaslu

Source: Research analysis based on NIST CSF 2.0 and Indonesia's electoral regulatory framework (Pascoe et al., 2024).

Conclusion

This study demonstrates that Indonesia's electoral information-system ecosystem continues to contain vulnerabilities across its main subsystems, including Sidalih, Sipol, Silon, Sikadeka, Silog, Sirekap, and Bawaslu's oversight systems. The analysis shows that the principal problems are not confined to technical aspects, but also involve access governance, data validation, system reliability, and interinstitutional coordination. The proposed dual-recording e-voting architecture with VVPAT confirms that physical evidence remains necessary to preserve transparency, auditability, and the legitimacy of election results. In addition, the risk assessment and gap analysis show that most deficiencies are high priority, particularly in the areas of protection, identity and access, anomaly detection, and incident recovery.

The scientific value of this study lies in integrating NIST CSF 2.0 with the Indonesian electoral cybersecurity context and strengthening the institutional-oversight perspective through the roles of KPU, Bawaslu, and DKPP. Its practical contribution is reflected in the formulation of mission objectives and an action plan that can serve as a basis for policymaking, strengthening technical controls, and designing more accountable governance. From a policy perspective, the findings affirm that e-voting

implementation cannot be separated from procedural reform, independent oversight, supply-chain security, and audit mechanisms that can be verified both physically and digitally.

This study is limited by its use of descriptive-diagnostic analysis based on qualitative data; consequently, the findings are not intended for broad statistical generalization. The scope is also limited to Indonesia's electoral ecosystem and to the documents, observations, and decisions available for this study. Future research should test the proposed security-profile design through technical simulations, implementation trials in more operational environments, and quantitative evaluation of the effectiveness of each mitigation control. Further studies should also examine human-resource readiness, institutional resistance, and the integration of cross-agency oversight in greater depth so that the resulting design is more applicable at the national scale.

Acknowledgment

The authors express their gratitude to the School of Industrial Engineering at Telkom University for providing academic support and research facilities throughout the preparation of this study. Appreciation is also extended to the General Election Commission (KPU), the Election Supervisory Body (Bawaslu), and the various related institutions that provided documents, regulations, and open reports serving as important data sources for this research.

The authors also acknowledge the lecturers, fellow researchers, and other parties who provided feedback, suggestions, and constructive academic discussions that helped improve this article. The perspectives of cybersecurity and electoral-governance practitioners also made a meaningful contribution to strengthening the analysis.

The authors further thank previous researchers and institutions that produced studies on electoral cybersecurity, e-voting, digital governance, and the NIST Cybersecurity Framework, which formed an important foundation for the development of this research.

References :

Afiansyah, H. G., & Amiruddin, A. (2019). Perancangan Rencana Tata Kelola dan Manajemen Teknologi Informasi Menggunakan COBIT 2019 dan NIST SP 800-53 Rev 5 (Studi Kasus: Instansi Pemerintah ABC). Jurnal Info Kripto, 6(1), 33–39.

Annisa, A. N., Kadaruddin, Yunus, A., Anas, A. M. A., Juniar, M. W., Wahyuni, A. S., Kurniawati, A., & Librayanto, R. (2020). Improving Accessibility of The Right to Persons with Mental Disabilities in General Election. Journal of Critical Reviews, 7(19), 905–909.

Arinze, S. N., & Nwajana, A. O. (2025). RFID-Enabled Electronic Voting Framework for Secure Democratic Processes. Telecom, 6(78), 1–19.

Berenjestanaki, M. H., Barzegar, H. R., Ioini, N. El, & Pahl, C. (2024). Blockchain-Based E-Voting Systems: A Technology Review. Electronics, 13(17), 1–38.

Brady, M., Franklin, J. M., Sames, C., Brady, M., Franklin, J. M., Sames, C., & Snyder, J. (2024). Cybersecurity Framework Election Infrastructure Profile.

Chaudary, T. (2022). Cybersecurity is Fundamental to Elections.

Dewan Kehormatan Penyelenggaraan Pemilihan Umum. Putusan Nomor 4-PKE-DKPP/I/2024, (2024).

Dewan Kehormatan Penyelenggaraan Pemilihan Umum. Putusan Nomor 53-PKE-DKPP/III/2024, (2024).

Fitzpatrick, J., & Jöst, P. (2022). “The High Mass of Democracy” — Why Germany Remains Aloof to the Idea of Electronic Voting. Frontiers in Political Science, 4(July), 1–14. https://doi.org/10.3389/fpos.2022.876476

Hastuti, D., Rochman, S., & Aini, R. S. Z. (2024). Cybersecurity Measures For Election Information Systems : Sistem Rekapitulasi Suara Pemilu 2024 (siRekap). Journal of Applied Electrical & Science Technology, 06(01), 20–24.

International Foundation for Electoral Systems. (2023). Electoral Cybersecurity : A Brief Guide for Donor Program Development.

Kementerian Petahanan Republik Indonesia. Pedoman Pertahanan Siber, (2014).

Kersting, N., & Baldersheim, H. (2004). Electronic Voting and Democracy: A Comparative Analysis.

Khatami, M. I., & Rahayu, R. (2024). Cybersecurity Leadership in Safeguarding Election Voter Data (Case Study: Implementation of the SIDALIH Information System by the Indonesian General Election Commission). Jurnal Komunikasi Indonesia, 13(1), 81–97. https://doi.org/10.7454/jkmi.v13i1.1215

Krivonosova, I., & Iova, R. A. S. (2021). From the Parliament to a Polling Station: How to Make Electoral Laws More Comprehensible to Election Administrators. Election Law Journal, 20(4), 364–381. https://doi.org/10.1089/elj.2020.0670

Mahkamah Konstitusi Republik Indonesia. Putusan Nomor 147/PUU-VII/2009, (2009).

National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0). Department of Commerce.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

Norris, P. (2014). Why Mass Perceptions of Electoral Integrity Matter for Legitimacy.

Presiden Republik Indonesia. Undang-Undang Republik Indonesia Nomor 7 Tahun 2017 tentang Pemilihan Umum, (2017).

Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, (1945).

Shackelford, S. J., Raymond, A., Stemler, A., & Loyle, C. (2020). Defending Democracy : Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity. Washington and Lee Law Review, 77(4).

Staak, S. Van Der, & Wolf, P. (2019). Cybersecurity in Elections. International Institure for Democracy and Electrocal Assistance.

Sumardi. (2024). Penguatan Sistem Pengawasan dalam Penyelenggaran Tahapan Pemilu 2024. Journal of Government Insight, 2, 210–220. https://doi.org/10.47030/jgi.v1i1.53

Tampubolon, F. D. G., Amin, M., & Harahap, H. (2021). Pengaruh Informasi Sistem Penghitungan Nasional Online pada Hasil Pemilu 2019 terhadap Kepercayaan Publik Kota Medan. PERSPEKTIF, 10(2), 399–415. https://doi.org/10.31289/perspektif.v10i2.4601

Vincent, A., Alihodzic, S., & Gale, S. (2021). Risk Management in Elections. Australian Electoral Commision and International for Democracy and Electoral Assistance.

Walker, C. P., Schiff, D. S., & Schiff, K. J. (2024). Merging AI Incidents Research with Political Misinformation Research: Introducing the Political Deepfakes Incidents Database. ArXiv, 38(21).

Wamala, F. (2011). ITU National Cybersecurity Strategy Guide. International Telecommunication Union.