



Digitalization of Electoral Governance in Indonesia: Pancasila, Online Voting, Verified Voter Registration, and Electoral Integrity for the 2029 National Election and Subsequent Local Elections

Maysarah

Universitas Dharmawangsa

Corresponding Author: Maysarah maysarah@dharmawangsa.ac.id

ARTICLE INFO

Kata Kunci: Pancasila, Digital Election, Online Voting, Voter Registry, Electoral Integrity, Election Law, Local Elections, Cybersecurity, Democratic Governance

Received : 6 August 2026

Revised : 24 September 2026

Accepted: 25 October 2026

©2026 Maysarah: This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRAK

This article examines the constitutional and governance challenges of digitalizing electoral administration in Indonesia, with attention to the 2029 national election and the subsequent local-election cycle. It integrates a Pancasila-based reconstruction of democratic governance with a proposed Verified Digital Electoral Integrity Model (V-DEIM), consisting of a continuously verified voter registry, electronic authentication, privacy-preserving online voting, immutable audit trails, multi-institutional complaint handling, and independent post-election audits. The study uses normative legal analysis, comparative governance analysis, and secondary-data analysis of official electoral sources. It does not assume that allegations of manipulation in the 2024 election were proven; documented administrative problems and enforcement data are treated as risk indicators. Official KPU data recorded 204,807,222 voters in the 2024 permanent voter register, while Bawaslu reported 531 violations, 386 matters classified as non-violations, and 279 matters still under process in its cited national handling snapshot. The analysis finds that Constitutional Court jurisprudence permits electronic voting only when cumulative conditions are met, that the 2024 data justify stronger preventive controls without supporting a generalized conclusion of manipulation, and that Pancasila values can be translated into verifiable technical safeguards. Online voting should therefore be introduced through staged, hybrid pilots after independent certification of secrecy, cybersecurity, auditability, accessibility, and institutional readiness. The model is conceptual and requires technical and empirical testing

INTRODUCTION

Indonesia's electoral system has entered a period in which constitutional law, administrative data governance, cybersecurity, and citizen participation must be treated as a single governance problem. The Constitutional Court has directed that, beginning in 2029, national and local elections be separated: elections for the President, the DPR, and the DPD form the national election, while DPRD and regional-head elections form the local election cycle. This development creates an opportunity to redesign electoral administration rather than reproduce the previous five-ballot model.

Reform must nevertheless remain anchored in Pancasila and the 1945 Constitution. The author's earlier Pancasila-oriented study on constructing a system of government that secures national stability, legal certainty, and public welfare is used here as a normative premise: stability and administrative order should not be separated from democracy, human rights, constitutional supremacy, accountability, and social welfare. In the electoral context, efficiency cannot justify a system that weakens ballot secrecy or public verification.

The problem is not simply whether Indonesia can place voting online. The deeper question is whether digitalization can make the whole electoral chain (voter registration, authentication, voting, counting, tabulation, complaints, adjudication, and audit) more transparent and more resistant to unauthorized intervention. The 2024 election supplies documented administrative and enforcement data that can serve as a baseline for 2029 risk mapping. Such data should not, however, be turned into unsupported allegations that a particular candidate or institution manipulated the national result.

This article focuses on five linked risks: inaccurate voter registers; identity impersonation or duplicate voting; manipulation or unauthorized alteration of vote data; inaccessible complaint mechanisms; and excessive logistical expenditure. It also addresses the concern that reserve ballots could create opportunities for abuse. The official record shows that the 2024 operational reserve was 2 percent, not 30 percent, so the policy question is whether reserve-ballot mechanisms should be reduced, redesigned, or replaced by secure digital contingencies.

The article asks three questions. (1) What do Indonesian constitutional and statutory law require of digital voting? (2) What does the official 2024 baseline show about risks that digitalization should address? (3) How can Pancasila values be translated into a verifiable digital election architecture? Its contribution is to integrate Pancasila constitutional values with a verifiable digital election architecture, rather than treating digitalization as a purely technological reform.

IMPLEMENTATION AND METHODS

This is a conceptual and normative policy study that combines three approaches. First, normative legal analysis examines the 1945 Constitution, Law No. 7 of 2017 on General Elections, Law No. 10 of 2016 on regional elections, the population-administration regime, personal-data protection legislation, and Constitutional Court decisions on electronic voting and on the separation of national and local elections. Second, comparative governance analysis draws on the Estonian experience of internet voting within a national digital-identity

infrastructure and on the standards and methodologies of the Council of Europe, OSCE/ODIHR, and International IDEA. Third, secondary-data analysis uses official Indonesian sources, namely KPU voter-register and logistics documentation and Bawaslu enforcement data and evaluation communications. The normative premise comes from a Pancasila-based reconstruction of democratic governance developed in the author's earlier manuscript. From that premise and the findings of the three approaches, the study builds the V-DEIM model through conceptual design. Because the topic is politically charged, the study applies an explicit evidentiary rule: it distinguishes (a) documented administrative findings, (b) allegations submitted by participants, (c) adjudicated violations, and (d) proven criminal conduct, and it draws conclusions only at the level that the source supports. Numerical data are taken from the official sources cited and are not re-estimated, except for simple shares calculated by the author and labelled as such.

The study has limits. It reports no primary data, no technical testing of any voting system, and no cost data. The Bawaslu figures are a handling snapshot taken from an evaluation communication, not a final adjudication record. The model is therefore a framework for further legal, technical, and empirical testing.

RESULTS AND DISCUSSION

Legal Framework and Constitutional Conditions

The constitutional basis is popular sovereignty under the 1945 Constitution, together with the principles governing elections and regional elections. The principal statutory framework consists of Law No. 7 of 2017 on General Elections, Law No. 10 of 2016 on regional elections, the population-administration regime, and personal-data protection legislation. Three Constitutional Court decisions shape the analysis (Table 1).

Table 1. Constitutional Court Decisions Relevant to Electoral Digitalization

Decision	Relevance to digital elections
No. 147/PUU-VII/2009	Electronic voting can be constitutional when cumulative conditions are met: compliance with the principles of direct, general, free, confidential, honest, and fair elections (LUBER-JURDIL), and sufficient readiness of technology, financing, human resources, software, and the community.
No. 137/PUU-XXII/2024	Again discusses electronic voting and recognizes its potential for effectiveness and efficiency, while referring back to the readiness requirements.
No. 135/PUU-XXII/2024	Separates national and local elections from 2029; this should be reflected in statutory reform, technology procurement, voter education, and audit planning.

The 2024 official baseline

The 2024 permanent voter register contained 204,807,222 voters: 203,056,748 domestic and 1,750,474 overseas. The infrastructure comprised 820,161 domestic polling stations and 3,059 overseas voting facilities (Table 2). These figures show the scale at which a verified digital registry would operate

Table 2. Official 2024 Voter Register and Voting Infrastructure

Indicator, 2024	Value
Permanent voter register, total	204,807,222
Domestic voters	203,056,748
Overseas voters	1,750,474
Male voters	102,218,503
Female voters	102,588,719
Domestic polling stations (TPS)	820,161
Overseas voting facilities	3,059
Operational reserve ballots	2% of DPT at polling-station level (not 30%)

Bawaslu's public data system reports national, provincial, and district-level information on violations. In the national handling snapshot cited in its evaluation communication, 531 matters were classified as violations, 386 as non-violations, and 279 were still under process (Figure 1). Of the 1,196 matters in this snapshot, these correspond to about 44.4%, 32.3%, and 23.3% respectively (author's calculation). The snapshot is not a national conviction rate and does not show that every report constituted an electoral crime.

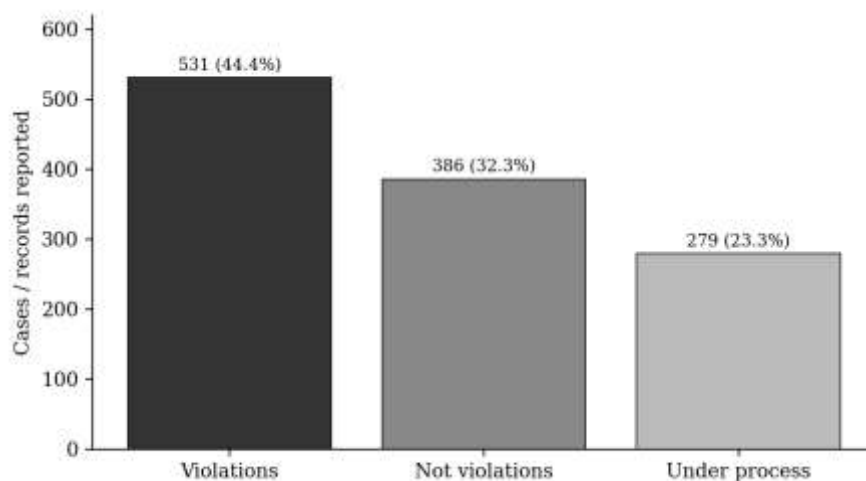


Figure 1. Bawaslu 2024 National Handling Snapshot. Counts from the Bawaslu Evaluation Communication; Percentages Calculated by the Author. Source: Bawaslu

Bawaslu's evaluation also identified operational problems during voting and counting, including mismatched ballots, late opening of polling stations, domicile-related voting issues, and instances of multiple voting. It reported recommendations for repeat or continued voting at 1,692 polling stations, of which 1,521 (about 89.9%, author's calculation) were reportedly acted upon by KPU in the cited evaluation.

Comparative findings

International experience shows that digital voting is not a single technology (Table 3). The lesson is not that one country can be copied wholesale, but that technology must be embedded in a wider legal and institutional ecosystem.

Table 3. Comparative Governance Findings

Jurisdiction / framework	Relevant feature	Lesson for Indonesia
Estonia	National digital identity and internet voting	Identity infrastructure must be mature before remote voting becomes scalable.
Council of Europe	Standards on e-voting, transparency, and trust	Legal and technical safeguards must operate together.
OSCE/ODIHR	Election observation and assessment methodology	Independent observation should include digital processes, not only polling stations.
Indonesia	Constitutional recognition of conditional e-voting	Readiness, LUBER-JURDIL, and public trust are legal conditions, not optional features.

Translation of Pancasila values into technical safeguards

The five principles of Pancasila can be operationalized as design requirements (Table 4). The first principle requires respect for human dignity and freedom of conscience; the second, humane and non-discriminatory access; the third, national interoperability without fragmentation; the fourth, authentic popular sovereignty and accountable decision-making; and the fifth, equal access, fairness, and prevention of structural exclusion. The table also lists a fifth dimension, constitutional legality, as used in the framework.

Table 4. Pancasila Dimensions and Electoral Design Implications

Pancasila dimension	Electoral design implication
Human dignity	Accessible authentication; disability accommodation; informed consent; no coercive voting environment.

Pancasila dimension	Electoral design implication
Unity of Indonesia	Single interoperable national standards with local implementation safeguards.
Popular sovereignty	End-to-end verifiability, public auditability, meaningful citizen observation, and lawful dispute resolution.
Social justice	Equal digital access, offline alternatives during verified outages, affordability, and assistance for vulnerable voters.
Constitutional legality	Clear statutory authority, independent oversight, judicial review, data protection, and sanctions with due process.

This mapping is a conceptual normative framework, not an empirical score; no weighting among the dimensions is implied.

The proposed Verified Digital Electoral Integrity Model (V-DEIM)

The V-DEIM integrates the Pancasila constitutional framework with a complete digital electoral chain in eight layers (Table 5 and Figure 2).

Table 5. The Eight Layers of V-DEIM

Layer	Core mechanism	Integrity objective
1. Living Voter Registry	Continuous legal-status reconciliation	Prevent stale, duplicate, and invalid identities
2. Verified Identity	NIK/e-KTP plus multi-factor authentication	Prevent impersonation
3. Secure Voting	End-to-end encryption and privacy separation	Preserve ballot secrecy
4. Immutable Audit Trail	Cryptographic logs and independent verification	Detect unauthorized changes
5. Transparent Tabulation	Publicly reproducible aggregation	Prevent opaque score alteration
6. Digital Complaint System	Case ID, evidence upload, deadlines	Fast and traceable enforcement
7. Independent Audit	Pre-election, penetration, source-code, and post-election audits	Reduce systemic risk
8. Constitutional Review	Judicial remedies and institutional checks	Protect rights and due process



Figure 2. Layered Architecture of the Verified Digital Electoral Integrity Model (V-DEIM). Source: Author's Conceptualization based on Pancasila, the 1945 Constitution, and the Integrated Pancasila Governance Framework.

The model is designed so that no administrator can both authenticate voters and identify their ballot choices. The identity layer and the ballot layer are cryptographically separated, and a successful vote generates evidence that the ballot was accepted without revealing the candidate selected. Two supporting instruments complete the model. The Digital Election Passport is a secure credential linked to legally verified identity attributes but not to ballot content; it shows eligibility, participation status where legally permissible, and security alerts, and every administrator access is logged and independently auditable. The real-time public audit dashboard publishes aggregate information, system status, cryptographic proofs, audit reports, turnout totals, rejected transactions, and correction logs, without publishing personal voter data or individual ballot choices.

DISCUSSION

Interpreting the 2024 Baseline

The empirical baseline should begin with official data rather than allegations. The KPU register and Bawaslu handling data show why a digital integrity system should focus on verifiable controls, particularly in voter-register accuracy, the prevention of multiple voting, and the traceability of complaints. They do not, by themselves, prove that the national vote total was secretly altered or that a particular candidate was predetermined as the winner. Scholarly analysis must distinguish documented administrative findings, allegations submitted by participants, adjudicated violations, and proven criminal conduct.

For the same reason, the article does not label 2019 or 2024 as the "worst election." Such a label would require a transparent multidimensional methodology covering violations, adjudicated outcomes, violence, administrative failures, accessibility, participation, cybersecurity, and institutional compliance. Bawaslu itself has described 2024 violation data as a baseline for risk mapping for 2029, which supports using 2024 as an evidence base rather than as an unsupported ranking.

Pancasila as the Architecture of Digital Elections

Pancasila should not be ceremonial language appended to a digital-election project. A digital election is legitimate only when technological efficiency is subordinated to constitutional rights and when institutional power remains reviewable by citizens, independent oversight bodies, and courts. The integrated approach rejects two extremes: a purely procedural democracy in which formal voting exists but institutional accountability is weak, and administrative authoritarianism in which efficiency and stability reduce meaningful participation. In practice this means that no single actor (party, candidate, administrator, vendor, or law-enforcement officer) should control the entire election data chain. Separation of functions must be reproduced digitally: identity verification, ballot casting, encrypted ballot storage, counting, tabulation, complaint handling, and audit should not rest with one database administrator or one institution (Table 6).

Table 6. Institutional Checks and Balances in a Digital Election

Institution	Digital governance role	Independent control
KPU	Register, voting platform, tabulation, publication	External security audit; party and citizen observation; judicial review
Bawaslu	Supervision, complaints, evidence preservation	Transparent case IDs and deadlines
Dukcapil / population administration	Legal identity and vital-event status	Data-protection controls and lawful access logs
Police / prosecutors	Criminal investigation and prosecution	Due process and judicial authorization where required
Courts	Electoral disputes and constitutional review	Public decisions and reasoned judgments
Civil society / academia	Independent observation and technical audit	Accreditation and public methodology

The objective is "single verified data, multiple accountable institutions," not one institution controlling all election information.

Voter-Register Integrity and the Reserve-Ballot Issue

The proposed Living Voter Registry would continuously reconcile the electoral register with legally verified population events. A death record should trigger a legally controlled status change after a death certificate is registered through the competent population-administration process, and citizens should be able to report suspected death-record discrepancies through authenticated channels, subject to verification. The aim is not to publish sensitive population data but to prevent an inactive or deceased identity from remaining usable as an electoral credential. The registry should keep identity status separate from voting history: a voter is eligible or ineligible according to law, and the system should not reveal the ballot choice.

The initial proposal framed the reserve-ballot issue as a 30 percent reserve. Official 2024 documentation identifies a 2 percent reserve based on the DPT at polling-station level. This correction matters for scholarly accuracy. A study may still recommend eliminating or redesigning physical reserve ballots, but it must state the exact baseline and the operational purpose of the reserve. A secure digital system could use controlled failover credentials and auditable emergency procedures, each cryptographically limited, logged, independently observable, and incapable of producing an extra vote outside the legally verified voter population. This is a more precise anti-fraud objective than asserting that all reserve mechanisms are inherently fraudulent.

Complaints, Enforcement, and Accountability of Office Holders

Indonesia already has digital reporting and information infrastructure within electoral supervision. The proposed model extends it with a unified case-tracking interface through which citizens submit evidence, receive a case identifier, monitor procedural status, and obtain the final administrative, ethical, or judicial disposition. The idea that every reported offender should be immediately arrested requires legal qualification. A digital complaint is not itself proof of a crime. Immediate law-enforcement action should be triggered only where statutory thresholds for urgent intervention, *flagrante delicto*, evidence preservation, or other lawful grounds are met; otherwise due process and institutional competence must be preserved.

Likewise, the article does not propose that an online popular vote automatically remove an elected official once a petition reaches a threshold. That would require constitutional and statutory authority, defined grounds, evidence, due process, and safeguards against retaliatory or automated campaigns. A safer reform is to strengthen legally recognized recall, impeachment, electoral-dispute, and public-accountability mechanisms, using secure digital petitioning only as a verified trigger for a lawful procedure.

Remote Voting, Cybersecurity, Privacy, and Accessibility

Remote voting introduces risks that do not exist in the same form at a supervised polling station, including family or workplace coercion, malware on personal devices, phishing, denial-of-service attacks, compromised credentials,

and uncertainty about the voting environment. For this reason a hybrid transition is more legally defensible than immediate nationwide remote voting: digitally enabled voting can be piloted under controlled conditions while verified alternatives are retained for citizens who cannot safely or reliably use the system. This is consistent with the cumulative conditions set by the Constitutional Court.

An online election can remove some physical risks while adding cyber risks. The threat model should cover credential theft, malware, server compromise, insider threats, supply-chain attacks, denial of service, ransomware, social engineering, deepfakes, coordinated disinformation, and unauthorized access to voter data. Controls must be independently tested and publicly documented to the maximum extent consistent with operational security. Personal-data protection is equally important: the electoral authority should apply data minimization, purpose limitation, access controls, encryption, retention schedules, breach-notification procedures, and independent oversight, consistent with the personal-data protection law. A voter should never have to give up more personal information than is legally necessary to establish eligibility and authenticate the vote.

Accessibility is a constitutional issue. Citizens without reliable internet, older voters, people with disabilities, people in remote areas, and citizens affected by disasters must have an effective means of voting. "Online" should therefore mean digitally integrated, not "online-only at any cost."

Efficiency, Budget Governance, and A Staged Roadmap

The case for digitalization should not be reduced to the claim that physical polling stations can immediately disappear. Election logistics include accessibility, emergency continuity, remote and disadvantaged communities, cybersecurity, equipment maintenance, audit, voter education, and support services. KPU's 2024 logistics documentation shows the scale of the physical infrastructure: hundreds of thousands of polling stations, millions of ballot-related items, transport, warehousing, security, and personnel. Digitalization may reduce some recurring costs but creates new ones for secure infrastructure, independent testing, redundancy, incident response, and public digital literacy. A credible efficiency assessment must therefore compare total lifecycle costs rather than printing costs alone. No cost estimate is made in this article.

Table 7. Proposed Five-Year Reform Roadmap

Period	Priority
2026	Legal review; threat modelling; population-data reconciliation; public consultation.
2027	Controlled pilots; independent cybersecurity tests; accessibility testing; legislative amendments.
2028	Nationwide readiness assessment; certification; source-code escrow; disaster-recovery tests.
2029	National election implementation only if cumulative constitutional and technical readiness conditions are met.

Period	Priority
Post-2029	Independent audit; correction program; local-election adaptation; continuous registry improvement.

Before 2029, progress should be measured with transparent indicators rather than political labels (Table 8).

Table 8. Indicators to Measure before 2029

Indicator	2024 baseline / issue	2029 target
DPT integrity	204,807,222 registered voters	Continuously verified and auditable register
Voting infrastructure	820,161 domestic TPS; 3,059 overseas facilities	Risk-based digital/hybrid architecture
Handling transparency	Bawaslu publishes case datasets	End-to-end case tracking with deadlines
Repeat/continued voting	1,692 recommendations cited in evaluation	Digital prevention plus auditable emergency procedures
Security	Fragmented technology and physical chain	Independent certification and continuous monitoring

Recommendations for Electoral Law Reform

Six legal-reform recommendations follow. First, electoral legislation should define digital voting as a legally regulated voting method, not merely an administrative application, and specify conditions for deployment, independent certification, auditability, secrecy, accessibility, incident response, and remedies. Second, the voter-register regime should mandate continuous synchronization between electoral records and legally verified population events, including deaths, changes of domicile, and duplicate identities, with a citizen-facing correction channel and appeal rights. Third, the physical reserve-ballot system should be reviewed against documented operational needs; if retained, every use should be logged, justified, reconciled, and independently audited, and if replaced by digital contingencies, emergency credentials must be cryptographically constrained and publicly auditable. Fourth, all electoral complaints should receive a unique digital case number and a procedural timeline, routed to the competent body without erasing jurisdictional boundaries, with criminal enforcement remaining evidence-based and compliant with due process. Fifth, tabulation should use independent verification, so that the official result database generates cryptographic evidence allowing authorized observers and auditors to confirm that published totals correspond to accepted encrypted ballots without exposing individual choices. Sixth, any recall or removal mechanism should be created through constitutional and statutory procedures, with a legally defined succession mechanism.

Limitations

The study is normative and conceptual. It has no technical validation of V-DEIM, no usability or accessibility testing, no cost modelling, and no primary data. The Bawaslu figures are a snapshot from an evaluation communication and may differ from final adjudication records. Constitutional Court decisions and official data should be re-verified against the original documents at the time of publication. Future work should test the model through controlled pilots, independent security assessments, and comparative empirical research.

CONCLUSION AND RECOMENDATION

The digitalization of Indonesian elections should be understood as constitutional governance reform, not as a simple replacement of paper ballots with an application. Pancasila supplies a substantive normative framework: human dignity, unity, popular sovereignty, social justice, and legality must be built into voter registration, authentication, voting, counting, complaint handling, and auditing.

The 2024 official baseline shows both the scale of Indonesian elections and the practical challenges to be addressed before 2029. The permanent voter register contained 204,807,222 voters, while Bawaslu's published evaluation identified multiple voting-administration problems and a substantial volume of cases requiring classification or further handling. These data justify stronger preventive controls, but they do not establish that the 2024 national result was manipulated.

The V-DEIM responds by combining a Living Voter Registry, verified identity, privacy-preserving online voting, immutable audit trails, transparent tabulation, digital complaints, independent audits, and constitutional remedies. The central principle is that no actor should control the entire electoral data chain: the citizen's vote must remain secret, while the integrity of the system must be publicly verifiable. Indonesia should proceed through staged legal and technical pilots, not on the assumption that internet voting is automatically safer. The standards set by the Constitutional Court (LUBER-JURDIL and cumulative technological, financial, human-resource, software, and public-readiness conditions) should be treated as minimum requirements; if they are not met, a secure hybrid system should be used until independent certification confirms readiness.

Practical recommendations.

- Adopt a Pancasila-based digital electoral integrity statute and implementing regulations.
- Build a continuously verified voter registry linked to legally verified population events, with privacy safeguards.
- Develop secure electronic authentication without linking voter identity to ballot choice.
- Replace opaque emergency procedures with cryptographically controlled, auditable contingencies.
- Create one interoperable complaint-tracking layer across KPU, Bawaslu, law enforcement, and courts while preserving institutional jurisdiction.

- Require independent pre-election, live-election, and post-election cybersecurity and statistical audits.
- Publish machine-readable aggregate election data and correction logs without exposing personal or ballot-secrecy information.
- Use 2024 data as a risk baseline for 2029 and measure improvement with transparent indicators rather than political labels.

REFERENCES

- Badan Pengawas Pemilihan Umum. (2025). Kompilasi data penanganan pelanggaran Pemilu 2024. Satu Data Bawaslu.
- Badan Pengawas Pemilihan Umum. Bawaslu sampaikan evaluasi pengawasan Pemilu 2024 ke DPR.
- Constitutional Court of the Republic of Indonesia. (2010). Decision No. 147/PUU-VII/2009, 30 March 2010.
- Constitutional Court of the Republic of Indonesia. (2024). Decision No. 137/PUU-XXII/2024.
- Constitutional Court of the Republic of Indonesia. (2024). Decision No. 135/PUU-XXII/2024.
- Constitution of the Republic of Indonesia of 1945.
- Council of Europe. (2017). Recommendation CM/Rec(2017)5 on standards for e-voting.
- International IDEA. Resources on electoral integrity, digital technology, and election management.
- Komisi Pemilihan Umum. (2023). Decision No. 857 of 2023 concerning the national permanent voter register for the 2024 election.
- Komisi Pemilihan Umum. (2024). Official 2024 voter-register fact sheet.
- Nasution, M. Rekonstruksi sistem pemerintahan berlandaskan Pancasila dalam mewujudkan stabilitas nasional, kepastian hukum, dan kesejahteraan rakyat dalam bingkai UUD 1945. Unpublished manuscript.
- OSCE Office for Democratic Institutions and Human Rights. Election observation and assessment methodologies.
- Republic of Indonesia. (2016). Law No. 10 of 2016 concerning the election of governors, regents, and mayors, as amended.

Republic of Indonesia. (2017). Law No. 7 of 2017 concerning general elections, as amended.

Republic of Indonesia. (2022). Law No. 27 of 2022 concerning personal data protection.