JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 4, No. 3, November 2025, pp. 896 - 905
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/151

COBIT 5-Based Evaluation of Sidalih Operational Governance in East Java Election Commission

Dea Ayu Retnaningrum*[1], Dwi Rolliawati[2], Mujib Ridwan[3]
[1,2,3] Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Ampel Surabaya
Jl. Ir. H. Soekarno, No. 682, 60237, Kota Surabaya, Jawa Timur, Indonesia
e-mail: deaayuretna2206@gmail.com*[1]; dwi_roll@uinsa.ac.id[2]; mujibrw@uinsa.ac.id[3]

ARTICLE INFO

Article History:

Received: 11-09-2025
Revised: 04-10-2025
Accepted: 18-11-2025
Published: 30-11-2025

ABSTRACT

Digital voter management is critical for electoral integrity. The Komisi Pemilihan Umum (KPU) of East Java implements the Sidalih platform to manage voter data in an integrated, near-real-time manner. This study evaluates Sidalih's operational governance using the COBIT 5 framework, focusing on the DSS domain (DSS01: Manage Operations; DSS02: Manage Service Requests and Incidents; DSS05: Manage Security Services). A descriptive qualitative approach was employed, using an in-depth interview with one Sidalih operator at KPU East Java and document analysis of operational procedures and system logs collected during March–May 2025. Data were mapped to COBIT 5 indicators and scored on a 0–5 capability scale using narrative analysis; results were aggregated to determine domain capability levels and to conduct a gap analysis against a target level of 3 (Established Process). Findings indicate that Sidalih's operational governance currently averages at approximately Level 1, with noteworthy weaknesses in documentation, incident recording, and periodic security audits. The study provides prioritised recommendations, including formalising SOPs, implementing an incident ticketing system, scheduling periodic security assessments, and enhancing user training programs. These actions aim to close capability gaps and strengthen the reliability and security of voter data management. The study contributes a practical assessment model and an evidence-based roadmap for KPU organizational improvement.

Keywords: *Sidalih, COBIT 5, IT Governance, Operational Governance, Voter Data Management.*

Abstrak

Sistem pengelolaan data pemilih yang andal sangat krusial bagi kredibilitas pemilu. Komisi Pemilihan Umum Provinsi Jawa Timur menggunakan Sidalih sebagai platform utama untuk pemutakhiran dan pengelolaan data pemilih. Penelitian ini mengevaluasi tata kelola operasional Sidalih menggunakan framework COBIT 5 pada domain DSS (DSS01, DSS02, DSS05). Penelitian bersifat kualitatif deskriptif dengan wawancara mendalam kepada satu orang operator Sidalih KPU Provinsi Jawa Timur dan analisis dokumen operasional yang dikumpulkan pada periode Maret–Mei 2025. Data dipetakan ke indikator COBIT 5 dan diberi skor capability 0–5 berdasarkan analisis naratif untuk kemudian dihitung level kapabilitas dan gap terhadap tingkat target (level 3). Hasil menunjukkan kelemahan pada dokumentasi proses, pencatatan insiden, dan audit keamanan berkala. Rekomendasi prioritas meliputi penyusunan SOP operasional, implementasi sistem tiket insiden,

DOI: https://doi.org/10.51903/ckgywg80

p-ISSN : 2803-1507 e-ISSN : 2803-1531

pelaksanaan audit keamanan berkala, serta peningkatan pelatihan pengguna. Studi ini menyajikan model penilaian yang dapat dijadikan acuan bagi KPU untuk meningkatkan tata kelola operasional Sidalih.

Kata Kunci: *Sidalih, COBIT 5, Tata Kelola TI, Operasi, Manajemen Data Pemilih.*

1. PENDAHULUAN

Komisi Pemilihan Umum (KPU) Provinsi Jawa Timur menggunakan Sistem Informasi Data Pemilih (SIDALIH) sebagai platform digital utama untuk mengelola data pemilih secara terintegrasi dan real-time. SIDALIH dikembangkan untuk mengatasi permasalahan utama dalam pemutakhiran data pemilih, seperti duplikasi data, kesalahan input manual, dan keterlambatan pembaruan data. Melalui sistem ini, proses verifikasi dan sinkronisasi data pemilih dapat dilakukan dengan lebih efisien, meningkatkan akurasi dan transparansi dalam penyelenggaraan pemilu [1]. Sistem ini juga menyediakan jejak pembaruan data yang dapat ditelusuri sehingga setiap perubahan dapat dipertanggungjawabkan secara administratif.

Penggunaan SIDALIH tidak hanya berperan dalam operasional pengelolaan data, tetapi juga sebagai alat strategis dalam mendukung kualitas demokrasi yang tinggi di Indonesia. KPU Jawa Timur secara rutin melaksanakan rapat koordinasi dan pemutakhiran data pemilih berkelanjutan sebagai bentuk komitmen pemeliharaan kualitas data. Kegiatan ini memperkuat koordinasi antar lembaga dan jenjang administratif mulai dari desa hingga pusat sehingga data pemilih yang terintegrasi dapat menjaga validitas proses pemilu. Langkah-langkah ini menunjukkan adanya upaya konsisten dalam membangun mekanisme pengawasan data yang lebih stabil dan terstruktur.

Meski demikian, implementasi SIDALIH dalam pengelolaan data masih menghadapi sejumlah tantangan, di antaranya kendala teknis seperti gangguan server yang memengaruhi kestabilan sistem serta kompleksitas fitur yang terkadang membingungkan sebagian pengguna operasional [2]. Hal ini menandakan perlunya evaluasi mendalam terhadap tata kelola operasional sistem agar pengelolaan data pemilih tidak hanya akurat tapi juga efisien dan aman. Beberapa pengguna juga menghadapi keterbatasan pemahaman terkait prosedur pemanfaatan fitur tertentu yang memerlukan bimbingan teknis lebih lanjut. Kondisi tersebut menunjukkan bahwa peningkatan kapasitas sumber daya manusia menjadi faktor penting dalam optimalisasi sistem.

Transformasi digital dalam tata kelola pemilu sejalan dengan tren global yang menekankan pentingnya pemanfaatan teknologi informasi untuk memperkuat kepercayaan publik. Beberapa penelitian menekankan bahwa sistem informasi yang tidak dievaluasi secara berkala berpotensi menurunkan keandalan serta meningkatkan risiko kesalahan yang berdampak pada legitimasi hasil pemilu [3]. Oleh karena itu, evaluasi sistem berbasis kerangka kerja tata kelola TI sangat relevan untuk memastikan keberlanjutan dan keandalan SIDALIH. Evaluasi yang terstruktur juga memberikan pemahaman menyeluruh mengenai pola penggunaan sistem yang dapat mempengaruhi kualitas pengelolaan data.

Selain itu, evaluasi tata kelola operasional juga berperan penting dalam mendeteksi tingkat kapabilitas proses TI, termasuk keamanan, efisiensi, serta kepatuhan terhadap regulasi. Penelitian terdahulu menunjukkan bahwa tata kelola TI di sektor publik dapat ditingkatkan melalui kerangka kerja formal seperti COBIT untuk menyelaraskan tujuan strategis dengan implementasi teknologi [4]. Dengan demikian, pemanfaatan framework COBIT 5 diharapkan dapat memberikan gambaran objektif mengenai kekuatan maupun kelemahan SIDALIH di lingkungan KPU Jawa Timur. Pendekatan ini juga membantu organisasi dalam memetakan perbaikan yang perlu dilakukan sesuai prioritas dan tingkat urgensi.

Framework COBIT 5 dipilih sebagai kerangka kerja dalam evaluasi tata kelola SIDALIH karena kemampuannya untuk menyediakan panduan komprehensif dalam tata kelola dan manajemen teknologi informasi yang sesuai dengan standar internasional. COBIT 5 memungkinkan penilaian yang sistematis terhadap proses pengelolaan, kontrol keamanan, dan efektivitas penggunaan teknologi dalam mendukung tujuan organisasi seperti KPU Provinsi Jawa Timur [5]. Pendekatan tersebut juga memberikan struktur analitis yang memudahkan peneliti dalam menilai konsistensi penerapan kebijakan TI yang berlaku. Selain itu, kerangka ini mendukung identifikasi faktor-faktor yang mempengaruhi keberhasilan implementasi sistem informasi secara menyeluruh.

Evaluasi menggunakan *framework* ini penting untuk mengidentifikasi gap antara kondisi aktual dan praktik terbaik pengelolaan sistem informasi, sehingga dapat memberikan rekomendasi strategis dan operasional dalam meningkatkan kinerja SIDALIH dalam jangka panjang. Proses identifikasi tersebut juga membantu memahami sejauh mana sistem telah memenuhi standar yang ditetapkan dalam tata kelola TI. Analisis ini

p-ISSN : 2803-1507 e-ISSN : 2803-1531

memberikan wawasan mengenai area yang memerlukan perbaikan untuk meningkatkan efektivitas sistem. Pendekatan tersebut sekaligus membuka peluang penerapan kebijakan yang lebih tepat dalam mendukung keberhasilan sistem informasi.

2. TINJAUAN PUSTAKA

Penelitian mengenai tata kelola teknologi informasi telah banyak memanfaatkan *framework* COBIT 5 sebagai acuan evaluasi dalam menilai keselarasan antara proses TI dan tujuan organisasi. [6] menunjukkan bahwa COBIT 5 efektif digunakan untuk mengukur tingkat *capability level* proses dan mendukung penciptaan nilai bisnis melalui praktik tata kelola yang terkontrol. [7], [8] menjelaskan bahwa *framework* ini dapat diterapkan pada organisasi besar maupun sektor publik karena menyediakan struktur evaluasi yang konsisten. [9] menguraikan bagaimana COBIT 5 digunakan dalam pengelolaan layanan digital untuk meningkatkan kualitas pengawasan dan ketepatan proses bisnis. [10], [11], [12] menjelaskan pemanfaatan COBIT 5 dalam memperkuat mekanisme kontrol dan akuntabilabilitas pada sistem informasi sektor publik.

Evaluasi terhadap tata kelola TI menggunakan COBIT 5 juga banyak dilakukan pada institusi yang berupaya meningkatkan kualitas proses operasionalnya. [13] menunjukkan bahwa COBIT 5 menyediakan struktur pengendalian risiko yang mendukung peningkatan kualitas layanan TI. [14] menjelaskan bahwa pendekatan *holistic* COBIT 5 memudahkan integrasi berbagai standar dan prosedur TI sehingga menghasilkan konsistensi pengendalian internal. [15], [16] menguraikan bagaimana organisasi publik menggunakan COBIT 5 untuk memperkuat proses pengawasan internal dan memastikan keselarasan kegiatan TI dengan kebutuhan organisasi. Temuan-temuan tersebut menunjukkan keberagaman implementasi COBIT 5 dalam evaluasi tata kelola TI pada berbagai jenis institusi.

Kajian terhadap domain COBIT 5 turut menjadi fokus sejumlah penelitian terdahulu. [17], [18] menunjukkan keterkaitan antara penguatan implementasi domain Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Deliver, Service and Support (DSS), serta Monitor, Evaluate and Assess (MEA) dengan stabilitas kinerja layanan TI. [19], [20] menguraikan peran domain APO dan BAI dalam mendukung perencanaan strategis serta peningkatan mutu layanan secara berkelanjutan. Kajian mengenai *capability level* seperti dijelaskan oleh [21], [22] memaparkan fungsi model kapabilitas dalam memetakan tingkat kematangan proses organisasi. [23], [24], [25] menampilkan bagaimana *capability level* mendukung proses pengembangan berkelanjutan pada institusi publik maupun swasta. Bagian ini memberikan landasan kontekstual bagi penempatan tabel *capability level* sebagaimana ditampilkan pada Tabel 1.

Tabel 1. Capability Level

Tingkat Level	Penjelasan Tingkat Level
Level 0 (Incomplete Process)	Tidak ada proses yang terdefisini, namun proses dilakukan.
Level 1 (Performed Process)	Proses dilakukan, tetapi belum terdokumentasi.
Level 2 (Managed Process)	Proses terdokumentasi dan dikelola secara terpusat.
Level 3 (Established Process)	Proses sudah di standarisasi.
Level 4 (Predictable Process)	Proses terukur secara kuantitatif.
Level 5 (Optimized Process)	Proses dioptimalkan untuk inovasi dan etisiensi maksimal.

Dalam konteks layanan publik, berbagai penelitian telah mengevaluasi penerapan COBIT 5 pada sistem informasi pemerintahan. [1] melakukan analisis terhadap efektivitas penggunaan COBIT 5 pada SIDALIH untuk pengelolaan data pemilih, menunjukkan pentingnya struktur tata kelola TI dalam menjaga akurasi dan integritas data pada penyelenggaraan pemilu. [26], [27] menjelaskan bahwa sistem informasi kepemiluan memerlukan pengendalian yang selaras dengan prinsip COBIT 5 untuk memastikan konsistensi, keandalan, dan transparansi pengelolaan data. [28] menguraikan penerapan kerangka COBIT 5 dalam memperkuat manajemen data kritis pada layanan publik digital, sehingga menunjukkan relevansi kerangka ini dalam evaluasi sistem informasi pemerintahan.

Rangkaian penelitian terdahulu tersebut membentuk dasar penting bagi penelitian ini dalam mengevaluasi tata kelola operasional SIDALIH. Kajian empiris yang membahas penerapan *framework* COBIT 5 menunjukkan bagaimana kerangka tersebut digunakan untuk menilai kelemahan proses, memetakan tingkat kematangan, dan memperkuat tata kelola TI pada berbagai institusi publik. Temuan tersebut menjelaskan bahwa COBIT 5 memiliki karakteristik evaluatif yang relevan untuk menilai kualitas pengendalian TI pada sistem informasi yang bersifat kritis dan berskala nasional. Dengan landasan tersebut, penelitian ini memusatkan perhatian pada penerapan COBIT 5 untuk mengevaluasi tata kelola SIDALIH di KPU Provinsi Jawa Timur dengan fokus pada efektivitas, kepatuhan, dan keselarasan proses TI dengan kebutuhan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

operasional lembaga. Pendekatan ini memberikan kerangka analitis yang memungkinkan identifikasi aspek-aspek yang perlu diperbaiki dalam pengelolaan sistem informasi pemilu.

3. METODOLOGI PENELITIAN

3.1. *Pendekatan Penelitian*

Penelitian ini menggunakan pendekatan kualitatif deskriptif, yang bertujuan untuk memberikan gambaran mendalam terkait tata kelola operasional dan penggunaan Sidalih di KPU Provinsi Jawa Timur. Pendekatan kualitatif dipilih karena mampu mengeksplorasi fenomena sosial secara kontekstual melalui wawancara dan analisis dokumen [18]. Pendekatan ini dipilih karena sesuai untuk menggali secara mendalam fenomena tata kelola operasional Sidalih di KPU Provinsi Jawa Timur. Metode kualitatif memungkinkan peneliti untuk memahami pengalaman, praktik, dan kendala yang dialami oleh operator secara kontekstual. Sementara itu, sifat deskriptif digunakan untuk menggambarkan kondisi nyata tanpa melakukan manipulasi terhadap variabel yang diteliti. Dengan demikian, hasil penelitian diharapkan dapat memberikan gambaran yang lebih komprehensif mengenai implementasi tata kelola TI berdasarkan kerangka COBIT 5.

3.2. *Lokasi, Waktu, dan Responden Penelitian*

Penelitian dilaksanakan di KPU Provinsi Jawa Timur selama periode Maret hingga Mei 2025. Responden penelitian adalah satu orang operator Sidalih yang dipilih dengan teknik purposive sampling, karena informan ini memiliki keterlibatan langsung dalam pengoperasian, pemeliharaan, dan penanganan insiden Sidalih. Pemilihan responden tunggal dilakukan dengan pertimbangan bahwa operator tersebut merupakan sumber informasi paling relevan dan memahami operasional Sidalih secara menyeluruh. Operator tersebut juga memiliki akses terhadap berbagai aktivitas teknis yang memungkinkan peneliti memahami proses kerja sistem secara lebih rinci.

3.3. *Teknik Pengumpulan Data*

Data penelitian diperoleh melalui wawancara mendalam dan analisis dokumen. Wawancara dilakukan berdasarkan pedoman yang disusun dengan mengacu pada indikator COBIT 5 pada domain DSS01 (Manage Operations), DSS02 (Manage Service Requests and Incidents), dan DSS05 (Manage Security Services). Proses wawancara direkam dengan persetujuan responden, kemudian ditranskrip untuk memudahkan analisis. Selain itu, peneliti mengumpulkan dokumen pendukung berupa SOP, catatan insiden, log sistem, serta laporan monitoring terkait operasional Sidalih. Untuk meningkatkan validitas hasil, penelitian ini juga menerapkan triangulasi data, yaitu dengan melakukan observasi langsung terhadap aktivitas operator SIDALIH selama proses pembaruan data pemilih serta pemeriksaan dokumen pendukung dari Divisi Data dan Informasi KPU Provinsi Jawa Timur. Langkah ini dilakukan untuk memverifikasi kesesuaian antara hasil wawancara, dokumen operasional, dan praktik di lapangan.

3.4. *Teknik Analisis Data*

Analisis data dilakukan secara naratif. Transkrip wawancara dan dokumen pendukung dibaca berulang, kemudian dilakukan koding untuk menemukan tema-tema utama yang berkaitan dengan operasional Sidalih. Temuan selanjutnya dipetakan ke dalam indikator COBIT 5 pada domain DSS, lalu diberikan skor capability level dalam rentang 0–5. Skor tiap indikator digabungkan untuk menghasilkan level kapabilitas subdomain dan domain, yang kemudian dibandingkan dengan level target (Level 3 – Established Process) yang diperoleh dari hasil observasi dan wawancara untuk mengetahui gap.

4. HASIL DAN PEMBAHASAN

4.1. *Hasil Penilaian Domain DSS01 (Manage Operations)*

Berdasarkan hasil pemetaan terhadap indikator COBIT 5, diperoleh capaian *capability level* pada tiga domain yang dianalisis, yaitu DSS01, DSS02, dan DSS05. Proses penilaian dilakukan untuk memberikan gambaran yang lebih jelas mengenai kondisi pengelolaan operasional berdasarkan indikator yang relevan. Analisis ini membantu menguraikan hubungan antara masing-masing domain dengan praktik operasional yang diterapkan dalam sistem. Hasil analisis ditampilkan pada Tabel 2.

Hasil menunjukkan bahwa pengelolaan operasional Sidalih masih berada pada **Level 1**, artinya proses sudah ada tetapi belum terdokumentasi dan belum dijalankan secara konsisten. Hal ini terlihat dari ketiadaan SOP yang baku untuk prosedur operasional dan perubahan sistem (DSS01.01 dan DSS01.02), serta tidak adanya

p-ISSN : 2803-1507 e-ISSN : 2803-1531

mekanisme yang jelas untuk pengelolaan kapasitas (DSS01.04). Konfigurasi sistem (DSS01.03) relatif lebih baik karena terdapat upaya pencatatan, meskipun masih terbatas. Ketiadaan pelatihan formal bagi operator (DSS01.05) juga menjadi penyebab rendahnya nilai. Kondisi ini menunjukkan bahwa operasi Sidalih sangat bergantung pada pengalaman individu, bukan prosedur organisasi. Jika dibandingkan dengan penelitian [2] mengenai Sidalih di KPU Kota Malang, temuan serupa juga muncul, di mana dokumentasi operasional menjadi titik lemah utama [7].

Tabel 2. Hasil Evaluasi Capability Level dan Gap DSS01

Sub Domain	Capability Level	Target Level	Gap
DSS01.01	1	3	2
DSS01.02	1	3	2
DSS01.03	2	3	1
DSS01.04	0	3	3
DSS01.05	0	3	3

4.2. *Hasil Penilaian Domain DSS02 (Manage Service Requests and Incidents)*

Domain DSS02 dianalisis untuk memahami bagaimana organisasi menangani permintaan layanan dan insiden yang muncul selama operasional sistem berlangsung. Setiap sub-domain dinilai berdasarkan kejelasan prosedur, ketepatan penanganan, serta konsistensi dokumentasi yang digunakan dalam aktivitas operasional. Analisis ini memberikan pemahaman mengenai efektivitas proses penanganan insiden serta kesiapan organisasi dalam mengelola gangguan layanan. Hasil pengukuran juga membantu mengidentifikasi area yang masih memerlukan peningkatan terutama terkait standarisasi mekanisme pelaporan. Ringkasan hasil evaluasi disajikan pada Tabel 3

Tabel 3. Hasil Evaluasi Capability Level dan Gap DSS02

Sub Domain	Capability Level	Target Level	Gap
DSS02.01	0	3	3
DSS02.02	1	3	2
DSS02.03	1	3	2
DSS02.04	1	3	2
DSS02.05	1	3	2
DSS02.06	0	3	3
DSS02.07	0	3	3

Penilaian domain DSS02 menunjukkan level kapabilitas **1 (Performed Process)**. Artinya penanganan insiden dan permintaan layanan masih bersifat ad-hoc, tidak terstruktur, dan sangat bergantung pada pengalaman operator. Proses pencatatan insiden dilakukan secara manual tanpa klasifikasi atau skema prioritas (DSS02.01 dan DSS02.02), sehingga laporan insiden tidak terdokumentasi dengan baik. Penanganan insiden seperti investigasi dan pemulihan (DSS02.04 dan DSS02.05) dilakukan secara reaktif, tanpa adanya SLA (Service Level Agreement) atau sistem tiket. Kondisi ini menyebabkan KPU kesulitan melakukan analisis tren insiden maupun menyiapkan perbaikan preventif. Hal ini sejalan dengan temuan [3] dalam evaluasi COBIT 5 di STMIK Mikroskil, di mana manajemen insiden menjadi salah satu tantangan utama organisasi publik karena ketiadaan sistem pelaporan formal.

4.3. *Hasil Penilaian Domain DSS05 (Manage Security Services)*

Evaluasi terhadap domain DSS05 dilakukan untuk menilai pengelolaan layanan keamanan yang diterapkan dalam operasional sistem. Setiap sub-domain dianalisis untuk melihat sejauh mana kontrol keamanan telah direncanakan, dilaksanakan, dan dipantau secara konsisten. Proses evaluasi ini penting untuk memahami kesiapan organisasi dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Data hasil penilaian memberikan gambaran tentang area keamanan yang sudah berjalan baik maupun yang memerlukan perbaikan lanjutan. Ringkasan hasil pengukuran tersebut disajikan pada Tabel 4.

Hasil evaluasi pada domain DSS05 menunjukkan rata-rata berada di **Level 2 (Managed Process)**. Hal ini menandakan bahwa layanan keamanan Sidalih sudah memiliki dokumentasi dasar dan beberapa proses berjalan secara konsisten, terutama pada perlindungan malware (DSS05.01) serta keamanan jaringan (DSS05.02). Namun, kelemahan signifikan terlihat pada pengelolaan akses pengguna (DSS05.04) dan kontrol fisik terhadap aset TI (DSS05.05). Pemantauan infrastruktur keamanan (DSS05.07) juga belum dilakukan secara rutin, sehingga potensi serangan tidak dapat terdeteksi lebih awal. Dibandingkan dengan penelitian [5] yang menilai manajemen risiko TI di KPU menggunakan COBIT 5, hasil ini menunjukkan pola

p-ISSN : 2803-1507 e-ISSN : 2803-1531

serupa: aspek keamanan sudah mulai diperhatikan, namun belum didukung dengan audit rutin dan pemantauan terintegrasi.

Tabel 4. Hasil Evaluasi Capability Level dan Gap DSS05

Sub Domain	Capability Level	Target Level	Gap
DSS05.01	2	3	1
DSS05.02	2	3	1
DSS05.03	2	3	1
DSS05.04	1	3	2
DSS05.05	1	3	2
DSS05.06	2	3	1
DSS05.07	1	3	2

4.4. *Analisis Agregat Domain DSS*

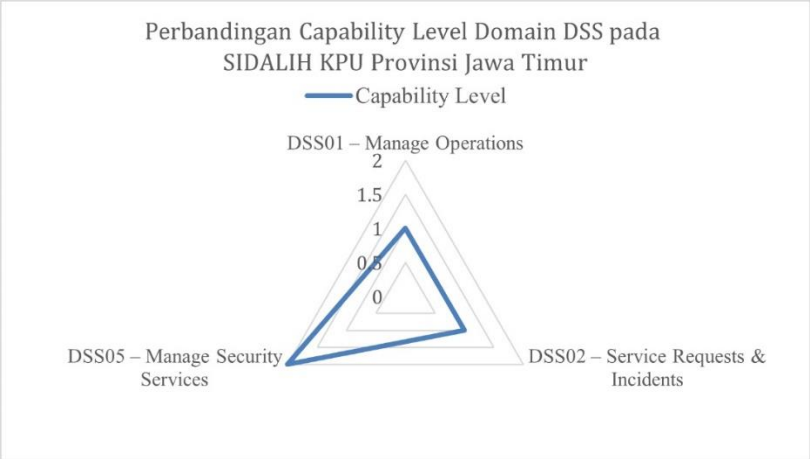
Secara keseluruhan, rata-rata kapabilitas domain DSS menunjukkan bahwa DSS01 berada pada nilai 0,8 (Level 1), DSS02 pada nilai 0,57 (Level 1), dan DSS05 pada nilai 1,57 (Level 2). Jika dirata-ratakan, kapabilitas keseluruhan adalah 0,98 yang setara dengan Level 1 (Performed Process). Temuan ini mengindikasikan bahwa tata kelola operasional Sidalih di KPU Provinsi Jawa Timur masih berada pada tahap awal, di mana proses telah berjalan tetapi belum terdokumentasi secara konsisten dan belum memiliki mekanisme pengendalian yang memadai. Kondisi ini menimbulkan gap yang cukup besar terhadap target Level 3 (Established Process). Rendahnya nilai DSS01 dan DSS02 menegaskan pentingnya penyusunan SOP operasional serta penerapan sistem pencatatan insiden yang lebih terstruktur. Sementara itu, DSS05 relatif lebih baik karena sudah terdapat kesadaran akan pentingnya aspek keamanan, meskipun masih perlu diperkuat dengan audit berkala, pemantauan log, serta kebijakan akses yang lebih ketat. Jika kesenjangan ini tidak segera ditutup, terdapat risiko serius terhadap keandalan data pemilih maupun keamanan sistem, yang pada akhirnya dapat memengaruhi kredibilitas pemilu.

Jika dibandingkan dengan penelitian sejenis di lembaga lain, hasil penelitian ini menunjukkan pola yang relatif serupa. Penelitian oleh [2] di KPU Kota Malang di KPU Kota Manado sama-sama menemukan bahwa aspek dokumentasi dan mekanisme penanganan insiden merupakan titik lemah utama dalam tata kelola operasional sistem pemilu. Sementara itu, [5] yang meneliti manajemen risiko TI di KPU pusat juga mencatat perlunya audit keamanan dan prosedur standar yang lebih kuat. Hal ini menunjukkan bahwa permasalahan tata kelola operasional Sidalih bersifat umum di berbagai wilayah, sehingga hasil penelitian ini dapat memperkuat dasar generalisasi terhadap kondisi tata kelola TI di lingkungan KPU secara nasional.

Secara keseluruhan, rata-rata kapabilitas domain DSS menunjukkan bahwa DSS01 berada pada nilai 0,8 (Level 1), DSS02 pada nilai 0,57 (Level 1), dan DSS05 pada nilai 1,57 (Level 2). Jika dirata-ratakan, kapabilitas keseluruhan adalah 0,98 yang setara dengan Level 1 (Performed Process). Temuan ini mengindikasikan bahwa tata kelola operasional Sidalih di KPU Provinsi Jawa Timur masih berada pada tahap awal, di mana proses telah berjalan tetapi belum terdokumentasi secara konsisten dan belum memiliki mekanisme pengendalian yang memadai. Kondisi ini menimbulkan gap yang cukup besar terhadap target Level 3 (Established Process). Rendahnya nilai DSS01 dan DSS02 menegaskan pentingnya penyusunan SOP operasional serta penerapan sistem pencatatan insiden yang lebih terstruktur. Sementara itu, DSS05 relatif lebih baik karena sudah terdapat kesadaran akan pentingnya aspek keamanan, meskipun masih perlu diperkuat dengan audit berkala, pemantauan log, serta kebijakan akses yang lebih ketat. Jika kesenjangan ini tidak segera ditutup, terdapat risiko serius terhadap keandalan data pemilih maupun keamanan sistem, yang pada akhirnya dapat memengaruhi kredibilitas pemilu.

Jika dibandingkan dengan penelitian sejenis di lembaga lain, hasil penelitian ini menunjukkan pola yang relatif serupa. Penelitian oleh [2] di KPU Kota Malang di KPU Kota Manado sama-sama menemukan bahwa aspek dokumentasi dan mekanisme penanganan insiden merupakan titik lemah utama dalam tata kelola operasional sistem pemilu. Sementara itu, [5] yang meneliti manajemen risiko TI di KPU pusat juga mencatat perlunya audit keamanan dan prosedur standar yang lebih kuat. Hal ini menunjukkan bahwa permasalahan tata kelola operasional Sidalih bersifat umum di berbagai wilayah, sehingga hasil penelitian ini dapat memperkuat dasar generalisasi terhadap kondisi tata kelola TI di lingkungan KPU secara nasional. Perbandingan capaian setiap domain tersebut divisualisasikan untuk memberikan gambaran yang lebih jelas mengenai perbedaan tingkat kapabilitas antarproses, seperti ditunjukkan pada Gambar 1.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 1. Perbandingan Capability Level Domain DSS pada SIDALIH KPU Provinsi Jawa Timur

4.5. *Rekomendasi*

Berdasarkan hasil analisis kapabilitas operasional Sidalih pada domain DSS, terdapat beberapa rekomendasi perbaikan yang dapat dilakukan oleh KPU Provinsi Jawa Timur untuk meningkatkan level kapabilitas hingga mencapai target level 3 (*Established Process*). Rekomendasi tersebut disusun berdasarkan posisi kapabilitas pada setiap sub-domain sehingga arah perbaikan dapat direncanakan secara lebih terfokus. Informasi ini juga membantu menggambarkan prioritas tindakan yang perlu dilakukan untuk memperbaiki kelemahan yang masih dominan pada proses operasional. Penyusunan rekomendasi ini dilakukan dengan mempertimbangkan kebutuhan organisasi dalam mencapai proses yang terdokumentasi dan terstandarisasi. Daftar rekomendasi tersebut disajikan pada Tabel 5.

Tabel 5. Rekomendasi pada Domain DSS01 (*Manage Operations*)

Rekomendasi
Menyusun dan mendokumentasikan **SOP operasional standar** terkait prosedur pengelolaan Sidalih, termasuk backup data, pemeliharaan sistem, dan perubahan konfigurasi.
Melaksanakan **pelatihan rutin** bagi operator untuk memastikan pemahaman dan penerapan SOP secara konsisten.
Mengembangkan sistem monitoring kapasitas dan ketersediaan layanan agar proses dapat diprediksi dan terukur.

Rekomendasi pada domain DSS02 disusun untuk memperbaiki proses penanganan permintaan layanan dan insiden yang selama ini masih dilakukan secara ad-hoc. Setiap rekomendasi diarahkan untuk memperkuat dokumentasi, alur kerja, serta mekanisme pelaporan agar proses menjadi lebih terstruktur. Informasi yang disusun dalam bagian ini juga memberikan gambaran mengenai kebutuhan organisasi dalam meningkatkan kecepatan respons dan konsistensi pengelolaan insiden. Penyusunan rekomendasi dilakukan dengan meninjau temuan utama pada setiap sub-domain sehingga arah perbaikan dapat dilakukan secara komprehensif. Rincian rekomendasi pada domain ini ditampilkan pada Tabel 6.

Tabel 6. Rekomendasi pada Domain DSS02 (*Manage Operations*)

Rekomendasi
Menggunakan form insiden standar (manual) untuk pencatatan permintaan layanan dan insiden, sehingga ada jejak dokumentasi minimal.
Mengimplementasikan **sistem helpdesk atau ticketing** (misalnya GLPI, OTRS, atau aplikasi serupa) untuk mengelola insiden secara terstruktur, termasuk klasifikasi, prioritas, dan SLA (Service Level Agreement).
Membangun **dashboard pelaporan insiden** terintegrasi yang memungkinkan analisis tren insiden serta evaluasi kinerja layanan.

Domain DSS05 memerlukan rekomendasi yang berfokus pada penguatan aspek keamanan, baik dari sisi kontrol akses, pengelolaan kerentanan, maupun pemantauan aktivitas sistem. Setiap rekomendasi yang disusun bertujuan mendukung penerapan perlindungan berlapis sehingga potensi risiko dapat dikurangi secara signifikan. Informasi ini juga memberikan penjelasan mengenai kebutuhan organisasi dalam memprioritaskan keamanan sebagai bagian dari operasional harian. Analisis temuan pada sub-domain membantu menentukan langkah teknis yang perlu dilakukan agar layanan keamanan berjalan lebih efektif. Rincian rekomendasi pada domain ini disajikan pada Tabel 7.

Tabel 7. Rekomendasi pada Domain DSS05 (Manage Operations)

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Rekomendasi
Menerapkan kebijakan **pengelolaan akses pengguna** berbasis peran (Role-Based Access Control/RBAC) serta memperketat kontrol fisik terhadap perangkat TI.
Melaksanakan **audit keamanan berkala** meliputi uji kerentanan (vulnerability assessment) dan manajemen patch.
Mengintegrasikan sistem pemantauan keamanan (SIEM/log management) untuk mendeteksi aktivitas anomali secara real-time dan mendukung continuous improvement.

4.6. *Rekomendasi Agregat Tata Kelola*

Secara umum, KPU Provinsi Jawa Timur perlu menetapkan kebijakan tata kelola operasional TI berbasis COBIT 5 secara formal agar seluruh proses pengelolaan Sidalih memiliki dasar hukum dan standar yang jelas. Selain itu, diperlukan pembentukan tim atau unit khusus IT Governance yang berfungsi mengawasi penerapan SOP, pelaksanaan audit keamanan, serta memastikan koordinasi lintas unit berjalan efektif. Untuk mendorong perbaikan yang berkelanjutan, KPU juga perlu menyusun rencana peningkatan kapabilitas secara bertahap, dimulai dari tahap dokumentasi proses (peningkatan dari Level 1 ke Level 2), kemudian standarisasi prosedur (Level 2 ke Level 3), hingga mencapai tahap pengukuran kuantitatif yang lebih matang (Level 4). Pendekatan bertahap ini diharapkan dapat membantu KPU memperkuat tata kelola operasional Sidalih sekaligus meningkatkan keandalan sistem dalam jangka panjang.

5. DISKUSI

Hasil penelitian menunjukkan bahwa tata kelola operasional Sidalih masih berada pada Level 1 untuk domain DSS01 dan DSS02 serta Level 2 untuk DSS05, yang berarti proses telah berjalan namun belum didukung dokumentasi dan mekanisme kontrol yang memadai. Kondisi ini sejalan dengan penjelasan pada [2] yang menegaskan bahwa pengelolaan Sidalih di KPU daerah lain juga menghadapi kendala serupa pada aspek dokumentasi dan prosedur kerja. Kelemahan pada pencatatan insiden dan ketiadaan SOP yang ditemui dalam penelitian ini memperkuat temuan sebelumnya bahwa proses operasional Sidalih masih sangat bergantung pada pengalaman individu, bukan pada sistem yang terdokumentasi. Interpretasi tersebut menjelaskan bahwa secara umum tata kelola operasional Sidalih belum mencapai standar *established process* sebagaimana dikonseptualisasikan dalam COBIT 5.

Apabila dibandingkan dengan penelitian lain, hasil penelitian ini memperkuat kajian pada [3] yang menunjukkan bahwa manajemen insiden di organisasi publik sering berjalan secara *ad-hoc* akibat minimnya sistem pelaporan formal. Temuan penelitian ini juga konsisten dengan pembahasan dalam [5] yang menyoroti rendahnya implementasi audit keamanan di lingkungan KPU sehingga pengendalian risiko belum optimal. Namun, capaian Level 2 pada beberapa aspek DSS05 memperlihatkan perbedaan positif dari pola yang ditunjukkan di [14], karena Sidalih di Jawa Timur telah memiliki dokumentasi dasar pada layanan keamanan meskipun belum sepenuhnya terintegrasi. Perbandingan ini menunjukkan bahwa sebagian temuan selaras dengan literatur, sementara aspek keamanan memberikan indikasi kemajuan yang tidak sepenuhnya dijelaskan oleh penelitian sebelumnya.

Meskipun sebagian besar hasil konsisten dengan ekspektasi, terdapat beberapa anomali yang muncul terutama pada aspek perlindungan keamanan yang memperoleh nilai relatif lebih tinggi dibandingkan domain lain. Fenomena ini berbeda dengan laporan pada [17] yang menyatakan bahwa domain keamanan biasanya menjadi area paling lemah dalam instansi publik, sehingga capaian Level 2 pada DSS05 mengindikasikan adanya langkah awal dalam penguatan kontrol. Variasi kecil pada nilai sub-domain juga menunjukkan bahwa beberapa praktik keamanan telah diterapkan secara rutin meskipun tanpa dokumentasi baku, sehingga menghasilkan performa yang tidak seragam antarproses. Temuan tersebut memperlihatkan bahwa adanya rutinitas *operational know-how* mampu menghasilkan capaian keamanan di atas domain operasional lainnya meskipun belum didukung struktur formal.

Secara teoretis, penelitian ini menegaskan relevansi framework COBIT 5 sebagai alat evaluasi untuk memetakan *gap* antara kondisi aktual dan standar tata kelola TI, sebagaimana dijelaskan dalam literatur [6] dan [7]. Kontribusi penelitian ini terletak pada pemetaan terperinci terhadap domain DSS yang menunjukkan area prioritas yang perlu diperbaiki, terutama dokumentasi proses, pencatatan insiden terstruktur, dan audit keamanan berkala. Dari sisi praktis, hasil penelitian memberikan dasar rekomendasi yang dapat digunakan KPU dalam membangun SOP operasional, sistem *ticketing* insiden, serta kebijakan keamanan yang lebih terukur. Namun, keterbatasan berupa keterlibatan hanya satu responden dan ketergantungan pada dokumen lokal membuat hasil penelitian ini perlu diuji ulang pada wilayah lain untuk memperkuat generalisasi.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

6. KESIMPULAN DAN SARAN

Dari sisi teoretis, penelitian ini memberikan kontribusi dalam bentuk pengembangan model adaptasi *framework COBIT 5* yang disesuaikan untuk konteks lembaga publik di Indonesia, khususnya pada sektor penyelenggara pemilu. Hasil evaluasi menghasilkan temuan empiris yang dapat dijadikan dasar dalam penyusunan kerangka kerja tata kelola TI berbasis *domain* DSS untuk instansi pemerintahan, sehingga tidak hanya memberikan manfaat praktis, tetapi juga memperkaya literatur mengenai penerapan *COBIT 5* di sektor publik. Temuan ini juga memberikan gambaran mengenai tantangan yang umum dihadapi lembaga publik dalam menerapkan tata kelola TI secara komprehensif. Dengan demikian, penelitian ini dapat menjadi rujukan bagi penelitian selanjutnya yang berfokus pada pengembangan tata kelola TI di sektor pemerintahan.

Berdasarkan hasil evaluasi menggunakan *framework COBIT 5* pada *domain Deliver, Service, and Support* (DSS), pengelolaan sistem SIDALIH di KPU Provinsi Jawa Timur menunjukkan bahwa implementasinya belum sepenuhnya sesuai dengan standar yang diharapkan. Dari pengukuran yang dilakukan, sebagian besar sub*domain* berada pada *level* 0 hingga 2, sedangkan target idealnya adalah *level* 3. Hal ini menandakan bahwa beberapa aspek, seperti proses operasional, pengelolaan permintaan layanan, dan layanan keamanan, masih memerlukan perbaikan terutama dalam hal penyusunan *SOP*, dokumentasi, *monitoring*, serta kontrol yang lebih memadai. Kondisi ini menunjukkan perlunya peningkatan kapasitas dan penguatan prosedur agar sistem dapat mendukung kebutuhan operasional secara lebih optimal.

Penerapan *framework COBIT 5* secara optimal pada *domain* DSS diharapkan dapat membantu KPU Provinsi Jawa Timur dalam meningkatkan efektivitas layanan operasional, memperkuat perlindungan data, dan mempercepat penanganan *insiden*. Rekomendasi yang telah disusun mencakup penyusunan prosedur operasional yang lebih rinci, pengelolaan *insiden* secara sistematis, serta penguatan kebijakan dan pengawasan keamanan jaringan maupun perangkat. Dengan penerapan langkah-langkah tersebut, diharapkan KPU Provinsi Jawa Timur dapat menutup kesenjangan antara kondisi saat ini dengan target yang diharapkan, mencapai *level* kapabilitas yang sesuai standar, dan mendukung tata kelola teknologi informasi yang lebih baik dan berkelanjutan. Penerapan rekomendasi ini juga diharapkan mampu meningkatkan keandalan sistem dan memastikan keberlanjutan operasional dalam jangka panjang.

DAFTAR PUSTAKA

[1] M. Handoko *et al.*, "Efektivitas Aplikasi Sistem Informasi Data Pemilih (Sidalih) terhadap Pengelolaan Data Pemilih Pilkada 2024 di Kecamatan Karangrejo," *J. Technol. Informatics Eng.*, vol. 4, no. 2, pp. 190–203, 2024, doi: 10.59966/jsph.v1i3.1428.

[2] M. Sugiarti and A. S. Ilmanada, "Analisis dan Evaluasi Sistem Informasi Data Pemilih (SIDALIH) dalam Pemilu tahun 2024 di KPU Kota Malang menggunakan Metode PIECES Framework," *Semin. Nas. Sist. Inf.*, vol. 8, pp. 5209–5220, 2024, [Online]. Available: https://jurnalfti.unmer.ac.id/index.php/senasif/article/view/613

[3] E. Elly and F. Halim, "Evaluasi Tatakelola Infrastruktur TI dengan Framework COBIT 5 (Studi Kasus: STMIK–STIE Mikroskil)," *Sebatik*, vol. 27, no. 2, pp. 74–82, 2018, doi: 10.46984/sebatik.v22i2.311.

[4] M. Sugiarti and A. S. Ilmananda, "Tata Kelola Teknologi Informasi pada Sektor Publik: Penyelarasan Teknologi Informasi dengan Visi Kepemimpinan (Studi Kasus: Kota Salatiga dan Kabupaten Bengkayang)," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 8, no. 6, pp. 1319–1330, 2021, doi: 10.25126/jtiik.202185379.

[5] M. A. Wirayudha, "Analysis of Information Technology Risk Management at KPU Using Cobit 5 Domain APO12 Analisis Manajemen Risiko Teknologi Informasi pada KPU Menggunakan Cobit 5 Domain APO12," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 4, no. 2, pp. 433–442, 2024, doi: 10.57152/malcom.v4i2.1225.

[6] S. J. Kuryanti, C. Adiwihardja, A. Suryadi, and D. A. Ambarsari, "Penerapan Framework COBIT Untuk Peningkatan Tata Kelola Teknologi Informasi," *J. Students' Res. Comput. Sci.*, vol. 4, no. 2, pp. 189–198, 2025, doi: 10.31599/zh4fy219.

[7] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, 1st ed. ISACA, 2012. [Online]. Available: https://www.isaca.org/resources/cobit

[8] H. N. R. Archaqie and P. Pratiwi, "Assessing IT Governance in Digital UMKM Application Projects:

p-ISSN : 2803-1507 e-ISSN : 2803-1531

A Comparative Study Using the COBIT 2019 Framework," *J. Ilm. Sist. Inf.*, vol. 4, no. 2, pp. 2803–1531, 2025, doi: 10.51903/wpt7q648.

[9] M. I. Sarwar, Q. Abbas, T. Alyas, A. Alzahrani, T. Alghamdi, and Y. Alsaawy, "Digital Transformation of Public Sector Governance With IT Service Management–A Pilot Study," *IEEE Access*, vol. 11, pp. 6490–6512, 2023, doi: 10.1109/access.2023.3237550.

[10] A. Sejati and S. I. Huda, "Evaluation and Audit of Academic Information Systems Based on COBIT 5 to Assess the Effectiveness of Information Technology Governance: A Case Study at Private Universities in Indonesia," *J. Ilm. Sist. Inf.*, vol. 4, no. 1, pp. 124–135, Mar. 2025, doi: 10.51903/h0q8tz79.

[11] A. Wardi and G. Aninditiyah, "The Impact of Regional Financial Accounting Systems, Public Transparency, and Control Activities on Financial Accountability in Local Governments," *J. Manag. Informatics*, vol. 3, no. 1, pp. 20–36, Dec. 2024, doi: 10.51903/jmi.v3i1.43.

[12] M. Handoko *et al.*, "The Architecture of Intellegent Transportation System based on Sensor Monitoring (Implementation in Jakarta Area)," *J. Technol. Informatics Eng.*, vol. 4, no. 2, pp. 190–203, May 2025, doi: 10.51903/jtie.v4i2.357.

[13] S. W. Hapsari, I. Aknuranda, and R. I. Rokhmawati, "Implementasi Tata Kelola Teknologi Informasi Berdasarkan Framework COBIT 5 Pada PT Krakatau Tirta Industri," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5726–5732, 2018, [Online]. Available: https://download.garuda.kemdikbud.go.id/article.php?article=872332&val=10384&title=Implementasi

[14] B. Gamaliel, Y. D. Y. Rindengan, and S. Karouw, "Pengukuran Tingkat Keselarasan Tata KelolaTeknologi Informasi Menggunakan FrameworkCOBIT 5 Pada Dinas KOMINFOKota Bitung," *J. Tek. Inform.*, vol. 11, no. 1, pp. 1–16, 2017, doi: 10.35793/jti.v11i1.16747.

[15] S. Alrahamneh, "Enhancing Internal Audit Quality in Jordanian Insurance Companies A Coso Framework Perspective," *EDPACS*, vol. 69, no. 6, pp. 1–27, Jun. 2024, doi: 10.1080/07366981.2024.2307068.

[16] O. H. Plant, J. van Hillegersberg, and A. Aldea, "Rethinking IT Governance: Designing a Framework for Mitigating Risk and Fostering Internal Control in a DevOps Environment," *Int. J. Account. Inf. Syst.*, vol. 45, p. 100560, 2022, doi: https://doi.org/10.1016/j.accinf.2022.100560.

[17] F. Imania and Q. H. Hidayah, "Pengukuran Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Domain Bai pada Fungsi Non -ERP Solution PT XYZ Measurement of Information Technology Governance Using the COBIT 5 Framework Domains Bai in Non-ERP Solution," *J. Sist. Inf. dan Bisnis Cerdas*, vol. 17, no. 2, pp. 1–10, 2024, doi: 10.33005/sibc.v17i2.283.

[18] C. Wibowo, T. Wijanarko, and A. Putra, "Utilizing phpMyAdmin for System Design in Enterprise Administration," *J. Technol. Informatics Eng.*, vol. 3, no. 2, pp. 217–234, 2024, doi: 10.51903/jtie.v3i2.193.

[19] S. M. U. Saleem, C. A. Taib, M. Ikram, and W. Mehmood, "A Comprehensive Analysis of Service Quality: A Systematic Literature Review," *Total Qual. Manag. Bus. Excell.*, vol. 35, no. 9–10, pp. 1124–1166, Jul. 2024, doi: 10.1080/14783363.2024.2357805.

[20] I. R. Saladdin and P. W. Handayani, "Information Technology Governance Implementation Challenges in Healthcare Facilities: A Systematic Literature Review," *Sage Open*, vol. 15, no. 4, p. 21582440251369320, Oct. 2025, doi: 10.1177/21582440251369322.

[21] T. Haryanti, N. A. Rakhmawati, and A. P. Subriadi, "The Extended Digital Maturity Model," 2023. doi: 10.3390/bdcc7010017.

[22] A. Aras and G. Büyüközkan, "Digital Transformation Journey Guidance: A Holistic Digital Maturity Model Based on a Systematic Literature Review," 2023. doi: 10.3390/systems11040213.

[23] S. Danladi, M. S. V Prasad, U. M. Modibbo, S. A. Ahmadi, and P. Ghasemi, "Attaining Sustainable Development Goals through Financial Inclusion: Exploring Collaborative Approaches to Fintech

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Adoption in Developing Economies," 2023. doi: 10.3390/su151713039.

[24] A. Androniceanu and O. M. Sabie, "Overview of Green Energy as a Real Strategic Option for Sustainable Development," 2022. doi: 10.3390/en15228573.

[25] F. Caputo, P. Magliocca, R. Canestrino, and E. Rescigno, "Rethinking the Role of Technology for Citizens' Engagement and Sustainable Development in Smart Cities," 2023. doi: 10.3390/su151310400.

[26] KPU, "Laporan Kinerja KPU Tahun 2019," 2019. [Online]. Available: https://www.kpu.go.id/koleksigambar/LAPKIN_KPU_2019_compressed.pdf

[27] K. Naseer and H. N. Ahmed, "Effectiveness and Reliability of Artificial Intelligence in Fraud Detection: A Mixed-Method Study on Financial Audit," *J. Manag. Informatics*, vol. 4, no. 1, pp. 706–722, 2025, doi: 10.51903/jmi.v4i1.168.

[28] M. Umbet, D. Askarov, K. Rudžionienė, Č. Christauskas, and L. Alikulova, "Evaluating the Implementation of Information Technology Audit Systems Within Tax Administration: A Risk Governance Perspective for Enhancing Digital Fiscal Integrity," *J. Risk Financ. Manag.*, vol. 18, no. 8, p. 422, Aug. 2025, doi: 10.3390/jrfm18080422.