TATA KELOLA KOTA CERDAS: PENILAIAN KEMATANGAN KEAMANAN SIBER NIST CSF 2.0 TERHADAP INFRASTRUKTUR LAYANAN PUBLIK KOTA CERDAS JAKARTA

Daffa Aryasatya Pratama
NPP. 33.0353
Program Studi Teknologi Rekayasa Informasi Pemerintahan
Email: daffaryasatya28@gmail.com

Pembimbing Skripsi: Mohammad Rezza Fahlevvi, S.Kom., M.Cs
Email: rezza@ipdn.ac.id

ABSTRACT

Problem Statement: *Cybersecurity vulnerabilities in Jakarta's digital governance have manifested through a series of incidents that undermine public trust in government digital services, while digital transformation demands increasingly robust security frameworks.* ***Purpose:*** *This study aims to assess the cybersecurity maturity level of Jakarta Smart City based on the NIST Cybersecurity Framework (CSF) 2.0 and to examine its implications for advancing the Sustainable Development Goals (SDGs), particularly SDG 16.* ***Method:*** *This study employs a descriptive qualitative approach with data collected through observation, in-depth interviews, and documentary analysis conducted at the Department of Communication, Information, and Statistics of DKI Jakarta Province between December 2025 and January 2026. Analysis was carried out across the six core functions of NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover.* ***Result:*** *The findings reveal that Jakarta Smart City has attained a Tier 3 (Repeatable) maturity level with an average CMMI score of 3.13, characterised by formal information security policies, risk management practices, IAM-based access controls, continuous incident monitoring, and consistently implemented response and recovery procedures. The Protect function recorded the highest score (3.60), while challenges persist in cross-system integration, human resource capacity development, and external collaboration.* ***Conclusion:*** *Advances in cybersecurity maturity contribute significantly to the reliability of digital public services and public trust, supporting sustainable Smart City governance in alignment with SDG 16, SDG 9, and SDG 11 targets.*

Keywords: *Cybersecurity; Jakarta Smart City; Maturity Assessment; NIST CSF 2.0; SDGs; Smart City*

ABSTRAK

Permasalahan: Kerentanan keamanan siber pada penyelenggaraan pemerintahan di Jakarta termanifestasi dalam serangkaian insiden yang mengancam kepercayaan publik terhadap layanan digital pemerintah, sementara transformasi digital menuntut kerangka keamanan yang semakin kuat. **Tujuan:** Penelitian ini bertujuan mengetahui tingkat kematangan keamanan siber Jakarta Smart City berdasarkan kerangka kerja NIST Cybersecurity Framework (CSF) 2.0 serta implikasinya dalam mendukung pencapaian Sustainable Development Goals (SDGs), khususnya SDG 16. **Metode:** Penelitian menggunakan pendekatan kualitatif deskriptif dengan teknik pengumpulan data melalui observasi, wawancara mendalam, dan studi dokumentasi yang dilaksanakan di Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta pada

Desember 2025 hingga Januari 2026. Analisis dilakukan terhadap enam fungsi inti NIST CSF 2.0 yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. **Hasil/Temuan:** Penelitian menunjukkan bahwa Jakarta Smart City berada pada Tier 3 (Repeatable) dengan nilai rata-rata CMMI sebesar 3,13. Fungsi Protect mencatat skor tertinggi (3,60) yang mencerminkan perlindungan sistem berlapis melalui autentikasi multi-faktor dan pengelolaan identitas yang kuat, sementara tantangan masih ada pada integrasi lintas sistem, pengembangan kapasitas SDM, dan penguatan kolaborasi eksternal. **Kesimpulan:** Peningkatan kematangan keamanan siber berkontribusi signifikan terhadap keandalan layanan publik digital dan kepercayaan publik, mendukung tata kelola Smart City yang berkelanjutan sesuai target SDG 16, SDG 9, dan SDG 11.

Kata kunci: Jakarta Smart City; Keamanan Siber; NIST CSF 2.0; Penilaian Kematangan; SDGs; Smart City

I. PENDAHULUAN

1.1. Latar Belakang

Transformasi digital mendorong pemerintah daerah mengembangkan ekosistem Smart City sebagai upaya meningkatkan efisiensi layanan publik dan akuntabilitas institusi. Jakarta sebagai ibu kota negara dan pusat pemerintahan Indonesia telah mengembangkan Jakarta Smart City (JSC) sebagai inisiatif tata kelola digital yang komprehensif. Namun, semakin luasnya ketergantungan pada infrastruktur digital juga membuka celah kerentanan keamanan siber yang berpotensi mengancam keberlangsungan layanan publik dan kepercayaan masyarakat.

Kerentanan keamanan siber pada penyelenggaraan pemerintahan di Jakarta secara nyata telah termanifestasi dalam serangkaian insiden yang mengancam kepercayaan publik terhadap layanan digital pemerintah. Insiden-insiden tersebut memperkuat urgensi penilaian kematangan keamanan siber secara sistematis dan berbasis kerangka kerja internasional yang diakui.

NIST Cybersecurity Framework (CSF) 2.0 merupakan kerangka kerja yang diterbitkan oleh National Institute of Standards and Technology pada tahun 2024, yang menyediakan panduan komprehensif bagi organisasi dalam mengelola risiko keamanan siber melalui enam fungsi inti: Govern, Identify, Protect, Detect, Respond, dan Recover. Kerangka ini telah banyak digunakan dalam konteks pemerintahan digital termasuk smart city di berbagai negara.

1.2. Kesenjangan Masalah yang Diambil (Research Gap)

Meskipun berbagai penelitian telah membahas implementasi keamanan siber di organisasi pemerintah, masih terdapat keterbatasan penelitian yang secara khusus mengkaji penilaian kematangan keamanan siber infrastruktur layanan publik smart city di Indonesia menggunakan NIST CSF 2.0 yang diperbarui. Penelitian yang ada umumnya menggunakan NIST CSF versi 1.1 atau kerangka kerja lain seperti ISO/IEC 27001 dan COBIT, sehingga penilaian menggunakan NIST CSF 2.0 terhadap ekosistem smart city pemerintah daerah di Indonesia masih sangat terbatas.

Selain itu, belum banyak penelitian yang mengkaitkan secara eksplisit antara tingkat kematangan keamanan siber suatu smart city dengan kontribusinya terhadap pencapaian Sustainable Development Goals (SDGs), khususnya SDG 16 tentang institusi yang kuat, transparan, dan akuntabel dalam konteks tata kelola pemerintahan digital Indonesia.

1.3. Urgensi Penelitian

Penelitian ini penting mengingat Jakarta Smart City mengelola data jutaan warga DKI Jakarta melalui berbagai platform digital termasuk aplikasi JAKI, sistem layanan terpadu, dan

infrastruktur kota cerdas lainnya. Ketidakmampuan dalam mengelola risiko keamanan siber secara matang dapat berdampak pada kebocoran data warga, gangguan layanan publik, dan erosi kepercayaan publik terhadap pemerintah digital. Apabila penelitian ini tidak dilaksanakan, pemangku kebijakan tidak akan memiliki dasar empiris yang kuat untuk merancang roadmap peningkatan keamanan siber yang tepat sasaran dan selaras dengan standar internasional.

1.4. Penelitian Terdahulu

Penelitian ini terinspirasi oleh beberapa penelitian terdahulu yang relevan. Ibrahim et al. (2018) melakukan tinjauan keamanan pemerintah lokal menggunakan NIST CSF dan menemukan bahwa sebagian besar pemerintah daerah berada pada tier yang rendah dalam pengelolaan risiko siber. Sulistyowati et al. (2020) melakukan analisis komparatif metodologi penilaian kematangan keamanan siber menggunakan NIST CSF, COBIT, ISO/IEC 27002, dan PCI DSS. Hossain et al. (2024) menyajikan tinjauan sistematis lanskap keamanan siber pemerintah daerah dan mengembangkan kerangka konseptual yang relevan. Andrade et al. (2020) mengkaji keamanan siber IoT pada smart city secara komprehensif. Bernardo et al. (2025) mengembangkan kerangka evaluasi kematangan keamanan siber yang selaras dengan NIST CSF. Irawan et al. (2024) merancang kerangka penilaian kematangan keamanan siber menggunakan NIST CSF v1.1 dan CIS Controls V8. Bibri dan Krogstie (2020) mengkaji solusi smart city berbasis data untuk keberlanjutan di London dan Barcelona.

1.5. Pernyataan Kebaruan Ilmiah

Penelitian ini merupakan penelitian baru yang berbeda dari penelitian sebelumnya dilihat dari: (1) penggunaan NIST CSF 2.0 (versi terbaru yang dirilis tahun 2024) untuk penilaian kematangan keamanan siber, bukan versi 1.1 yang digunakan mayoritas penelitian sebelumnya; (2) objek penelitian berupa infrastruktur smart city pemerintah daerah di Indonesia, khususnya Jakarta Smart City yang memiliki karakteristik unik sebagai kota dengan ekosistem digital terbesar di Indonesia; (3) keterkaitan eksplisit antara tingkat kematangan keamanan siber dengan pencapaian SDGs melalui rantai hubungan kausal yang terstruktur.

1.6. Tujuan

Penelitian ini bertujuan untuk menganalisis dan mendeskripsikan tingkat kematangan keamanan siber Jakarta Smart City berdasarkan kerangka kerja NIST Cybersecurity Framework (CSF) 2.0 serta mengkaji implikasinya dalam mendukung pencapaian Sustainable Development Goals (SDGs).

II. METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang dipilih karena kebutuhan untuk memahami secara mendalam kondisi, proses, dan praktik keamanan siber Jakarta Smart City yang tidak dapat sepenuhnya dijelaskan melalui data kuantitatif semata. Pendekatan kualitatif memungkinkan peneliti menggali pemahaman kontekstual yang kaya tentang implementasi NIST CSF 2.0 di lingkungan smart city pemerintah daerah.

Pengumpulan data dilakukan melalui tiga teknik yang saling melengkapi. Observasi lapangan dilakukan untuk mengamati secara langsung kondisi infrastruktur, prosedur operasional, dan praktik keamanan siber JSC. Wawancara mendalam dilakukan terhadap dua informan kunci, yaitu Kepala Jakarta Smart City dan Security Engineer Jakarta Smart City, yang dipilih secara purposive berdasarkan peran dan pengetahuan mereka tentang sistem keamanan siber JSC. Kepala Jakarta Smart City dipilih sebagai informan kunci pertama karena memegang otoritas tertinggi dalam pengambilan keputusan strategis terkait kebijakan dan tata kelola keamanan siber di ekosistem JSC, sehingga mampu memberikan perspektif kebijakan

yang komprehensif. Security Engineer dipilih sebagai informan kunci kedua karena merupakan praktisi teknis yang secara langsung merancang, mengoperasikan, dan memelihara sistem keamanan siber JSC sehari-hari, sehingga dapat memberikan data teknis yang akurat terkait implementasi kontrol pada setiap fungsi NIST CSF 2.0. Kombinasi kedua informan ini memungkinkan triangulasi antara perspektif kebijakan dan perspektif teknis-operasional. Studi dokumentasi dilakukan terhadap kebijakan keamanan informasi, laporan penilaian risiko, prosedur operasional, dan dokumen perencanaan strategis yang relevan.

Keabsahan data dijaga melalui triangulasi sumber (membandingkan informasi dari informan yang berbeda), triangulasi teknik (membandingkan hasil wawancara, observasi, dan dokumentasi), serta member check untuk memastikan kesesuaian interpretasi peneliti dengan kondisi aktual di lapangan.

Analisis dilakukan menggunakan kerangka NIST CSF 2.0 yang mencakup enam fungsi inti: Govern (GV), Identify (ID), Protect (PR), Detect (DE), Respond (RS), dan Recover (RC). Tingkat kematangan setiap kontrol dinilai menggunakan skala CMMI (Capability Maturity Model Integration) dari level 1 hingga 5. Penilaian tier keseluruhan mengacu pada panduan Implementation Tier NIST CSF 2.0, dengan rentang nilai 3,0-3,9 berada pada Tier 3 (Repeatable).

Penelitian dilaksanakan di Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta dan Unit Pengelola Jakarta Smart City pada Desember 2025 hingga Januari 2026.

III. HASIL DAN PEMBAHASAN

3.1. Penilaian Kematangan Berdasarkan Enam Fungsi NIST CSF 2.0

Penilaian kematangan keamanan siber Jakarta Smart City dilakukan terhadap 22 kontrol yang tersebar pada enam fungsi inti NIST CSF 2.0. Rekapitulasi hasil penilaian disajikan pada Tabel 1 berikut.

Tabel 1.

Skor Kematangan Keamanan Siber Jakarta Smart City Berdasarkan NIST CSF 2.0

Fungsi NIST CSF 2.0	Jumlah Kontrol	Rata-rata CMMI Level	Kategori Kematangan
GOVERN	9	3,17	Defined (3)
IDENTIFY	3	3,00	Defined (3)
PROTECT	5	3,60	Defined-Quant. (3-4)
DETECT	2	3,00	Defined (3)
RESPOND	4	3,00	Defined (3)
RECOVER	2	3,00	Defined (3)
RATA-RATA KESELURUHAN	**22**	**3,13**	**Defined (3)**

Sumber: Diolah Oleh Penulis, 2026

3.1.1. Fungsi Govern (GV)

Fungsi Govern memperoleh rata-rata CMMI Level 3,17 yang menempatkannya dalam kategori Defined. Tata kelola keamanan siber JSC telah dibangun di atas fondasi regulasi yang kuat, mengacu pada Peraturan Gubernur DKI tentang SPBE, ISO/IEC 27001, dan panduan teknis BSSN. Manajemen risiko rantai pasok (GV.SC) mencatat kematangan tertinggi pada Level 4, mencerminkan proses tiga tahap yang komprehensif dalam pengelolaan risiko vendor (pra-kontrak, selama kontrak, dan pasca-kontrak). Peran, tanggung jawab, dan kewenangan keamanan siber telah ditetapkan secara hierarkis dengan penetapan ISMS Manager, Data

Protection Officer (DPO), dan tim CSIRT. Terkait tata kelola kebijakan keamanan siber, Kepala Jakarta Smart City menyatakan: *"Kami sudah punya ISMS Manager, DPO, dan tim CSIRT yang berjalan. Regulasi dasarnya mengacu ke Pergub SPBE dan standar ISO 27001, jadi hierarkinya sudah jelas. Yang masih perlu kami perkuat adalah risk appetite statement yang lebih kuantitatif, supaya threshold-nya tidak hanya deskriptif."* Pernyataan ini mengonfirmasi bahwa fondasi tata kelola telah terbangun secara formal, namun ambang batas risiko yang terukur belum terdokumentasi secara eksplisit.. Aspek yang masih perlu diperkuat adalah pengembangan risk appetite statement yang spesifik dengan ambang batas kuantitatif dan pembentukan Cybersecurity Steering Committee dengan jadwal pertemuan rutin yang terformalisasi.

3.1.2. Fungsi Identify (ID)

Fungsi Identify memperoleh rata-rata CMMI Level 3,00. Pengelolaan aset teknologi informasi telah berjalan dengan dasar yang cukup kuat, dengan inventaris aset fisik yang dikelola secara konsisten pada Level 4. Penilaian risiko (ID.RA) dilaksanakan melalui pendekatan terstruktur meliputi uji penetrasi, Vulnerability Assessment and Penetration Testing (VAPT), dan security audit berkala. Aspek kritis yang memerlukan perhatian adalah pemetaan alur data organisasi: diagram alur data yang menggambarkan pergerakan data warga mulai dari aplikasi JAKI hingga penyimpanan dan penghapusan belum dipetakan secara eksplisit dan terpusat, yang merupakan kelemahan fundamental berimplikasi langsung pada kepatuhan Undang-Undang Pelindungan Data Pribadi (UU PDP). Security Engineer JSC menjelaskan kondisi pemetaan alur data sebagai berikut: *"Inventaris aset fisik sudah kami kelola dengan cukup baik dan konsisten. Tapi kalau bicara data flow diagram yang menggambarkan pergerakan data warga dari JAKI sampai ke penyimpanan akhir, itu memang belum ada dalam satu dokumen terpusat. Ini yang sedang kami kejar, apalagi dengan berlakunya UU PDP."* Temuan ini mengindikasikan adanya risiko kepatuhan regulasi yang perlu segera ditangani.

3.1.3. Fungsi Protect (PR)

Fungsi Protect mencatat skor tertinggi dalam penelitian ini dengan rata-rata CMMI Level 3,60. JSC telah menerapkan strategi proteksi berlapis (defense in depth) yang mengintegrasikan kontrol teknis, administratif, dan sumber daya manusia. Pengelolaan identitas (PR.AA) dan ketahanan infrastruktur (PR.IR) mencapai Level 4, didukung oleh implementasi SSO terintegrasi dengan NIK warga, Multi-Factor Authentication (MFA), autentikasi biometrik, Role-Based Access Control (RBAC), serta arsitektur DC/DRC dengan koneksi multi-ISP dan sistem anti-DDoS. Kepala Jakarta Smart City menjelaskan keunggulan sistem proteksi yang dibangun: *"Kami mengintegrasikan SSO dengan NIK warga, jadi autentikasinya sudah dua lapis — NIK plus MFA. Untuk akses internal juga sudah role-based. Infrastruktur DC dan DRC kami jalankan paralel dengan multi-ISP dan anti-DDoS. Tapi memang untuk environment dev dan production, pemisahannya belum seketat yang seharusnya kadang masih ada data yang karakteristiknya mirip produksi masuk ke testing tanpa data masking yang memadai."* Pengakuan ini memperkuat temuan kritis pada kontrol PR.PS-06 yang mencatat level kematangan terendah (Level 2). Kelemahan kritis yang teridentifikasi adalah pemisahan lingkungan pengembangan dan produksi yang belum formal (PR.PS-06, Level 2), di mana aplikasi terkadang diuji menggunakan data berkarakteristik serupa produksi tanpa mekanisme data masking yang memadai.

3.1.4. Fungsi Detect (DE)

Fungsi Detect memperoleh rata-rata CMMI Level 3,00. JSC telah membangun kapabilitas deteksi yang menggabungkan teknologi otomatisasi, pengawasan tim 24/7, dan

pemanfaatan intelijen ancaman siber. Pemantauan berkelanjutan dilakukan melalui sistem SIEM yang beroperasi real-time, tim analis keamanan bergiliran, dan threat intelligence dari BSSN. Security Engineer memaparkan kapabilitas pemantauan yang berjalan: *"SIEM kami beroperasi real-time 24 jam dengan tim analis yang bergiliran. Feed threat intelligence dari BSSN juga sudah kami integrasikan. Tantangannya adalah pemantauan terhadap perilaku pengguna internal masih manual dan rule-based — kami belum punya UEBA yang otomatis, sehingga anomali yang subtle kadang baru ketahuan setelah agak lama."* Pernyataan ini memperkuat penilaian bahwa kapabilitas deteksi berada pada Level 3, belum mencapai Level 4 yang mensyaratkan analitik perilaku otomatis. Meskipun pemantauan jaringan telah mencapai tingkat kematangan yang baik, pemantauan terhadap aktivitas aktor manusia (internal dan eksternal) masih bergantung pada analisis manual dan log berbasis aturan, belum memanfaatkan User and Entity Behavior Analytics (UEBA) secara otomatis.

3.1.5. Fungsi Respond (RS)

Fungsi Respond memperoleh rata-rata CMMI Level 3,00. Manajemen insiden di JSC dijalankan melalui siklus penanganan yang komprehensif menggunakan sistem ticketing, dengan tiga jalur penerimaan laporan: laporan otomatis dari SIEM, laporan internal staf, dan pengaduan masyarakat melalui aplikasi JAKI. Kepala Jakarta Smart City menjelaskan mekanisme respons insiden: *"Setiap insiden masuk melalui tiga jalur otomatis dari SIEM, laporan internal staf, atau pengaduan warga lewat JAKI. Setelah itu langsung kami triage dan masuk ke proses DFIR. Komunikasi ke publik kami lakukan satu pintu supaya tidak simpang siur. Yang memang masih perlu kami formalisasi adalah kriteria eskalasi kapan harus langsung ke level pimpinan, kapan cukup ditangani tim teknis."* Kondisi ini menjelaskan mengapa fungsi Respond berada pada Level 3 dengan potensi peningkatan pada aspek formalisasi prosedur eskalasi. Proses Digital Forensics and Incident Response (DFIR) dilaksanakan melalui empat tahapan berurutan: pengumpulan dan preservasi bukti, analisis log, forensik sistem, dan identifikasi akar masalah (Root Cause Analysis). Komunikasi insiden dilaksanakan melalui kerangka empat tahap yang mencakup koordinasi lintas instansi (BSSN, Polri, OPD terdampak) dan komunikasi publik satu pintu. Area yang perlu diperkuat adalah formalisasi kriteria eskalasi insiden, otomatisasi tindakan containment, dan ketersediaan templat komunikasi pra-disiapkan.

3.1.6. Fungsi Recover (RC)

Fungsi Recover memperoleh rata-rata CMMI Level 3,00. Rencana pemulihan layanan dieksekusi berdasarkan prinsip bahwa sistem hanya boleh dinyatakan pulih setelah ancaman dipastikan benar-benar hilang total, dengan prosedur empat tahap: validasi keamanan, eksekusi pemulihan bertahap, pengujian fungsional internal, dan normalisasi dengan enhanced monitoring. JSC menggunakan pendekatan out-of-band communication melalui kanal alternatif (WhatsApp Group darurat, SMS Blast, Portal Status layanan terpisah). Aspek yang perlu diperkuat adalah penyusunan Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) yang komprehensif dengan Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) yang terdefinisi secara kuantitatif untuk setiap layanan kritikal. Security Engineer menjelaskan prinsip pemulihan layanan yang dianut JSC: *"Sistem baru kami nyatakan pulih kalau ancamannya sudah benar-benar hilang total, bukan sekedar layanan sudah kembali online. Prosedurnya ada empat tahap: validasi keamanan dulu, baru eksekusi pemulihan bertahap, pengujian fungsional internal, kemudian normalisasi dengan enhanced monitoring selama beberapa hari ke depan. Untuk komunikasi darurat kami pakai out-of-band WhatsApp Group darurat dan SMS Blast kalau sistem utama terganggu."* Meski prosedur pemulihan telah berjalan konsisten, tidak adanya RTO dan RPO yang terdefinisi secara kuantitatif untuk setiap layanan kritikal menjadi area yang perlu segera diperkuat.

3.2. Posisi Tier Jakarta Smart City dalam NIST CSF 2.0

Berdasarkan nilai rata-rata CMMI sebesar 3,13, posisi kematangan keamanan siber Jakarta Smart City ditetapkan berada pada Tier 3 (Repeatable) dalam kerangka NIST CSF 2.0. Hal ini menandakan bahwa proses, kebijakan, dan kontrol keamanan siber telah terdokumentasi secara formal, diimplementasikan secara konsisten, serta terintegrasi dalam operasional organisasi, meskipun belum sepenuhnya adaptif. Pemetaan tier disajikan pada Tabel 2.

Tabel 2.

Pemetaan Tier NIST CSF 2.0

Tier	Nilai CMMI	Deskripsi	Karakteristik Utama
Tier 1	1,0-1,9	Partial	Praktik ad-hoc, reaktif, tidak terdokumentasi
Tier 2	2,0-2,9	Risk-Informed	Kesadaran risiko ada, implementasi belum konsisten
Tier 3	3,0-3,9	Repeatable	Kebijakan terdokumentasi, implementasi konsisten, manajemen risiko terintegrasi
Tier 4	4,0-5,0	Adaptive	Pendekatan proaktif, adaptif berbasis pembelajaran berkelanjutan

*Sumber: NIST CSF 2.0, 2024; *) Posisi Jakarta Smart City*

3.3. Implikasi terhadap Pencapaian SDGs

Tingkat kematangan keamanan siber Jakarta Smart City pada Tier 3 (Repeatable) berkontribusi secara bermakna terhadap pencapaian Sustainable Development Goals melalui rantai hubungan kausal yang dapat dijelaskan sebagai berikut.

Pertama, kapabilitas keamanan siber yang terukur (cybersecurity capability) memperkuat good governance pemerintahan digital, khususnya dalam aspek efektivitas layanan, akuntabilitas pengelolaan data, transparansi sistem digital, dan kepercayaan masyarakat terhadap layanan pemerintah berbasis teknologi. Hal ini berkontribusi langsung pada SDG 16 (Peace, Justice and Strong Institutions) melalui terwujudnya institusi yang akuntabel, transparan, dan terpercaya.

Kedua, pembangunan infrastruktur digital yang tangguh melalui penerapan arsitektur DC/DRC, sistem anti-DDoS, dan ketahanan jaringan berkontribusi pada SDG 9 (Industry, Innovation and Infrastructure) melalui pengembangan infrastruktur yang andal dan berkelanjutan.

Ketiga, keandalan layanan publik digital Jakarta Smart City yang dijamin oleh keamanan siber yang matang berkontribusi pada SDG 11 (Sustainable Cities and Communities) melalui pengembangan kota cerdas yang aman, inklusif, dan berkelanjutan.

3.4. Diskusi Temuan Utama Penelitian

Temuan penelitian menunjukkan bahwa Jakarta Smart City berada pada Tier 3 (Repeatable), yang sejalan dengan temuan Ibrahim et al. (2018) bahwa pemerintah daerah yang telah menerapkan kerangka kerja formal cenderung berada pada tier ini. Berbeda dengan temuan Norris et al. (2020) yang menemukan kebanyakan pemerintah lokal di Amerika Serikat masih berada pada Tier 1-2, JSC telah melampaui tahap reaktif dan memiliki fondasi kebijakan

yang lebih matang, kemungkinan didukung oleh regulasi SPBE yang mengharuskan pemenuhan standar minimal keamanan informasi.

Temuan ini memperkuat penelitian Sulistyowati et al. (2020) bahwa penilaian kematangan menggunakan kerangka NIST CSF memberikan gambaran yang lebih komprehensif dan terstruktur dibandingkan penilaian parsial. Senada dengan temuan Hossain et al. (2024), pemerintah daerah yang memiliki regulasi khusus keamanan informasi (seperti Pergub DKI tentang SPBE) cenderung memiliki tingkat kematangan yang lebih tinggi.

Satu temuan menarik yang membedakan penelitian ini adalah ditemukannya kontribusi kausal antara kematangan keamanan siber smart city dengan pencapaian SDGs, yang belum banyak dieksplorasi dalam penelitian sebelumnya. Hal ini memperluas perspektif bahwa keamanan siber bukan hanya isu teknis operasional, melainkan juga merupakan instrumen strategis dalam mewujudkan tata kelola yang berkelanjutan.

3.5. Diskusi Temuan Menarik Lainnya

Penelitian ini menemukan bahwa pemisahan lingkungan pengembangan dan produksi (PR.PS-06) menjadi kontrol dengan gap paling kritis (Level 2), di mana aplikasi terkadang diuji menggunakan data berkarakteristik serupa produksi tanpa mekanisme data masking yang memadai. Temuan ini mengindikasikan risiko kebocoran data sensitif warga yang tidak kalah serius dengan ancaman eksternal. Selain itu, ketiadaan pemetaan alur data (data flow diagram) yang komprehensif untuk seluruh aplikasi kritikal menjadi hambatan fundamental bagi kepatuhan UU PDP yang baru diberlakukan di Indonesia.

Peneliti juga menemukan bahwa JSC memiliki keunggulan komparatif pada pengelolaan identitas dan kontrol akses (PR.AA) yang mencapai Level 4, didukung oleh integrasi SSO dengan NIK warga yang merupakan implementasi unik yang belum banyak ditemukan pada smart city lain di Indonesia. Hal ini menunjukkan bahwa pemanfaatan data kependudukan nasional dapat menjadi enabler kematangan keamanan siber yang signifikan.

IV. KESIMPULAN

Penelitian ini menyimpulkan bahwa Jakarta Smart City berada pada Tier 3 (Repeatable) dalam kerangka NIST CSF 2.0, dengan nilai rata-rata CMMI sebesar 3,13. Seluruh proses, kebijakan, dan kontrol keamanan siber telah terdokumentasi secara formal dan diimplementasikan secara konsisten. Fungsi Protect mencatat skor tertinggi (3,60) melalui penerapan autentikasi multi-faktor dan pengelolaan identitas yang kuat, sementara aspek kritis yang perlu segera ditangani adalah pemetaan alur data dan pemisahan lingkungan pengembangan-produksi.

Kematangan keamanan siber JSC pada Tier 3 berkontribusi secara bermakna terhadap pencapaian SDG 16 melalui institusi digital yang akuntabel dan terpercaya, SDG 9 melalui infrastruktur digital yang tangguh, serta SDG 11 melalui tata kelola kota cerdas yang aman dan berkelanjutan. Dengan demikian, peningkatan kematangan keamanan siber merupakan instrumen strategis, bukan sekadar upaya teknis-operasional, dalam mewujudkan tata kelola Smart City yang inklusif dan selaras dengan agenda pembangunan global.

Keterbatasan penelitian ini terletak pada cakupan informan yang terbatas pada dua narasumber dan lokus penelitian yang hanya mencakup satu ekosistem smart city. Untuk penelitian selanjutnya, disarankan agar dilakukan kajian komparatif antar Smart City di Indonesia menggunakan NIST CSF 2.0 serta kajian tentang efektivitas implementasi UU PDP dalam tata kelola data warga pada ekosistem Smart City Indonesia.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih ditujukan kepada Kepala Jakarta Smart City dan Security Engineer Jakarta Smart City atas kesediaan menjadi informan dalam penelitian ini, serta kepada Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta yang telah memberikan akses dan fasilitas selama penelitian berlangsung. Terima kasih juga disampaikan kepada Bapak Mohammad Rezza Fahlevvi, S.Kom., M.Cs. selaku dosen pembimbing atas bimbingan dan arahan yang diberikan.

VI. DAFTAR PUSTAKA

Aferudin, F. (2022). Skema Berbagi Informasi Keamanan Siber Menggunakan Model Hub and Spoke Untuk Mendapatkan Kepercayaan Dalam Public-Private Partnership. *Info Kripto*. https://doi.org/10.56706/ik.v16i2.51

Alfarizi, B. Z., Silvyasari, D., & Heryadi, D. (2024). Global *Govern*ance in the 21st Century: A Digital Trends and Transformation. *Gli*. https://doi.org/10.22219/gli.v4i1.31682

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local *govern*ment authorities. *Government Information Quarterly*, *37*(1), 101419. https://doi.org/https://doi.org/10.1016/j.giq.2019.101419

Aliza, N. O., Prianto, Y., & Rahaditya, R. (2022). Regulasi Proteksi Data Pribadi Pasien Covid-19 Di Indonesia. *Jurnal Muara Ilmu Sosial Humaniora Dan Seni*. https://doi.org/10.24912/jmishumsen.v6i1.13462.2022

Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garces, I. (2020). A Comprehensive Study of the IoT *Cybersecurity* in Smart Cities. *IEEE Access*, *8*, 228922–228941. https://doi.org/10.1109/ACCESS.2020.3046442

Arief, A., & Abbas, M. (2021). Kajian Literatur (Systematic Literature Review): Kendala Penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). *Protek Jurnal Ilmiah Teknik Elektro*. https://doi.org/10.33387/protk.v8i1.1978

Barunea, P. P., Anastasya, M. P., R, N. D., & Wahyuni, O. S. (2023). Evaluasi Jakarta Kini (Jaki) Dalam Mewujudkan Jakarta *Smart City* (Kajian Pemanfaatan Layanan JakWifi). *JSC*. https://doi.org/10.61183/jsc.v1i1.12

Bernardo, L., Malta, S., & Magalhães, J. (2025). An Evaluation Framework for *Cybersecurity Maturity* Aligned with the NIST CSF. *Electronics (Switzerland)*, *14*(7), 1–20. https://doi.org/10.3390/electronics14071364

Bibri, S. E., & Krogstie, J. (2020). The emerging data–driven *Smart City* and its innovative applied solutions for sustainability: the cases of London and Barcelona. *Energy Informatics*, *3*(1), 5. https://doi.org/10.1186/s42162-020-00108-6

Creswell, J. W. (1994). Research design: Qualitative & quantitative approaches. In *Research design: Qualitative & quantitative approaches*. (pp. xix, 228–xix, 228). Sage Publications, Inc.

Dankevych, Y., & Dankevych, V. (2025). Digital Tools for Enhancing Public Policy and *Govern*ance in the Context of Global Challenges. *Ape*. https://doi.org/10.32752/1993-6788-2025-1-289-95-105

Demirel, D. (2023). The Impact of Managing Diversity on Building the *Smart City* a Comparison of *Smart City* Strategies: Cases From Europe, America, and Asia. *Sage Open*. https://doi.org/10.1177/21582440231184971

Dewi, A. S., & Avianto, B. N. (2023). Implementation of Jakarta *Smart City* in One-Stop-Service: Daily Need in the City South Jakarta? *Journal Research of Social Science Economics and Management*. https://doi.org/10.59141/jrssem.v2i09.428

Dickens, C., Boynton, P., & Rhee, S. (2019). Principles for designed-in security and privacy for smart cities. *SCOPE 2019 - Proceedings of the 2019 International Science of Smart City Operations and Platforms Engineering*, 25–29.

https://doi.org/10.1145/3313237.3313300
Fadli, M. R. (2021). *Memahami desain metode penelitian kualitatif*. *21*(1), 33–54. https://doi.org/10.21831/hum.v21i1.
Fahlevvi, M. R., Apriyansa, A., Huda, N., Utami, D., Putri, K., & Tawil, Z. N. (n.d.). *From Smart Government to Smart People : Policy Challenges and Green Innovation for Sustainable City in Malang*.
Fleming, C., Reith, M., & Henry, W. (2023). Securing Commercial Satellites for Military Operations: a *Cybersecurity* Supply Chain Framework. *International Conference on Cyber Warfare and Security*. https://doi.org/10.34190/iccws.18.1.1062
Fukuda-Parr, S. (2018). *Sustainable Development Goals*. https://doi.org/10.1093/oxfordhb/9780198803164.013.42
Güler, M., & Büyüközkan, G. (2023). A Survey of Digital *Govern*ment: Science Mapping Approach, Application Areas, and Future Directions. *Systems*. https://doi.org/10.3390/systems11120563
Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local *Govern*ment *Cybersecurity* Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences (Switzerland)*, *14*(13). https://doi.org/10.3390/app14135501
Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local *govern*ment using NIST CSF: a case study. *Journal of Supercomputing*, *74*(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2
Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of *Cybersecurity Maturity* Assessment Framework Using NIST CSF v1.1 and CIS Controls V8. *Inovtek Polbeng - Seri Informatika*. https://doi.org/10.35314/isi.v9i1.3973
Kelana, M. A., & Fahlevvi, M. R. (2024). *Manajemen Aplikasi SIPD di Inspektorat Provinsi Riau Dalam Perspektif George R . Management of SIPD Application at the Riau Provincial Inspectorate from the Perspective of George R . Terry*. *4*(1), 19–35.
Klarić, M. (2023). *Smart Digitalization and Public Services in the Eu*. https://doi.org/10.25234/eclic/27446
Komninos, D., Dermatis, Z., Papageorgiou, C., & Anastasiou, A. (2024). Comparative Analysis Between Greece and Cyprus of the Impact of Digital Transformation on the Development of Quality of Life. *Theoretical Economics Letters*. https://doi.org/10.4236/tel.2024.141014
Machlul, M. (2024). Peningkatan Kualitas SDM Melalui Pelatihan Cyber Security Pada Anggota Polisi Daerah Jawa Timur. *Parta Jurnal Pengabdian Kepada Masyarakat*. https://doi.org/10.38043/parta.v4i2.4655
Margaretha, A. M., & Nugroho, A. A. (2023). Transportasi Publik Terintegrasi: Optimalisasi Implementasi Smart Mobility Di DKI Jakarta. *Jplan*. https://doi.org/10.32834/jplan.v5i2.676
Mastrogiovanni, S. (2025). AI-Driven Data *Govern*ance for Smart Cities: Balancing Privacy, Efficiency, and Public Trust. *South Florida Journal of Development*. https://doi.org/10.46932/sfjdv6n9-029
Meher, C., Sidi, R., & Risdawati, I. (2023). Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum Dan Kebijakan Di Indonesia. *Jurnal Ners*. https://doi.org/10.31004/jn.v7i2.16088
Nair, P. (2023). Enhancing *Cybersecurity* Awareness Training Through the NIST Framework. *Ijarcce*. https://doi.org/10.17148/ijarcce.2023.121203
Najiyya, A., & Wulandari, S. S. (2023). Eksplorasi Implementasi Kebijakan Pembentukan Computer Security Incident Response Team (Csirt) Di Kementerian Perdagangan: Sebuah Studi Kualitatif. *Jram (Jurnal Riset Akuntansi Multiparadigma)*. https://doi.org/10.30743/akutansi.v10i1.7246

Nanik Alfiani, F. R. (2024). Regulation and Literacy Must Strengthen Digital Transformation. *Ajesh*. https://doi.org/10.46799/ajesh.v3i1.213

Nethan Kuru, G. S., Surya Gumilang, S. F., & Nugraha, R. A. (2021). Model Arsitektur Sistem Pemerintahan Berbasis Elektronik (Spbe) Domain Proses Bisnis Pada Pemerintah Kabupaten Kuningan. *Jipi (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*. https://doi.org/10.29100/jipi.v6i2.2116

Norris, D., Mateczun, L., Joshi, A., & Finin, T. (2020). Managing *cybersecurity* at the grassroots: Evidence from the first nationwide survey of local *govern*ment *cybersecurity*. *Journal of Urban Affairs*, *43*, 1–23. https://doi.org/10.1080/07352166.2020.1727295

Nurmala Fairuzyah, I., Ahmad Arkaan, G., Alfath Marfariza, H., Meisya Indira Putri Suhendar, & Syifa Khoirunnisa. (2024). Building Public Trust Through E-*Govern*ance Strategy: Case Study in DKI Jakarta, Indonesia. *Social Impact Journal*, *3*(2), 32–41. https://doi.org/10.61391/sij.v3i2.170

Pratiwi, P. (2020). Menuju Pemerintahan Elektronik Yang Transformatif Pratiwi. *Jurnal Wacana Kinerja Kajian Praktis-Akademis Kinerja Dan Administrasi Pelayanan Publik*. https://doi.org/10.31845/jwk.v23i2.689

Ridho Alkadrie, S. M. (2023). SIM Card Dengan Identitas Palsu: Melanggar Hukum Atau Area Kelabu Dalam Perlindungan Data Pribadi. *Arus Jurnal Sosial Dan Humaniora*. https://doi.org/10.57250/ajsh.v3i3.292

Rigopoulos, K. (2024). *NIST Cybersecurity Framework 2.0 :* https://doi.org/10.6028/nist.sp.1299.spa

Sandy, S., & Solihin, H. H. (2021). Audit Keamanan Dan Manajemen Risiko Pada E-Learning Universitas Sangga Buana. *Jurnal Manajemen Informatika (Jamika)*. https://doi.org/10.34010/jamika.v11i1.3641

Sarjito, A. (2024). Data Security and Privacy in the Digital Era: Challenges for Modern *Govern*ment. *Jian*. https://doi.org/10.56071/jian.v8i3.933

SMART AND SECURE CITIES AND COMMUNITIES CHALLENGE (SC3) A Risk Management Approach to Smart City Cybersecurity and Privacy. (2019). *July 2019*. https://pages.nist.gov/GCTC/uploads/blueprints/2019-CPAC-Guidebook-Datasheet-FINAL-20190816.pdf

Sugiyono. (2023). *Metode Penelitian Kuantitatif, Kualitatif Dan r&d Sugiyono*.

Sugiyono, D. (2013). *Metode Penelitian Kuantitatif, Kualitatif, dan Tindakan*.

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of *Cybersecurity Maturity* Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS [Análisis comparativo y diseño de la metodología de evaluación de la madurez de la ciberseguridad utilizando NIST CSF, COBIT,. *Joiv*, *4*(4), 1–6.

Wekke, I. S. (2019). *Metode Penelitian Sosial* (Issue October 2019).

Yoo, Y. (2021). Toward Sustainable *Govern*ance: Strategic Analysis of the *Smart City* Seoul Portal in Korea. *Sustainability*. https://doi.org/10.3390/su13115886