ANALISIS KEKUATAN KEAMANAN DIGITAL BERBASIS *AI CYBERSECURITY* MENGGUNAKAN *NIST CSF 2.0* PADA DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KABUPATEN MINAHASA UTARA PROVINSI SULAWESI UTARA

Ricky Estefan Pandelaki
NPP. 33.0862
Program Studi Teknologi Rekayasa Informasi Pemerintahan
Email: estefanpandelaki91@gmail.com

Pembimbing Skripsi: Rina Wahyuni, S.Kom., M.T.I
Email: rinawahyuni@ipdn.ac.id

ABSTRACT

Problem Statement: *The North Minahasa Regency Government's digital security implementation is not yet optimal, as outlined in the 2024 Minut Communications and Information Technology Service (Diskominfosan Minut) LKJIP, while cyber threats continue to increase over time.* ***Purpose:*** *This study aims to determine and analyze the strength of digital security using NIST CSF 2.0 and describe efforts to improve it based on AI Cybersecurity at the Communication, Informatics and Cryptography Service of North Minahasa Regency.* ***Method:*** *This study aims to determine and analyze the strength of digital security using NIST CSF 2.0 at the Communication, Informatics and Cryptography Service of North Minahasa Regency.* ***Result:*** *Research findings indicate that the digital security strength of the North Minahasa Regency Communication, Informatics, and Cryptography Agency is at the Partial to Risk-Informed level based on the NIST CSF 2.0. The Govern is at the Partial to Risk-Informed level because it already has a basic organizational context, roles, and policies, but cybersecurity governance is not yet running optimally. The Identify, Protect, and Detect is at the Partial level because risk identification, asset protection, and threat monitoring are still limited and not standardized. Meanwhile, the Respond and Recover is at the Partial to Risk-Informed level because there have been incident response and recovery efforts, but they are not supported by mature, tested, and integrated procedures. Furthermore, the implementation of AI Cybersecurity has not been implemented operationally.* ***Conclusion:*** *This study concludes that all functions have not been implemented consistently and have not integrated AI Cybersecurity operationally. Improvement efforts include strengthening technical cybersecurity policies, developing asset management, implementing layered authentication, implementing an AI-based continuous monitoring system, activating a Cyber Incident Response Team, developing a DRP, and continuously developing human resource capacity. It is recommended that the North Minahasa Regency Government allocate a proportional budget for digital security and make cybersecurity a strategic agenda in the RPJMD and APBD.*
Keywords**:** *AI Cybersecurity; Digital Security; Local Government; NIST CSF 2.0*

ABSTRAK

Permasalahan: Penerapan keamanan digital Pemerintah Kabupaten Minahasa Utara belum optimal sebagaimana tertuang dalam LKJIP Diskominfosan Minut Tahun 2024, sementara ancaman siber terus meningkat seiring berjalannya waktu. **Tujuan:** Penelitian ini bertujuan untuk mengetahui dan menganalisis kekuatan keamanan digital menggunakan *NIST CSF 2.0* pada Diskominfosan Kabupaten Minahasa Utara. **Metode:** Penelitian ini menggunakan metode deskriptif kualitatif dengan pengumpulan data melalui wawancara semi-terstruktur, observasi, dan studi dokumentasi. Informan dipilih secara *purposive sampling*, terdiri dari Kepala Bidang Persandian, Kepala Bidang E-Government, dan Analis Kebijakan Ahli Muda Bidang E-Government. Analisis data menggunakan model *Miles* dan *Huberman.* **Hasil/Temuan:** Temuan penelitian menunjukkan bahwa kekuatan keamanan digital Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara berada pada tingkat *Partial* hingga *Risk-Informed* berdasarkan *NIST CSF 2.0*. *Govern* berada pada tingkat *Partial* menuju *Risk-Informed* karena telah memiliki konteks organisasi, peran, dan kebijakan dasar, namun tata kelola keamanan siber belum berjalan secara optimal. *Identify, Protect,* dan *Detect* berada pada tingkat *Partial* karena identifikasi risiko, perlindungan aset, serta pemantauan ancaman masih bersifat terbatas dan belum terstandarisasi. Sementara itu, *Respond* dan *Recover* berada pada tingkat *Partial* menuju *Risk-Informed* karena telah terdapat upaya respons dan pemulihan insiden, namun belum didukung prosedur yang matang, teruji, dan terintegrasi. **Kesimpulan:** Penelitian ini menyimpulkan bahwa seluruh fungsi belum berjalan konsisten dan belum mengintegrasikan *AI Cybersecurity* secara operasional. Upaya peningkatan mencakup penguatan kebijakan teknis keamanan siber, pengembangan manajemen aset, implementasi autentikasi berlapis, penerapan sistem pemantauan berkelanjutan berbasis *AI*, aktivasi Tim Tanggap Insiden Siber, penyusunan DRP, serta pengembangan kapasitas SDM yang berkelanjutan. Disarankan agar Pemerintah Kabupaten Minahasa Utara mengalokasikan anggaran proporsional untuk keamanan digital dan menjadikan keamanan siber sebagai agenda strategis dalam RPJMD dan APBD.

Kata kunci: *AI Cybersecurity*; Keamanan Digital*; NIST CSF 2.0*; Pemerintah Daerah

I. PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi *Artificial Intelligence* (AI) telah mengubah paradigma keamanan siber di sektor publik, menjadikannya elemen strategis dalam mendeteksi ancaman, menganalisis pola serangan, serta merespons insiden digital secara otomatis dan adaptif (Busetti & Scanni, 2025; Sarker, 2023; Schmitt, 2023). Pada pemerintahan daerah, kemampuan ini sangat penting karena sistem informasi publik mengelola data yang bersifat sensitif dan krusial bagi keberlangsungan layanan digital pemerintahan. Berbagai regulasi telah menegaskan pentingnya keamanan digital, mulai dari Perpres No. 47/2023 tentang Strategi Keamanan Siber Nasional dan UU 27/2022 tentang Perlindungan Data Pribadi (Wiredarme, 2025). Oleh karena itu, keamanan digital berbasis *AI Cybersecurity* menjadi salah satu kunci keberhasilan penerapan Pemerintahan Digital (Achuthan et al., 2024; Hossain et al., 2024a).

Disisi lain, krisis ancaman siber di tingkat nasional menunjukkan peningkatan yang signifikan. Berdasarkan data GoodStats (2025), insiden serangan siber di Indonesia meningkat dari 40 insiden pada triwulan pertama 2021 menjadi 139 insiden pada triwulan pertama 2025. Insiden kebocoran data Pusat Data Nasional Sementara (PDNS) pada Juni 2024 akibat serangan *ransomware LockBit 3.0* menjadi salah satu krisis siber terbesar yang menunjukkan lemahnya sistem keamanan siber nasional (Tommy et al., 2025). Laporan SOCRadar (2025) juga mencatat bahwa sektor administrasi publik

menguasai paparan *dark web* sebesar 34,93%, menjadikannya sasaran utama kejahatan siber. Kondisi ini menunjukan perkembangan ancaman digital yang terus meningkat dan lebih kompleks serta menunjukan sasaran utama kejahatan siber ialah sektor pemerintahan (Hapsari & Pambayun, 2023).

Berdasarkan Laporan Kinerja Instansi Pemerintah Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara tahun 2024 menunjukkan bahwa penerapan keamanan digital belum optimal. Masalah ini diperkuat dengan wawancara bersama Kepala Bidang Persandian bahwa website minut.go.id pernah mengalami penyusupan iklan judi online, dan pernah terjadi kebocoran data akibat insiden pada PDNS tahun 2024. Kondisi ini menunjukkan kesenjangan antara tuntutan standar keamanan penyelenggaraan SPBE dengan penerapan keamanan digital yang dimiliki Pemerintah Kabupaten Minahasa Utara.

1.2. Kesenjangan Masalah yang Diambil (Research Gap)

Penulis berfokus pada permasalahan belum optimalnya kekuatan keamanan digital di Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara dalam menghadapi perkembangan ancaman siber yang semakin kompleks. Di satu sisi, Dinas Komunikasi Informatika dan Persandian memiliki peran strategis dalam mengelola data, informasi, dan layanan digital pemerintah daerah serta dituntut menjamin keamanan penyelenggaraan SPBE. Namun di sisi lain, berdasarkan kondisi yang ditemukan masih terdapat kelemahan dalam penerapan keamanan digital sehingga menunjukkan adanya kesenjangan antara kebutuhan keamanan digital yang adaptif terhadap ancaman siber modern dengan kondisi keamanan digital yang dimiliki organisasi saat ini. Selain itu, meskipun berbagai penelitian telah membahas adopsi *AI Cybersecurity* di instansi pemerintahan (Agus Kurniati, 2024; Fauziyyah et al., 2025) dan penerapan *NIST CSF* di berbagai sektor (Ferdynandus et al., 2024; Hossain et al., 2024b), masih terdapat keterbatasan penelitian yang secara empiris mengintegrasikan *AI Cybersecurity* dengan *NIST CSF 2.0* untuk menganalisis kekuatan keamanan digital pada instansi pemerintah daerah, khususnya Dinas Komunikasi Informatika dan Persandian.

1.3. Urgensi Penelitian

Penelitian ini penting dilakukan untuk memberikan gambaran empiris mengenai kekuatan keamanan digital berbasis *AI Cybersecurity* menggunakan *NIST CSF 2.0* pada Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara sebagai dasar perumusan strategi penguatan keamanan digital. Tanpa analisis ini, pemerintah dan pemangku kebijakan akan kekurangan dasar empiris untuk memahami kondisi aktual keamanan digital daerah, sehingga perumusan strategi pengembangan berisiko tidak tepat sasaran dan tidak efektif dalam menghadapi ancaman siber yang terus berkembang (Gaffur & Fachry Fachrudin, 2023; Hidayah & Almadani, 2022; Imran et al., 2024; Setyasih, 2022; Woods & Seymour, 2023).

1.4. Penelitian Terdahulu

Penelitian ini terinspirasi oleh beberapa penelitian terdahulu yang berkaitan dengan keamanan digital, penerapan *NIST Cybersecurity Framework*, dan *AI Cybersecurity*. Penelitian oleh Hossain et al. mengkaji kebijakan keamanan siber pemerintah daerah menggunakan metode kualitatif dengan analisis konten dan menemukan bahwa kebijakan keamanan siber pemerintah daerah masih memiliki berbagai celah, terutama pada aspek pemulihan insiden, manajemen rantai pasok, dan deteksi ancaman (Hossain et al., 2024b). Ferdynandus et al. meneliti implementasi *NIST CSF* pada sektor jasa keuangan menggunakan pendekatan *mixed-methods* dan menemukan bahwa penerapan *NIST CSF* mampu memperkuat tata kelola serta kontrol keamanan siber, meskipun masih terdapat kendala pada aspek sumber daya manusia dan proses organisasi (Ferdynandus et al., 2024). Ulfa et al. mengkaji

manajemen risiko menggunakan *NIST CSF 1.1* pada sektor perbankan dan menemukan bahwa fungsi deteksi masih memerlukan penguatan karena belum tersedia sistem yang mampu mendeteksi ancaman secara optimal (Ulfa et al., 2023). Nurochman et al. (2024) meneliti keamanan siber sistem informasi perpustakaan menggunakan pendekatan kualitatif dan menemukan bahwa implementasi *NIST CSF* belum dilakukan secara prosedural dan masih bergantung pada pengalaman administrator sistem (Nurochman et al., 2024).

Selanjutnya, Adhinugroho dan Kilian mengkaji keamanan siber pada lingkungan pemerintah daerah dan menemukan bahwa pemerintah daerah masih menghadapi berbagai tantangan seperti keterbatasan sumber daya manusia, tata kelola keamanan siber, dan kesiapan organisasi dalam menghadapi ancaman digital (Adhinugroho, 2024; Kilian & Rudianto, 2024). Sementara itu, Kurniati meneliti *AI Cybersecurity* melalui pendekatan *systematic literature review* dan menemukan bahwa kecerdasan buatan mampu meningkatkan kemampuan deteksi, respons, dan pengelolaan risiko keamanan siber, namun masih menghadapi tantangan transparansi, etika, dan privasi data (Agus Kurniati, 2024). Fauziyyah et al. juga menemukan bahwa *AI Cybersecurity* memiliki potensi besar dalam memperkuat pertahanan siber, tetapi implementasinya masih menghadapi keterbatasan sumber daya manusia, kebijakan teknis, dan kesiapan infrastruktur organisasi (Fauziyyah et al., 2025).

Secara umum, penelitian-penelitian tersebut menunjukkan bahwa penerapan *NIST Cybersecurity Framework* efektif dalam meningkatkan keamanan siber organisasi dan *AI Cybersecurity* memiliki potensi untuk memperkuat kemampuan perlindungan, deteksi, dan respons terhadap ancaman siber. Namun, sebagian besar penelitian masih berfokus pada penerapan *NIST CSF* atau *AI Cybersecurity* secara terpisah, serta dilakukan pada sektor selain pemerintah daerah.

1.5. Pernyataan Kebaruan Ilmiah

Penelitian ini memiliki kebaruan dibandingkan penelitian terdahulu karena menganalisis kekuatan keamanan digital pada Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara menggunakan *NIST Cybersecurity Framework (CSF) 2.0* yang merupakan kerangka kerja keamanan siber terbaru. Selain itu, penelitian ini tidak hanya mengidentifikasi kondisi keamanan digital berdasarkan fungsi *Govern, Identify, Protect, Detect, Respond,* dan *Recover,* tetapi juga mengintegrasikan pendekatan *AI Cybersecurity* sebagai upaya penguatan keamanan digital. Dengan demikian, penelitian ini menghasilkan analisis yang lebih komprehensif mengenai kondisi keamanan digital pemerintah daerah sekaligus memberikan rekomendasi penguatan keamanan digital berbasis *AI Cybersecurity* yang belum banyak dikaji dalam penelitian sebelumnya.

1.6. Tujuan

Penelitian ini bertujuan untuk mengetahui dan menganalisis kekuatan keamanan digital menggunakan *NIST CSF 2.0* pada Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara Provinsi Sulawesi Utara.

II. METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif yang dipilih karena fokus penelitian membutuhkan pemahaman mendalam terhadap kondisi, proses, dan dinamika implementasi keamanan digital yang tidak dapat dijelaskan hanya melalui data numerik (Saputra et al., 2023). Pendekatan ini memungkinkan eksplorasi secara holistik terhadap fenomena kekuatan keamanan digital berbasis *AI Cybersecurity* di Diskominfosan Minut.

Pengumpulan data dilakukan melalui tiga teknik utama. Pertama, wawancara semi-terstruktur terhadap tiga informan yang dipilih secara *purposive sampling* berdasarkan peran dan kompetensinya yakni Kepala Bidang Persandian sebagai informan kunci yang memiliki otoritas dalam kebijakan keamanan, Kepala Bidang E-Government, dan Analis Kebijakan Ahli Muda Bidang E-Government yang memiliki pengetahuan teknis operasional. Kedua, observasi lapangan terhadap kondisi infrastruktur dan dokumen kebijakan digital. Ketiga, studi dokumentasi terhadap Renstra 2025-2029, LKJIP 2024-2025, Keputusan Bupati Minahasa Utara, dan Perbup SPBE.

Pengujian keabsahan data dilakukan melalui triangulasi sumber (membandingkan informasi dari berbagai informan) dan triangulasi teknik (wawancara, observasi, dan dokumentasi). Analisis data menggunakan model *Miles* dan *Huberman* melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan, dengan *NIST CSF 2.0* sebagai kerangka analisis utama. Penelitian dilaksanakan di Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara, Provinsi Sulawesi Utara, selama bulan Desember 2025 hingga Januari 2026..

III. HASIL DAN PEMBAHASAN

Penulis menganalisis kekuatan keamanan digital Diskominfosan Minut menggunakan kerangka kerja *NIST CSF 2.0* yang mencakup enam fungsi: *Govern, Identify, Protect, Detect, Respond,* dan *Recover*, yang dikaitkan dengan pendekatan *AI Cybersecurity* sebagai standar keamanan adaptif (White & Sjelin, 2021).

3.1. Analisis Kekuatan Keamanan Digital Menggunakan NIST CSF 2.0

Penulis melakukan analisis kekuatan keamanan digital Diskominfosan Minut menggunakan NIST CSF 2.0 sehingga mendapatkan kondisi kekuatan keamanan digital saat ini (*current profile*).

Tabel 1.
Kondisi Kekuatan Keamanan Digital Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara

Dimensi	Indikator	Tier	Deskripsi Temuan	Status	Kode	Bukti Pendukung
Govern	Organizational Context	2	Struktur organisasi dan dokumen perencanaan telah tersedia, namun belum spesifik mengarah pada keamanan siber berbasis risiko	Risk-Informed	GV.OC	Renstra Diskominfosan 2025–2029; LKJIP 2025; Perbup SPBE 27/2022; wawancara i1 tentang TTIS masih sebatas dokumen
	Risk Management Strategy	1	Strategi keamanan digital belum menjadi prioritas utama dan belum berbasis manajemen risiko	Partial	GV.RM	Keputusan Bupati Minut 172/2023; Keputusan Bupati Minut 161/2023; Perbup SPBE 27/2022; wawancara i1 tentang anggaran yang belum memadai

	Roles, Responsibilities, and Authorities	2	Pembagian peran sudah jelas secara administratif, tetapi belum optimal dalam implementasi keamanan digital	Risk-Informed	GV.RR	LKJIP 2025; Renstra Diskominfosan 2025–2029; wawancara i1 tentang bidang persandian hanya diisi kabid tanpa staf
	Policy	2	Kebijakan sudah ada dalam dokumen Renstra namun belum spesifik sebagai kebijakan keamanan siber teknis	Risk-Informed	GV.PO	Renstra Diskominfosan 2025–2029; LKJIP 2025; RPJMD Minut; Perbup SPBE 27/2022; Peraturan BSSN 4/2021
	Oversight	1	Pengawasan keamanan siber belum berjalan secara rutin dan sistematis	Partial	GV.OC	Wawancara i1 tentang anggaran Rp10 juta per tahun dan kebutuhan IPS server yang belum terpenuhi
	Cybersecurity Supply Chain Risk Management	1	Pengelolaan risiko rantai pasok keamanan siber belum dilakukan karena belum ada kerja sama dengan pihak ketiga untuk memperkuat keamanan digital	Partial	GV.SC	Wawancara i1 tentang belum adanya pihak ketiga; rekomendasi MoU dari BSSN dalam rapat koordinasi provinsi
Identify	Asset Management	2	Inventaris aset TIK telah diketahui, tetapi klasifikasi aset berdasarkan tingkat kekritisan belum dilakukan secara sistematis sebagai dasar manajemen risiko	Risk-Informed	ID.AM	LKJIP 2025; Keputusan Bupati 164/2023 tentang Arsitektur SPBE; wawancara i2,i3 mengenai dokumen spesifikasi aset di bagian umum
	Risk Assessment	1	Penilaian risiko ada dalam bentuk audit SPBE dan audit TIK, bukan asesmen risiko keamanan siber yang formal, berulang, dan berbasis ancaman aktual (belum melakukan penilaian risiko)	Partial	ID.RA	Wawancara i2,i3 tentang audit TIK dari BRIDA dan perbedaan dengan audit keamanan siber dari BSSN
	Improvement	1	Upaya perbaikan terjadi setelah ada masalah, belum menjadi siklus pembelajaran organisasi yang	Partial	ID.IM	Wawancara i2,i3 tentang uji coba AI gratis pada server sebagai inisiatif belajar mandiri

			terdokumentasi dan berkelanjutan			
Protect	Identity Management, Authentication, and Access Control	1	Pengelolaan akses masih bertumpu pada kebiasaan administratif seperti pergantian kata sandi, tanpa mekanisme otentikasi berlapis atau pengendalian akses adaptif yang memadai	Partial	PR.AA	Wawancara i2,i3 tentang kebiasaan OPD kadang mengganti password dan kerentanan website
	Awareness and Training	1	Edukasi dan pelatihan keamanan digital belum menjadi program rutin. Peningkatan kapasitas masih bergantung pada kegiatan eksternal seperti agenda BSSN di tingkat provinsi	Partial	PR.AT	Wawancara i1,i2,i3 tentang tidak ada pelatihan serta belum ada tindak lanjut setelah kegiatan BSSN
	Data Security	1	Backup data sudah dilakukan pada aplikasi tertentu, tetapi belum menyeluruh dan belum didukung mekanisme enkripsi maupun tata kelola perlindungan data yang kuat	Partial	PR.DS	Wawancara i2,i3 tentang backup ke Google Drive pada aplikasi tertentu dan belum ada mekanisme enkripsi tambahan
	Platform Security	1	Keamanan platform masih lemah karena masih ditemukan penggunaan perangkat lunak tidak berlisensi dan antivirus gratis, sehingga perlindungan terhadap malware dan eksploitasi belum optimal	Partial	PR.PS	Wawancara i2i3 tentang penggunaan Windows bajakan dan antivirus gratis karena keterbatasan anggaran
	Technology Infrastructure Resilience	2	Ada indikasi ketahanan infrastruktur melalui penggunaan router/firewall dan backup server, namun pengamanannya belum terencana secara menyeluruh	Risk-Informed	PR.IR	Wawancara i2.i3 tentang penggunaan Mikrotik/firewall, pembatasan akses, serta perlunya server dan IPS yang belum tersedia

			dan sangat bergantung pada konfigurasi manual			
Detect	Continuous Monitoring	1	Monitoring belum berjalan secara real-time dan berkelanjutan	Partial	DE.CM	Wawancara i1,i2,i3 tentang website baru diketahui bermasalah setelah iklan judi online muncul dan tidak ada monitoring real-time
	Adverse Event Analysis	1	Deteksi ancaman masih manual dan belum berbasis sistem otomatis	Partial	DE.AE	Wawancara i2,i3 tentang belum adanya prosedur formal analisis kejadian tidak normal dan belum terintegrasi dengan threat intelligence
Respond	Incident Management	2	Tim tanggap insiden siber telah dibentuk, tetapi kerja operasionalnya masih sebatas dokumen sehingga belum menjadi struktur respons yang benar-benar aktif	Risk-Informed	RS.MA	Wawancara i1,i2,i3 tentang pembentukan TTIS/CSIRT baru sebatas SK dan belum ditindaklanjuti
	Incident Analysis	1	Analisis insiden belum dilakukan secara mendalam, hanya perspektif pegawai	Partial	RS.AN	Wawancara i1 tentang insiden dibersihkan oleh pusat dan belum ada kemampuan analisis insiden internal
	Incident Response Reporting and Communication	1	Pelaporan dan komunikasi insiden belum memiliki SOP yang jelas	Partial	RS.CO	Wawancara i1 tentang belum adanya mekanisme pelaporan baku dan komunikasi insiden masih bergantung pada koordinasi ad hoc
	Incident Mitigation	1	Mitigasi dilakukan secara reaktif setelah insiden terjadi, (pembersihan website dan bantuan pusat), belum melalui respons yang terstandar	Partial	RS.MI	Wawancara i1,i2,i3 tentang pembersihan website oleh Kemenkomdigi pusat sebagai bentuk mitigasi reaktif
Recover	Incident Recovery Plan Execution	2	Pemulihan sistem dilakukan melalui backup dan	Risk-Informed	RC.RP	Wawancara i2,i3 tentang backup data pada aplikasi tertentu

		penggantian server, tetapi belum didukung rencana pemulihan yang teruji			dan dampak insiden PDNS terhadap hilangnya data Minut
Incident Recovery Communication	1	Komunikasi dan evaluasi pemulihan belum terstruktur	Partial	RC.CO	Wawancara i1,i2,i3 tentang BSSN yang memberi informasi saat insiden dan belum adanya mekanisme komunikasi pemulihan formal

Sumber: Hasil pengolahan data riset 2026

1. **Govern**

Diskominfosan Minut telah memiliki modal tata kelola berupa dokumen Renstra 2025-2029, LKJIP, Perbup SPBE, dan Keputusan Bupati yang memuat klausul manajemen risiko. Namun, berdasarkan wawancara dengan Kepala Bidang Persandian (i1), kebijakan teknis keamanan siber yang spesifik dan operasional belum tersusun, anggaran keamanan digital sangat terbatas (±Rp10 juta/tahun), dan belum ada kerja sama (MoU) dengan pihak ketiga. Pimpinan daerah juga dinilai kurang menyoroti isu keamanan digital sehingga komitmen kelembagaan masih rendah. Fungsi Govern berada pada tingkat *Partial* menuju *Risk-Informed*.

2. **Identify**

Dinas telah mengetahui keberadaan aset digital (server, website, subdomain OPD, data perangkat daerah) yang tercantum dalam Keputusan Bupati Nomor 164 Tahun 2023 tentang Arsitektur SPBE. Namun, berdasarkan wawancara dengan Analisis Kebijakan Ahli Muda Bidang E-Government (i2,i3), klasifikasi aset berdasarkan kekritisan belum dilakukan dan penilaian risiko bersifat reaktif, hanya dilakukan setelah insiden terjadi. AI belum digunakan dalam proses identifikasi aset dan risiko. Fungsi *Identify* berada pada tingkat *Partial*. Temuan ini sejalan dengan Hossain et al. (2024b) dan Fauziyyah et al. (2025) yang menyoroti lemahnya manajemen risiko di pemerintah daerah.

3. **Protect**

Seluruh indikator *Protect* menunjukkan kondisi *Partial*. Pengelolaan akses masih manual (penggantian kata sandi berkala tanpa SOP). Pelatihan keamanan digital belum pernah dilaksanakan. Perlindungan data hanya berupa backup terbatas ke Google Drive untuk aplikasi tertentu. Keamanan platform belum optimal serta website minut.go.id pernah disusupi konten iklan judi online akibat lemahnya *platform hardening*. Infrastruktur hanya mengandalkan firewall berbasis Mikrotik gratis tanpa IDS/IPS. Tidak ada pemanfaatan teknologi AI dalam fungsi *Protect.* Temuan ini konsisten dengan Hossain et al. (2024b), Ferdynandus et al. (2024), dan Kurniati (2024) terkait tantangan keamanan siber di sektor publik.

4. **Detect**

Kemampuan deteksi Diskominfosan Minut sangat terbatas. Insiden penyusupan konten judi online pada website minut.go.id baru diketahui setelah pemberitahuan dari BSSN, bukan melalui sistem deteksi internal. Tidak ada sistem continuous monitoring, SIEM, atau teknologi anomaly detection berbasis AI. Analisis kejadian tidak normal juga belum dilakukan secara sistematis. Ini menggambarkan kondisi *Partial* yang jauh dari prinsip *proactive security posture dalam NIST CSF 2.0.* Gustina dan Ananda (2024) menegaskan bahwa integrasi AI dalam sistem SOAR dapat mengurangi waktu deteksi secara signifikan, namun hal ini belum diterapkan.

5. **Respond**

Tim Tanggap Insiden Siber (TTIS) telah dibentuk melalui SK Bupati, namun sebatas dokumen administratif dan belum aktif secara operasional. Analisis insiden tidak dilakukan secara mendalam, koordinasi bergantung sepenuhnya pada BSSN dan Kemenkomdig, dan belum ada SOP penanganan insiden yang terstruktur. Mitigasi yang dilakukan masih bersifat reaktif terkait pembersihan website, penggantian password, dan koordinasi dengan BSSN. Fungsi *Respond* berada pada tingkat *Partial* menuju *Risk-Informed*. Islam et al. (2025) menunjukkan bahwa integrasi AI dalam sistem manajemen insiden mampu menurunkan MTTD dan MTTR lebih dari 40%.

6. **Recover**

Upaya pemulihan seperti penggantian server, pembersihan website, dan backup data telah dilakukan, namun bersifat reaktif. Tidak tersedia *Disaster Recovery Plan* (DRP), SOP komunikasi pemulihan, dan evaluasi pasca-insiden. Ketergantungan pada bantuan pemerintah pusat masih dominan. Dampak insiden PDNS 2024 juga mengakibatkan hilangnya sejumlah data Diskominfosan Minut. Fungsi *Recover* berada pada tingkat *Partial* menuju *Risk-Informed*. Hal ini sejalan dengan Hossain et al. (2024b) yang menekankan kelemahan pemulihan insiden pada kebijakan siber pemerintah daerah.

3.2. Diskusi Temuan Utama Penelitian

Secara keseluruhan, kekuatan keamanan digital Diskominfosan Minut berada pada tingkat *Partial* hingga *Risk-Informed* berdasarkan *tier NIST CSF 2.0*. Kondisi ini menunjukkan adanya dasar kelembagaan dan kesadaran awal, namun implementasi belum konsisten dan *AI Cybersecurity* belum terintegrasi secara operasional. Temuan ini sejalan dengan Fauziyyah et al. (2025) yang menemukan disparitas antara adopsi AI dan kesiapan mitigasi risiko di pemerintahan Indonesia, serta Hossain et al. (2024b) yang menyoroti celah kritis pada kebijakan keamanan siber pemerintah daerah. Berbeda dengan Ferdynandus et al. (2024) pada sektor keuangan yang telah menerapkan *NIST CSF* lebih matang, pemerintah daerah menghadapi tantangan berupa keterbatasan anggaran, SDM, dan komitmen pimpinan. Kendala utama yang ditemukan adalah anggaran keamanan digital yang sangat rendah, minimnya kompetensi SDM di bidang keamanan siber, lemahnya kebijakan teknis, dan kurangnya dukungan dari pimpinan daerah.

3.3. Diskusi Temuan Menarik Lainnya

Penulis menemukan temuan menarik bahwa Diskominfosan Minut memiliki inisiatif uji coba AI secara mandiri dimana salah satu aparat pernah memasang *machine learning* berbasis data lokal (RPJMD) pada server, meskipun terkendala kapasitas RAM. Hal ini menunjukkan adanya potensi dan motivasi SDM yang perlu difasilitasi secara kelembagaan. Selain itu, ditemukan bahwa integrasi layanan digital dengan Pusat Data Nasional menciptakan ketergantungan yang tinggi, hal ini terlihat ketika PDNS terganggu, data dan layanan Diskominfosan Minut ikut terdampak tanpa adanya mekanisme *backup* mandiri yang memadai.

IV. KESIMPULAN

Penelitian ini menyimpulkan bahwa kekuatan keamanan digital Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara berada pada tingkat *Partial* hingga *Risk-Informed* berdasarkan *tier NIST CSF 2.0*. Seluruh fungsi *Govern, Identify, Protect, Detect, Respond*, dan *Recover* belum berjalan konsisten dan *AI Cybersecurity* belum terintegrasi secara operasional. Upaya peningkatan yang diperlukan mencakup:

1. penguatan kebijakan teknis keamanan siber yang operasional mengacu pada Peraturan BSSN Nomor 4 Tahun 2021 dan *NIST CSF 2.0*
2. pengembangan sistem inventarisasi dan klasifikasi aset digital berbasis risiko
3. implementasi autentikasi berlapis (MFA), penguatan keamanan platform, sistem *backup* terenkripsi, dan pengadaan *antivirus enterprise*
4. implementasi sistem SIEM dan *anomaly detection* berbasis AI
5. aktivasi operasional TTIS dengan SOP penanganan insiden yang terstruktur
6. penyusunan *Disaster Recovery Plan* dan *Business Continuity Plan*
7. pengembangan kapasitas SDM melalui pelatihan, sertifikasi, dan kolaborasi dengan perguruan tinggi. Disarankan agar Pemerintah Kabupaten Minahasa Utara mengalokasikan anggaran proporsional untuk keamanan digital dan menjadikan keamanan siber sebagai agenda strategis dalam RPJMD dan APBD.

Keterbatasan Penelitian.

Penelitian ini memiliki keterbatasan utama pada waktu dan biaya penelitian, serta hanya dilakukan pada satu dinas di satu kabupaten, sehingga temuan tidak dapat digeneralisasi langsung ke daerah lain.

Arah Masa Depan Penelitian (*future work*).

Penulis menyarankan agar dilakukan penelitian lanjutan pada beberapa dinas/instansi serupa di kabupaten/kota lain di Indonesia untuk memperoleh gambaran komparatif kekuatan keamanan digital pemerintah daerah berbasis *NIST CSF 2.0*, serta penelitian yang mengintegrasikan implementasi nyata *AI Cybersecurity* secara operasional.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih terutama ditujukan kepada Kepala Dinas Komunikasi Informatika dan Persandian Kabupaten Minahasa Utara beserta seluruh jajarannya, khususnya Kepala Bidang Persandian, Kepala Bidang E-Government, dan Analis Kebijakan Ahli Muda yang telah memberikan waktu dan informasi dalam pelaksanaan penelitian. Terima kasih juga kepada Ibu Rina Wahyuni, S.Kom., M.T.I selaku Dosen Pembimbing atas bimbingan dan arahan yang diberikan, serta seluruh pihak yang mendukung penyelesaian penelitian ini.

VI. DAFTAR PUSTAKA

Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data*, *7*. https://doi.org/10.3389/fdata.2024.1497535

Adhinugroho, D. S. (2024). *Analisis Tata Kelola Persandian Oleh Dinas Komunikasi Dan Informatika Untuk Peningkatan Sistem Keamanan Informasi Di Kabupaten Magetan Provinsi Jawa Timur* [(Institut Pemerintahan Dalam Negeri)]. http://eprints.ipdn.ac.id/id/eprint/18819

Agus Kurniati. (2024). Study of the Artificial Intelligence Role in Achieving Cybersecurity for Critical Information Infrastructure. *Monas: Jurnal Inovasi Aparatur*, *6*(2), 154–165. https://doi.org/10.54849/monas.v6i2.251

Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, *42*(1), 102000. https://doi.org/10.1016/j.giq.2024.102000

Fauziyyah, G., Maulana, I., Selamet, R., Catur, U., & Cendekia, I. (2025). Risk Security Cyber in System

AI -Based : Study Evaluative on Indonesian Government Digital Infrastructure. *Journal of Artificial Intelligence Research*, *1*(2), 80–89. https://doi.org/10.64910/jouair.v1i2.15

Ferdynandus, F., Natu Prihanto, J., & Winarno, W. (2024). Implementing NIST Framework and the People, Process, Technology approach in Indonesian Financial Services. *International Journal of Engineering Continuity*, *3*(1), 172–182. https://doi.org/10.58291/ijec.v3i1.265

Gaffur, B., & Fachry Fachrudin, M. (2023). Evaluasi Pengelolaan Persandian dalam Menjaga Keamanan Informasi Diskominfo dan Persandian Lombok Timur. *Jurnal Terapan Pemerintahan Minangkabau*, *3*(1), 28–41. https://doi.org/10.33701/jtpm.v3i1.3049

Gustina, V., & Ananda. (2024). Kecerdasan Buatan Untuk Security Orchestration Automation And Respond : Tinjauan Cakupan. *Jurnal Komputer Terapan*, *10*(1), 36–47. https://www.semanticscholar.org/reader/3650bc46c97cc5a1e6d4df3664f8e2f6837f1b5e

Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Hidayah, E. S., & Almadani, M. (2022). Analisis Tingkat Kematangan Sistem Pemerintahan Berbasis Elektronik (SPBE) pada Pemerintah Provinsi Sulawesi Selatan. *Jurnal Teknologi dan Komunikasi Pemerintahan*, *4*(2), 49–67. https://ejournal.ipdn.ac.id/JTKP/article/view/2680/1428

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024a). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences (Switzerland)*, *14*(13), 5501. https://doi.org/10.3390/app14135501

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024b). Understanding Local Government Cybersecurity Policy: A Concept Map and Framework. In *Information (Switzerland)* (Vol. 15, Nomor 6). mdpi.com. https://doi.org/10.3390/info15060342

Imran, M. F., Gunawan, H., & Asmoro, D. (2024). Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty. *Jurnal Manajemen Pelayanan Publik*, *8*(2), 275–290. https://doi.org/10.24198/jmpp.v8i2.52212

Islam, M. T., Mission, M. R., Refat, T. K., & ... (2025). Cybersecurity risk assessment frameworks for engineering databases: A systematic literature review. *... Data Management and ...*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5190444

Kilian, M. A., & Rudianto, H. (2024). *Analisis Keamanan Website Pemerintah Provinsi Maluku Menggunakan Metode Vulnerability*. http://eprints.ipdn.ac.id/id/eprint/19601

Nurochman, A., Astuti, E. Y., & Widianingtias, S. (2024). Analisis keamanan siber sistem informasi perpustakaan di Perpustakaan Universitas Jenderal Soedirman. *BACA: Jurnal Dokumentasi dan Informasi*, *45*(1), 49–64. https://doi.org/10.55981/j.baca.2024.1237

Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. *Jurnal Teknologi dan Komunikasi Pemerintahan*, *5*(2), 159–187. https://doi.org/10.33701/jtkp.v5i2.3735

Sarker, I. H. (2023). Multi-aspects AI -based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview . *Security and Privacy*, *6*(5), 1–26. https://doi.org/10.1002/spy2.295

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, *36*(September), 100520. https://doi.org/10.1016/j.jii.2023.100520

Setyasih, E. T. (2022). TRANSFORMASI DIGITAL PEMERINTAH DAERAH DI ERA SOCIETY 5.0: STUDI KASUS DI PROVINSI JAWA BARAT. *Jurnal Administrasi Publik*, *9*(2), 59–66. https://doi.org/10.54783/japp.v5i3.657

Tommy, S., Irwan, M., & Nasution, P. (2025). Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah : Studi Kasus Pusat Data Nasional (PDN). *Jurnal Ilmiah Ekonomi*

Dan Manajemen, *3*(6), 330–346. https://ejurnal.kampusakademik.co.id/index.php/jiem/article/view/5266/4577

Ulfa, A. R., Aprilia, E. F., Sanyoko, C. R., Lusianti, T. U., & Permatasari, R. (2023). Analisis Manajemen Risiko Menggunakan Framework NIST (Studi Kasus: PT. BRI Kc Surabaya Kusuma Bangsa). *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, *3*(1), 563–570. https://doi.org/10.33005/sitasi.v3i1.345

White, G. B., & Sjelin, N. (2021). The NIST Cybersecurity Framework. In *Research Anthology on Business Aspects of Cybersecurity* (Vol. 61, Nomor 1–2). https://doi.org/10.4018/978-1-6684-3698-1.ch003

Wiredarme. (2025). *Tanggung Jawab Konstitusional Negara terhadap Perlindungan Data Pribadi Warga dalam Penyelenggaraan Pemerintahan Digital*. *02*(1), 17–30. https://ejournal.ipdn.ac.id/jpa/article/view/6233/2429

Woods, D. W., & Seymour, S. (2023). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. *Journal of Cyber Policy*, *8*(3), 365–383. https://doi.org/10.1080/23738871.2024.2335461