AUDIT KEAMANAN SISTEM PENGELOLAAN DATA DI DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL BENGKULU UTARA MENGGUNAKAN FRAMEWORK NIST (NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY)

Annisa Rahmadhani DM[1], Muhammad Tosan Bingamawa[2]
[1,2]Institut Pemerintahan Dalam Negeri
[1]annisa.rdm@gmail.com, [2]tossan@ipdn.ac.id

ABSTRACT

This study aims to analyze the security level of the population data management system at the Department of Population and Civil Registration of North Bengkulu Regency using the NIST Cybersecurity Framework 2.0. This study employed a descriptive quantitative approach with 44 respondents selected through purposive sampling. Data were collected using a closed-ended questionnaire consisting of 25 items based on six NIST CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover. The data were analyzed using descriptive statistics by calculating the average score and percentage of each function, then classifying the results into Implementation Tiers. The results show that all functions are in the Repeatable category. The Protect function obtained the highest score of 3.2 or 64%, followed by Govern at 3.1 or 62%, Identify at 3.0 or 60%, Detect at 2.8 or 56%, Respond at 2.7 or 54%, and Recover at 2.6 or 52%. These findings indicate that technical protection, system maintenance, database security, and basic governance have been implemented consistently. However, detection, incident response, and recovery functions remain less optimal. Therefore, the Department of Population and Civil Registration of North Bengkulu Regency needs to strengthen detection procedures, incident response mechanisms, disaster recovery planning, and employee capacity to ensure more secure, reliable, and sustainable protection of population data.

Keywords: Cybersecurity; Population Data; NIST CSF 2.0; Security Audit; Public Service

ABSTRAK

Penelitian ini bertujuan untuk menganalisis tingkat keamanan sistem pengelolaan data kependudukan pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menggunakan NIST Cybersecurity Framework 2.0. Penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan jumlah responden sebanyak 44 orang yang ditentukan melalui teknik purposive sampling. Data dikumpulkan menggunakan kuesioner tertutup yang terdiri atas 25 butir pertanyaan berdasarkan enam fungsi NIST CSF 2.0, yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. Data dianalisis menggunakan statistik deskriptif dengan menghitung rata-

rata skor dan persentase setiap fungsi, kemudian diklasifikasikan ke dalam kategori Implementation Tiers. Hasil penelitian menunjukkan bahwa seluruh fungsi berada pada kategori Repeatable. Fungsi Protect memperoleh capaian tertinggi sebesar 3,2 atau 64%, disusul Govern sebesar 3,1 atau 62%, Identify sebesar 3,0 atau 60%, Detect sebesar 2,8 atau 56%, Respond sebesar 2,7 atau 54%, dan Recover sebesar 2,6 atau 52%. Temuan ini menunjukkan bahwa perlindungan teknis, pemeliharaan sistem, pengamanan basis data, dan tata kelola dasar telah berjalan cukup konsisten. Namun, fungsi deteksi, respons insiden, dan pemulihan masih belum optimal. Oleh karena itu, Disdukcapil Kabupaten Bengkulu Utara perlu memperkuat prosedur deteksi, mekanisme respons insiden, perencanaan pemulihan, dan kapasitas pegawai agar perlindungan data kependudukan berjalan lebih aman, andal, dan berkelanjutan.

Kata Kunci: *Keamanan Siber; Data Kependudukan; NIST CSF 2.0; Audit Keamanan; Pelayanan Publik*

A. Pendahuluan

Pemerintah memiliki tanggung jawab utama dalam menyelenggarakan pelayanan publik, pembangunan, dan pemberdayaan masyarakat secara terarah melalui sistem administrasi yang tertib dan dapat dipertanggungjawabkan (Ndraha, 2003). Dalam perkembangan tata kelola modern, pelayanan publik tidak lagi hanya bertumpu pada proses manual, tetapi juga menuntut pemanfaatan teknologi informasi untuk meningkatkan efisiensi, transparansi, dan kualitas layanan pemerintahan (Indrajit, 2016). Pemanfaatan teknologi dalam pemerintahan kemudian mendorong lahirnya e-government sebagai bentuk interaksi baru antara pemerintah, masyarakat, dunia usaha, dan lembaga lain melalui sistem berbasis elektronik (Saputra Rambe & Oktalisa, 2021). Transformasi tersebut diperkuat melalui kebijakan Sistem Pemerintahan Berbasis Elektronik yang menekankan pentingnya integrasi layanan, keamanan informasi, dan keberlanjutan sistem digital pemerintahan (Peraturan Presiden Nomor 95 Tahun 2018).

Penerapan e-government dalam sektor administrasi kependudukan memiliki posisi strategis karena data penduduk menjadi dasar bagi pelayanan publik, perencanaan pembangunan, pemberian bantuan sosial, dan penyusunan kebijakan daerah (Undang-Undang Nomor 24 Tahun 2013). Data kependudukan juga termasuk data pribadi yang

memuat identitas, karakteristik, dan informasi sensitif warga negara sehingga pengelolaannya harus dilakukan secara hati-hati dan terlindungi (Undang-Undang Nomor 27 Tahun 2022). Dalam konteks sistem informasi, data yang akurat, terjaga, dan terstruktur merupakan bahan utama dalam menghasilkan informasi yang dapat digunakan untuk pengambilan keputusan organisasi (Jogiyanto H.M., 2018). Oleh sebab itu, instansi pengelola data kependudukan wajib memastikan bahwa sistem yang digunakan mampu menjaga kerahasiaan, keutuhan, ketersediaan, dan akuntabilitas data masyarakat (Whitman & Mattord, 2023).

Dinas Kependudukan dan Pencatatan Sipil menjadi salah satu instansi pemerintah daerah yang memiliki peran langsung dalam pengelolaan data kependudukan dan penerbitan dokumen administrasi bagi masyarakat (Permendagri Nomor 102 Tahun 2019). Di Kabupaten Bengkulu Utara, Disdukcapil mengelola data penduduk yang terus bertambah seiring dinamika jumlah penduduk dan kebutuhan pelayanan administrasi kependudukan yang semakin kompleks . Kondisi ini menuntut dukungan infrastruktur teknologi informasi yang memadai agar proses perekaman, penyimpanan, pemutakhiran, dan pemanfaatan data dapat berjalan aman serta berkelanjutan (Stallings, 2022). Apabila pengelolaan data tidak diimbangi dengan sistem keamanan yang kuat, maka risiko kebocoran, penyalahgunaan akses, gangguan layanan, dan kehilangan data dapat meningkat secara signifikan (Tipton & Krause, 2022).

Keamanan data kependudukan semakin penting karena layanan administrasi penduduk saat ini bergantung pada sistem elektronik, perangkat perekaman biometrik, jaringan, server, dan basis data yang saling terhubung (Jogiyanto H.M., 2018). Penyelenggara sistem elektronik wajib menjalankan sistem secara andal, aman, dan bertanggung jawab agar informasi elektronik yang dikelola tidak disalahgunakan oleh pihak yang tidak berwenang (Undang-Undang Nomor 11 Tahun 2008). Perlindungan data pribadi juga mengharuskan pengendali data menerapkan prinsip keamanan, akurasi, transparansi, dan

pembatasan penggunaan data sesuai ketentuan hukum yang berlaku (Undang-Undang Nomor 27 Tahun 2022). Dengan demikian, pengelolaan data kependudukan tidak cukup hanya berorientasi pada kelancaran pelayanan, tetapi juga harus memperhatikan kepatuhan hukum dan ketahanan keamanan siber (Von Solms & Van Niekerk, 2021).

Regulasi nasional telah memberikan dasar yang jelas bagi penguatan keamanan informasi dalam penyelenggaraan administrasi kependudukan digital (Peraturan Presiden Nomor 82 Tahun 2022). Permendagri Nomor 72 Tahun 2022 secara tegas menyebutkan bahwa keamanan Identitas Kependudukan Digital harus berpedoman pada standar internasional, termasuk International Organization for Standardization/International Electrotechnical Commission dan National Institute of Standards and Technology (Permendagri Nomor 72 Tahun 2022). Ketentuan tersebut menunjukkan bahwa keamanan data kependudukan harus dikelola melalui standar yang sistematis, terukur, dan dapat diaudit secara berkala (Ross & Pillitteri, 2024). Selain itu, audit teknologi informasi dan komunikasi dalam penyelenggaraan pemerintahan digital diperlukan untuk menilai efektivitas tata kelola, keamanan, infrastruktur, aplikasi, dan layanan SPBE (Peraturan Menteri Komunikasi dan Informatika Nomor 16 Tahun 2022).

Namun, penguatan regulasi belum selalu diikuti oleh pelaksanaan audit keamanan secara optimal pada tingkat pemerintah daerah (Fadila et al., 2023). Dalam konteks Kabupaten Bengkulu Utara, Peraturan Bupati Nomor 31 Tahun 2023 telah memuat arah arsitektur SPBE, tetapi pelaksanaan audit keamanan SPBE masih menjadi aspek yang perlu diperkuat (Peraturan Bupati Bengkulu Utara Nomor 31 Tahun 2023). Kondisi tersebut memperlihatkan adanya kesenjangan antara tuntutan regulasi keamanan informasi dan praktik pengendalian keamanan sistem pada perangkat daerah (Muthi'atur Rofi'ah, 2025). Kesenjangan ini perlu diperhatikan karena Disdukcapil mengelola data yang bersifat sensitif, bernilai strategis, dan berisiko tinggi apabila mengalami kebocoran atau penyalahgunaan (Rahman et al., 2025).

Audit keamanan sistem informasi diperlukan untuk menilai apakah pengendalian keamanan telah berjalan sesuai standar, kebijakan, dan kebutuhan organisasi (Hamzah, 2018). Audit juga berfungsi sebagai proses evaluatif untuk mengidentifikasi kelemahan sistem, menilai tingkat risiko, dan menghasilkan rekomendasi perbaikan yang dapat mendukung peningkatan keamanan berkelanjutan (Gimnastiar & Nursyanti, 2024). Dalam tata kelola keamanan informasi, proses audit tidak hanya menilai aspek teknis, tetapi juga mencakup kebijakan, sumber daya manusia, prosedur, pengawasan, dan respons organisasi terhadap insiden (Whitman & Mattord, 2023). Oleh karena itu, audit pada sistem pengelolaan data kependudukan penting dilakukan agar Disdukcapil dapat mengetahui posisi keamanan aktual dan menentukan prioritas peningkatan yang paling relevan (Handoyo & Nigrum, 2024).

Salah satu kerangka kerja yang dapat digunakan untuk audit keamanan sistem pengelolaan data adalah NIST Cybersecurity Framework 2.0 (Moore, 2024). NIST CSF 2.0 menyediakan pendekatan berbasis risiko yang fleksibel melalui enam fungsi utama, yaitu Govern, Identify, Protect, Detect, Respond, dan Recover (Ross & Pillitteri, 2024). Fungsi Govern menekankan tata kelola, kebijakan, peran, tanggung jawab, dan pengawasan risiko siber organisasi (Raimondo, 2024). Fungsi Identify, Protect, Detect, Respond, dan Recover membantu organisasi mengenali aset dan risiko, menerapkan perlindungan, mendeteksi ancaman, merespons insiden, serta memulihkan layanan setelah gangguan terjadi (Muthi'atur Rofi'ah, 2025).

Penggunaan NIST CSF dalam audit keamanan telah banyak diterapkan karena kerangka ini mampu memberikan gambaran sistematis mengenai kesiapan organisasi menghadapi risiko siber (Fadila et al., 2023). Penelitian sebelumnya menunjukkan bahwa penggunaan NIST dapat membantu organisasi menilai tingkat keamanan, mengidentifikasi risiko, dan merumuskan rekomendasi penguatan sistem informasi (Gimnastiar & Nursyanti, 2024). Kajian lain juga menegaskan bahwa NIST relevan digunakan pada berbagai konteks

organisasi karena mampu menyesuaikan kebutuhan keamanan dengan karakteristik risiko dan kapasitas institusi (Rahman et al., 2025). Dalam konteks Indonesia, penerapan NIST juga dinilai sesuai untuk memperkuat peran auditor internal dalam menilai tata kelola keamanan siber secara lebih terarah (Muthi'atur Rofi'ah, 2025).

Meskipun demikian, kajian mengenai audit keamanan sistem pengelolaan data kependudukan pada tingkat Disdukcapil daerah masih perlu dikembangkan secara lebih spesifik (Hamzah, 2018). Sebagian penelitian terdahulu lebih banyak berfokus pada sistem e-learning, sistem absensi, perguruan tinggi, atau perbandingan framework keamanan jaringan, sehingga belum sepenuhnya menjawab kebutuhan audit pada data kependudukan daerah (Handoyo & Nigrum, 2024). Padahal, sistem pengelolaan data kependudukan memiliki karakteristik berbeda karena menyangkut data pribadi, kewajiban pelayanan publik, kepatuhan terhadap regulasi administrasi kependudukan, serta keterhubungan dengan sistem nasional (Permendagri Nomor 102 Tahun 2019). Oleh karena itu, audit keamanan berbasis NIST CSF 2.0 pada Disdukcapil Kabupaten Bengkulu Utara menjadi penting untuk mengukur tingkat implementasi keamanan sistem secara lebih kontekstual dan operasional (Moore, 2024).

Berdasarkan uraian tersebut, penelitian ini difokuskan pada audit keamanan sistem pengelolaan data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menggunakan framework NIST CSF 2.0 (Ross & Pillitteri, 2024). Fokus ini dipilih karena Disdukcapil memiliki tanggung jawab besar dalam menjaga keamanan data kependudukan sebagai bagian dari pelayanan publik berbasis digital (Undang-Undang Nomor 24 Tahun 2013). Penelitian ini juga diarahkan untuk mengetahui tingkat keamanan sistem berdasarkan fungsi Govern, Identify, Protect, Detect, Respond, dan Recover agar dapat memberikan gambaran objektif mengenai kekuatan dan kelemahan pengelolaan keamanan data (Raimondo, 2024). Hasil penelitian diharapkan dapat menjadi dasar rekomendasi bagi Disdukcapil Kabupaten Bengkulu Utara dalam memperkuat tata kelola keamanan

informasi, menutup kesenjangan kepatuhan, dan meningkatkan perlindungan data masyarakat secara berkelanjutan (Peraturan Bupati Bengkulu Utara Nomor 31 Tahun 2023).

B. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif deskriptif untuk mengukur tingkat keamanan sistem pengelolaan data kependudukan pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara. Pendekatan ini digunakan karena penelitian berfokus pada pengukuran kondisi aktual keamanan sistem berdasarkan skor numerik dari responden, kemudian hasilnya dideskripsikan sesuai fungsi dalam NIST Cybersecurity Framework 2.0. Materi yang diteliti adalah keamanan sistem pengelolaan data kependudukan yang mencakup aspek tata kelola risiko, identifikasi aset, perlindungan data, deteksi ancaman, respons insiden, dan pemulihan layanan.

Rancangan Penelitian

Penelitian dilaksanakan melalui beberapa tahapan operasional. Tahap pertama adalah mengidentifikasi permasalahan keamanan sistem pengelolaan data kependudukan di Disdukcapil Kabupaten Bengkulu Utara berdasarkan kondisi infrastruktur, regulasi, dan kebutuhan perlindungan data. Tahap kedua adalah menentukan kerangka audit yang digunakan, yaitu NIST CSF 2.0 dengan enam fungsi utama, yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. Tahap ketiga adalah menyusun instrumen kuesioner berdasarkan indikator pada setiap fungsi NIST CSF 2.0. Tahap keempat adalah melakukan uji validitas dan reliabilitas instrumen sebelum kuesioner digunakan sebagai alat pengumpulan data. Tahap kelima adalah menyebarkan kuesioner kepada responden yang telah ditentukan. Tahap keenam adalah mengolah data menggunakan statistik deskriptif melalui perhitungan skor rata-rata dan persentase capaian. Tahap ketujuh adalah mengklasifikasikan hasil pengukuran ke dalam kategori Implementation Tiers, yaitu Partial, Risk-Informed, Repeatable, dan Adaptive.

Subjek, Lokasi, Waktu, dan Sampel Penelitian

Penelitian dilakukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara yang beralamat di Jalan Jenderal Sudirman Nomor 01, Kelurahan Gunung Alam, Kecamatan Kota Arga Makmur, Kabupaten Bengkulu Utara, Provinsi Bengkulu. Lokasi ini dipilih karena Disdukcapil merupakan instansi pemerintah daerah yang mengelola data kependudukan, dokumen administrasi kependudukan, serta sistem layanan berbasis data yang memiliki tingkat sensitivitas tinggi.

Subjek penelitian adalah pegawai Disdukcapil Kabupaten Bengkulu Utara yang terlibat dalam pelayanan, pengelolaan, pemanfaatan, dan pengamanan data kependudukan. Populasi penelitian mengacu pada pegawai aktif di lingkungan Disdukcapil Kabupaten Bengkulu Utara. Sampel penelitian berjumlah 44 orang, yang terdiri atas pegawai berstatus ASN dan P3K/PPPK yang berkaitan langsung dengan kegiatan administrasi kependudukan, pengolahan data, pelayanan pendaftaran penduduk, pencatatan sipil, pengelolaan informasi administrasi kependudukan, serta pemanfaatan data dan inovasi pelayanan.

Teknik penentuan sampel menggunakan purposive sampling. Teknik ini dipilih karena tidak semua pegawai memiliki keterlibatan langsung dengan sistem pengelolaan data kependudukan. Responden dipilih berdasarkan pertimbangan bahwa mereka memahami proses pelayanan, penggunaan perangkat, akses sistem, pengelolaan data, serta prosedur kerja yang berkaitan dengan keamanan sistem di Disdukcapil. Pengumpulan data utama dilakukan melalui kuesioner yang diisi oleh responden pada masa penelitian di lingkungan Disdukcapil Kabupaten Bengkulu Utara.

Instrumen dan Teknik Pengumpulan Data

Instrumen utama penelitian berupa kuesioner tertutup yang disusun berdasarkan enam fungsi dalam NIST CSF 2.0. Kuesioner terdiri atas 25 butir pertanyaan yang dibagi ke dalam enam fungsi, yaitu Govern sebanyak 6 butir, Identify sebanyak 3 butir, Protect sebanyak 5 butir, Detect sebanyak 4 butir, Respond sebanyak 4 butir, dan Recover sebanyak 3 butir.

Setiap butir pertanyaan diarahkan untuk mengukur kondisi implementasi keamanan sistem pengelolaan data kependudukan berdasarkan indikator operasional pada masing-masing fungsi.

Skala pengukuran menggunakan skala Likert 1–5. Skor 1 menunjukkan bahwa aspek keamanan belum ada atau belum pernah dijalankan. Skor 2 menunjukkan bahwa aspek keamanan sudah ada dan sudah dijalankan, tetapi belum optimal. Skor 3 menunjukkan bahwa aspek keamanan sudah ada dan berjalan sesuai prosedur. Skor 4 menunjukkan bahwa aspek keamanan sudah dilaksanakan dan dievaluasi secara berkala. Skor 5 menunjukkan bahwa aspek keamanan sudah dilaksanakan secara matang dan berkelanjutan.

Teknik pengumpulan data dilakukan melalui kuesioner online menggunakan Google Form. Kuesioner diberikan kepada responden yang telah ditentukan sesuai kriteria sampel. Selain kuesioner, penelitian juga menggunakan dokumentasi sebagai data pendukung, seperti data kelembagaan Disdukcapil, jumlah pegawai, kondisi infrastruktur teknologi informasi, regulasi terkait pengelolaan data kependudukan, dan dokumen pendukung lain yang relevan dengan audit keamanan sistem.

Validasi instrumen dilakukan melalui uji validitas dan uji reliabilitas. Uji validitas dilakukan dengan membandingkan nilai r hitung setiap butir pertanyaan dengan r tabel sebesar 0,355. Butir pertanyaan dinyatakan valid apabila nilai r hitung lebih besar daripada r tabel. Uji reliabilitas dilakukan menggunakan Cronbach’s Alpha untuk melihat konsistensi jawaban pada setiap fungsi NIST CSF 2.0. Hasil reliabilitas menunjukkan nilai Cronbach’s Alpha pada fungsi Govern sebesar 0,506, Identify sebesar 0,548, Protect sebesar 0,615, Detect sebesar 0,619, Respond sebesar 0,630, dan Recover sebesar 0,620. Berdasarkan nilai tersebut, instrumen dinilai cukup konsisten dan dapat digunakan untuk mengukur tingkat keamanan sistem pengelolaan data kependudukan.

Teknik Analisis Data

Data dianalisis menggunakan statistik deskriptif kuantitatif. Setiap

jawaban responden diberi skor sesuai skala Likert 1–5. Skor dari setiap butir pertanyaan kemudian dijumlahkan untuk memperoleh total nilai pada masing-masing indikator. Setelah itu, nilai rata-rata dihitung dengan membagi total skor dengan jumlah responden. Perhitungan ini digunakan untuk mengetahui tingkat implementasi keamanan pada setiap indikator NIST CSF 2.0.

Analisis dilakukan secara bertahap pada setiap fungsi. Pada fungsi Govern, analisis diarahkan untuk menilai konteks organisasi, strategi manajemen risiko, peran dan tanggung jawab, kebijakan keamanan siber, pengelolaan risiko pihak ketiga, dan pengawasan. Pada fungsi Identify, analisis digunakan untuk menilai inventarisasi aset, tata kelola keamanan, dan identifikasi risiko. Pada fungsi Protect, analisis diarahkan untuk menilai pengelolaan identitas dan akses, perlindungan data, prosedur perlindungan informasi, pemeliharaan sistem, dan teknologi pelindung. Pada fungsi Detect, analisis digunakan untuk menilai pemantauan berkelanjutan, analisis kejadian, pengawasan aktivitas pihak eksternal, dan proses deteksi. Pada fungsi Respond, analisis digunakan untuk menilai perencanaan respons, komunikasi insiden, mitigasi, dan perbaikan setelah insiden. Pada fungsi Recover, analisis digunakan untuk menilai perencanaan pemulihan, perbaikan pemulihan, dan komunikasi selama proses pemulihan.

Nilai rata-rata setiap fungsi kemudian dikonversi ke dalam persentase dengan rumus:

Persentase capaian = (rata-rata skor / 5) × 100%

Hasil persentase tersebut diklasifikasikan ke dalam kategori Implementation Tiers. Persentase 0–25% dikategorikan sebagai Partial, yaitu keamanan masih bersifat reaktif dan belum memiliki standar yang jelas. Persentase 26–50% dikategorikan sebagai Risk-Informed, yaitu organisasi sudah mengenali risiko tetapi penerapannya belum konsisten. Persentase 51–75% dikategorikan sebagai Repeatable, yaitu proses keamanan sudah berjalan, terdokumentasi secara dasar, dan dilakukan secara rutin. Persentase 76–100% dikategorikan sebagai Adaptive, yaitu keamanan

sudah menyesuaikan perubahan ancaman dan menjadi bagian dari budaya organisasi.

Melalui teknik analisis tersebut, penelitian ini menghasilkan gambaran kuantitatif mengenai tingkat keamanan sistem pengelolaan data kependudukan di Disdukcapil Kabupaten Bengkulu Utara berdasarkan enam fungsi NIST CSF 2.0. Hasil analisis digunakan untuk menentukan fungsi yang paling kuat, fungsi yang masih lemah, serta aspek yang membutuhkan rekomendasi perbaikan agar keamanan data kependudukan dapat ditingkatkan secara berkelanjutan.

C. Hasil Penelitian dan Pembahasan

Hasil Penelitian

Hasil penelitian ini diperoleh dari pengolahan data kuesioner audit keamanan sistem pengelolaan data kependudukan pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara. Kuesioner disusun berdasarkan enam fungsi utama **NIST Cybersecurity Framework 2.0**, yaitu **Govern, Identify, Protect, Detect, Respond, dan Recover**. Setiap indikator dinilai menggunakan skala Likert 1–5, kemudian dihitung nilai rata-rata, persentase capaian, dan kategori **Implementation Tiers**. Hasil skripsi menunjukkan bahwa seluruh fungsi keamanan berada pada kategori **Repeatable**, dengan fungsi **Protect** memperoleh capaian tertinggi sebesar **3,2 atau 64%**, sedangkan fungsi **Recover** memperoleh capaian terendah sebesar **2,6 atau 52%** .

Secara umum, hasil audit menunjukkan bahwa sistem keamanan pengelolaan data kependudukan di Disdukcapil Kabupaten Bengkulu Utara sudah memiliki dasar pengendalian keamanan yang berjalan cukup konsisten. Hal tersebut terlihat dari seluruh fungsi NIST CSF 2.0 yang berada pada rentang 51%–75%, sehingga termasuk dalam kategori Repeatable. Kategori ini menunjukkan bahwa proses keamanan sudah dilaksanakan secara berulang dan cukup dikenal oleh organisasi, tetapi belum sepenuhnya matang, terukur, adaptif, dan terintegrasi secara menyeluruh.

Tabel 1. Rekapitulasi Hasil Audit Keamanan Berdasarkan Fungsi NIST CSF 2.0

No.	Fungsi NIST CSF 2.0	Rata-Rata Skor	Persentase	Kategori Tiers	Urutan Capaian
1	Govern	3,1	62%	Repeatable	2
2	Identify	3,0	60%	Repeatable	3
3	Protect	3,2	64%	Repeatable	1
4	Detect	2,8	56%	Repeatable	4
5	Respond	2,7	54%	Repeatable	5
6	Recover	2,6	52%	Repeatable	6

Berdasarkan tabel tersebut, fungsi Protect menjadi aspek dengan capaian paling tinggi, yaitu 3,2 atau 64%. Hasil ini menunjukkan bahwa aspek perlindungan sistem, data, akses, pemeliharaan, dan teknologi pelindung sudah relatif lebih kuat dibandingkan fungsi lainnya. Fungsi Govern berada pada urutan kedua dengan skor 3,1 atau 62%, yang menunjukkan bahwa tata kelola keamanan, kebijakan, peran pimpinan, dan pengawasan risiko sudah mulai berjalan. Fungsi Identify memperoleh skor 3,0 atau 60%, yang berarti proses identifikasi aset, tata kelola, dan risiko telah dilaksanakan, tetapi masih membutuhkan pemetaan yang lebih sistematis.

Fungsi Detect, Respond, dan Recover menjadi tiga fungsi dengan capaian paling rendah. Fungsi Detect memperoleh skor 2,8 atau 56%, yang menunjukkan bahwa proses deteksi kejadian keamanan sudah ada, tetapi belum optimal. Fungsi Respond memperoleh skor 2,7 atau 54%, yang berarti kesiapan organisasi dalam merespons insiden keamanan masih memerlukan penguatan. Fungsi Recover memperoleh skor 2,6 atau 52%, sehingga menjadi fungsi paling rendah dan menunjukkan bahwa aspek pemulihan sistem, evaluasi pemulihan, serta komunikasi saat pemulihan masih menjadi kelemahan utama.

Hasil Audit Fungsi Govern

Fungsi Govern digunakan untuk menilai tata kelola keamanan siber pada Disdukcapil Kabupaten Bengkulu Utara. Fungsi ini mencakup pemahaman konteks organisasi, strategi manajemen risiko, pembagian peran dan tanggung jawab, kebijakan keamanan siber, pengelolaan risiko

kerja sama pihak luar, serta pengawasan. Hasil pengukuran menunjukkan bahwa fungsi Govern memperoleh rata-rata skor 3,1 dengan persentase 62% dan termasuk kategori Repeatable.

Tabel 2. Hasil Audit Fungsi Govern

No.	Indikator	Skala 1	Skala 2	Skala 3	Skala 4	Skala 5	Jumlah Responden	Jumlah Nilai	Rata-Rata	Persentase	Tiers
1	Organizational Context	10	9	9	7	9	44	128	2,9	58%	Repeatable
2	Risk Management Strategy	9	10	9	6	10	44	130	2,9	58%	Repeatable
3	Roles, Responsibilities, and Authorities	8	8	10	8	10	44	136	3,1	62%	Repeatable
4	Cybersecurity Policy Implemented	9	7	7	11	10	44	138	3,1	62%	Repeatable
5	Cybersecurity Supply Chain Risk Managed	6	11	10	8	9	44	135	3,1	62%	Repeatable
6	Oversight	10	6	11	6	11	44	134	3,0	60%	Repeatable

Hasil pada fungsi Govern menunjukkan bahwa indikator dengan capaian tertinggi berada pada aspek Roles, Responsibilities, and Authorities, Cybersecurity Policy Implemented, dan Cybersecurity Supply Chain Risk Managed, masing-masing memperoleh skor rata-rata 3,1 atau 62%. Artinya, Disdukcapil telah memiliki dasar pembagian peran, kebijakan keamanan, dan pengawasan risiko kerja sama dengan pihak luar, meskipun belum sepenuhnya optimal. Indikator Oversight memperoleh skor 3,0 atau 60%, yang menunjukkan bahwa pengawasan terhadap pengelolaan risiko sudah dilakukan, tetapi masih perlu diperkuat melalui evaluasi yang lebih rutin dan terdokumentasi.

Indikator dengan capaian lebih rendah adalah Organizational Context dan Risk Management Strategy, masing-masing dengan skor 2,9 atau 58%. Hasil ini menunjukkan bahwa pemahaman terhadap visi, misi, tujuan organisasi, dan strategi pengelolaan risiko keamanan belum sepenuhnya merata pada seluruh pegawai. Dengan demikian, fungsi Govern sudah berada pada kategori cukup baik, tetapi masih membutuhkan penguatan pada aspek perencanaan risiko, komunikasi kebijakan, dan pengawasan keamanan secara lebih formal.

Hasil Audit Fungsi Identify

Fungsi Identify digunakan untuk menilai kemampuan organisasi dalam mengenali aset, kebijakan tata kelola, dan risiko yang berkaitan dengan sistem pengelolaan data kependudukan. Fungsi ini penting karena perlindungan sistem hanya dapat dilakukan secara tepat apabila organisasi mengetahui aset apa saja yang dimiliki, risiko apa yang dihadapi, serta kebijakan apa yang menjadi dasar pengelolaannya. Hasil pengukuran menunjukkan bahwa fungsi Identify memperoleh rata-rata skor 3,0 dengan persentase 60% dan termasuk kategori Repeatable.

Tabel 3. Hasil Audit Fungsi Identify

No.	Indikator	Skala 1	Skala 2	Skala 3	Skala 4	Skala 5	Jumlah Responden	Jumlah Nilai	Rata-Rata	Persentase	Tiers
1	Asset Management	9	7	9	9	10	44	136	3,1	68%	Repeatable
2	Governance	9	10	9	7	9	44	129	3,0	60%	Repeatable
3	Risk Assessment	10	10	8	8	8	44	126	2,9	58%	Repeatable

Hasil pada fungsi Identify menunjukkan bahwa indikator Asset Management memperoleh capaian tertinggi dengan rata-rata 3,1 dan persentase 68%. Hal ini menunjukkan bahwa inventarisasi aset teknologi informasi, seperti server, basis data, aplikasi kependudukan, dan perangkat pendukung pelayanan, sudah cukup dikenal dan dijalankan oleh organisasi. Capaian ini menjadi tanda bahwa Disdukcapil telah memiliki dasar dalam mengenali aset penting yang digunakan dalam pengelolaan data kependudukan.

Indikator Governance memperoleh skor 3,0 atau 60%, yang menunjukkan bahwa kebijakan tata kelola keamanan data kependudukan sudah mulai diterapkan. Namun, capaian ini belum menunjukkan tingkat kematangan yang tinggi karena kebijakan yang ada masih perlu diperkuat dari sisi dokumentasi, sosialisasi, dan penerapan konsisten pada seluruh unit. Indikator Risk Assessment memperoleh skor terendah dalam fungsi Identify, yaitu 2,9 atau 58%. Hasil ini memperlihatkan bahwa proses identifikasi dan analisis risiko kebocoran atau penyalahgunaan data sudah dilakukan, tetapi belum cukup mendalam dan belum sepenuhnya

berbasis pemetaan risiko yang terstruktur.

Hasil Audit Fungsi Protect

Fungsi Protect digunakan untuk menilai sejauh mana Disdukcapil menerapkan perlindungan terhadap sistem, data, perangkat, akses pengguna, dan teknologi pendukung keamanan. Fungsi ini menjadi komponen penting karena berkaitan langsung dengan upaya pencegahan gangguan, pembatasan akses tidak sah, perlindungan basis data, serta pemeliharaan sistem. Hasil pengukuran menunjukkan bahwa fungsi Protect memperoleh rata-rata skor 3,2 dengan persentase 64% dan termasuk kategori Repeatable.

Tabel 4. Hasil Audit Fungsi Protect

No.	Indikator	Skala 1	Skala 2	Skala 3	Skala 4	Skala 5	Jumlah Responden	Jumlah Nilai	Rata-Rata	Persentase	Tiers
1	Identity Management and Access Control	6	7	12	13	6	44	138	3,1	68%	Repeatable
2	Protect Database	10	10	8	9	7	44	155	3,5	70%	Repeatable
3	Information Protection Process and Procedures	10	8	10	9	7	44	147	3,3	66%	Repeatable
4	Maintenance	3	4	14	11	12	44	157	3,6	72%	Repeatable
5	Protective Technology	2	11	15	10	6	44	139	3,1	68%	Repeatable

Hasil fungsi Protect menunjukkan bahwa indikator Maintenance memperoleh capaian tertinggi dengan skor rata-rata 3,6 atau 72%. Hasil ini menunjukkan bahwa perawatan sistem atau aplikasi kependudukan sudah cukup baik dan relatif lebih konsisten dibandingkan indikator lain. Indikator Protect Database memperoleh skor 3,5 atau 70%, yang menunjukkan bahwa perlindungan terhadap data kependudukan sudah cukup kuat, terutama pada aspek perlindungan data yang tersimpan.

Indikator Information Protection Process and Procedures memperoleh skor 3,3 atau 66%, yang menunjukkan bahwa prosedur perlindungan informasi sudah tersedia dan mulai dijalankan. Sementara itu, indikator Identity Management and Access

Control dan Protective Technology masing-masing memperoleh skor 3,1 atau 68%. Hasil tersebut menunjukkan bahwa pengelolaan akses pengguna dan pemanfaatan teknologi pelindung, seperti sistem keamanan perangkat dan jaringan, sudah berjalan, tetapi masih perlu ditingkatkan agar lebih matang dan berkelanjutan.

Secara keseluruhan, fungsi Protect menjadi fungsi dengan capaian terbaik dalam audit ini. Hal tersebut menandakan bahwa perlindungan teknis pada sistem pengelolaan data kependudukan sudah menjadi aspek yang paling kuat di Disdukcapil Kabupaten Bengkulu Utara. Meskipun demikian, karena seluruh indikator masih berada pada kategori Repeatable, maka perlindungan yang ada belum dapat dikategorikan adaptif terhadap ancaman siber yang terus berkembang.

Hasil Audit Fungsi Detect

Fungsi Detect digunakan untuk menilai kemampuan Disdukcapil dalam memantau aktivitas sistem, mengenali anomali, mengawasi aktivitas penyedia layanan eksternal, dan menjalankan proses deteksi kejadian keamanan. Fungsi ini berperan penting untuk memastikan potensi gangguan dapat diketahui sejak dini sebelum berkembang menjadi insiden yang lebih besar. Hasil pengukuran menunjukkan bahwa fungsi Detect memperoleh rata-rata skor 2,8 dengan persentase 56% dan termasuk kategori Repeatable.

Tabel 5. Hasil Audit Fungsi Detect

No.	Indikator	Skala 1	Skala 2	Skala 3	Skala 4	Skala 5	Jumlah Responden	Jumlah Nilai	Rata-Rata	Persentase	Tiers
1	Continuous Monitoring	1	10	9	12	12	44	156	3,5	70%	Repeatable
2	Adverse Event Analysis	4	4	8	15	13	44	161	3,6	70%	Repeatable
3	Continuous Monitoring of External Provider	1	6	22	9	6	44	145	3,3	66%	Repeatable
4	Detection Processes	4	15	15	3	7	44	126	2,9	58%	Repeatable

Hasil pada fungsi Detect menunjukkan bahwa indikator Adverse Event Analysis memperoleh skor tertinggi, yaitu 3,6 atau 70%. Hal ini menunjukkan bahwa kemampuan untuk mengenali dan menganalisis anomali akses data, seperti akses di luar jam kerja atau aktivitas tidak biasa, sudah cukup baik. Indikator Continuous Monitoring juga memperoleh capaian tinggi dengan skor 3,5 atau 70%, yang menunjukkan bahwa pemantauan aktivitas akses ke basis data kependudukan sudah dilakukan secara rutin.

Indikator Continuous Monitoring of External Provider memperoleh skor 3,3 atau 66%. Hasil ini menunjukkan bahwa aktivitas akses dan pemeliharaan sistem oleh penyedia layanan luar sudah diawasi, meskipun belum sepenuhnya kuat. Adapun indikator Detection Processes memperoleh skor paling rendah, yaitu 2,9 atau 58%. Hal ini memperlihatkan bahwa prosedur tertulis untuk mendeteksi kejadian keamanan belum sepenuhnya berjalan optimal.

Dengan demikian, fungsi Detect memperlihatkan kondisi yang cukup menarik. Beberapa aspek pemantauan dan analisis anomali sudah memiliki capaian baik, tetapi prosedur deteksi formal masih lemah. Artinya, aktivitas deteksi sudah dilakukan, tetapi belum sepenuhnya didukung oleh mekanisme baku, dokumentasi yang kuat, dan sistem deteksi yang terintegrasi.

Hasil Audit Fungsi Respond

Fungsi Respond digunakan untuk menilai kesiapan Disdukcapil dalam merespons insiden keamanan, termasuk perencanaan respons, komunikasi insiden, mitigasi dampak, dan perbaikan setelah insiden. Fungsi ini penting karena serangan atau gangguan keamanan tidak hanya harus dicegah, tetapi juga harus ditangani secara cepat dan terkoordinasi apabila terjadi. Hasil pengukuran menunjukkan bahwa fungsi Respond memperoleh rata-rata skor 2,7 dengan persentase 54% dan termasuk kategori Repeatable.

Tabel 6. Hasil Audit Fungsi Respond

No.	Indikator	Skala 1	Skala 2	Skala 3	Skala 4	Skala 5	Jumlah Responden	Jumlah Nilai	Rata-Rata	Persentase	Tiers
1	Response Planning	3	14	13	7	7	44	133	3,0	60%	Repeatable
2	Respond Communication	5	13	13	8	5	44	127	2,9	58%	Repeatable

3	Respond Mitigation	4	13	18	5	4	44	124	2,8	56%	Repeatable
4	Response Improvements	6	16	10	10	2	44	118	2,7	54%	Repeatable

Hasil fungsi Respond menunjukkan bahwa indikator Response Planning memperoleh capaian tertinggi dengan skor 3,0 atau 60%. Artinya, rencana tertulis untuk merespons insiden kebocoran data sudah mulai tersedia atau dipahami, tetapi masih belum sepenuhnya matang. Indikator Respond Communication memperoleh skor 2,9 atau 58%, yang menunjukkan bahwa mekanisme komunikasi resmi saat terjadi insiden sudah ada, tetapi belum cukup kuat untuk memastikan koordinasi berjalan cepat dan jelas.

Indikator Respond Mitigation memperoleh skor 2,8 atau 56%. Hasil ini menunjukkan bahwa strategi untuk menghentikan atau mengurangi dampak gangguan keamanan sudah mulai dilakukan, tetapi belum optimal. Indikator Response Improvements memperoleh skor terendah, yaitu 2,7 atau 54%. Hasil ini menunjukkan bahwa evaluasi setelah insiden belum sepenuhnya digunakan secara konsisten untuk perbaikan sistem ke depan.

Secara keseluruhan, fungsi Respond menjadi salah satu aspek yang masih lemah. Meskipun seluruh indikator masih masuk kategori Repeatable, capaian yang berada di kisaran bawah menunjukkan bahwa kesiapan respons insiden belum cukup kuat. Disdukcapil perlu memperkuat prosedur respons, pembagian peran saat insiden, mekanisme komunikasi darurat, serta dokumentasi evaluasi pascainsiden.

Hasil Audit Fungsi Recover

Fungsi Recover digunakan untuk menilai kemampuan Disdukcapil dalam memulihkan sistem dan layanan setelah terjadi insiden keamanan. Fungsi ini mencakup perencanaan pemulihan, perbaikan setelah proses pemulihan, dan komunikasi publik ketika terjadi gangguan besar terhadap data. Hasil pengukuran menunjukkan bahwa fungsi Recover memperoleh rata-rata skor 2,6 dengan persentase 52% dan termasuk kategori Repeatable.

Tabel 7. Hasil Audit Fungsi Recover

No.	Indikator	Skala 1	Skala 2	Skala 3	Skala 4	Skala 5	Jumlah Responden	Jumlah Nilai	Rata-Rata	Persentase	Tiers
1	Recover Planning	8	15	11	5	5	44	116	2,6	52%	Repeatable
2	Recover Improvements	9	12	17	3	3	44	111	2,5	50%	Repeatable
3	Recover Communications	7	15	14	4	4	44	115	2,6	52%	Repeatable

Hasil pada fungsi Recover menunjukkan bahwa indikator Recover Planning memperoleh skor 2,6 atau 52%. Hal ini menunjukkan bahwa perencanaan pemulihan jika terjadi kehilangan atau kerusakan data kependudukan sudah ada, tetapi belum berjalan secara optimal. Indikator Recover Communications juga memperoleh skor 2,6 atau 52%, yang menunjukkan bahwa komunikasi publik ketika terjadi insiden besar masih perlu diperkuat agar informasi yang disampaikan lebih cepat, jelas, dan terkoordinasi.

Indikator Recover Improvements memperoleh skor terendah, yaitu 2,5 atau 50%. Secara persentase, nilai ini berada pada batas antara kategori Risk-Informed dan Repeatable, sehingga menjadi titik paling lemah dalam hasil audit. Hasil ini menunjukkan bahwa evaluasi setelah proses pemulihan belum menjadi mekanisme yang kuat untuk mencegah insiden berulang. Dengan demikian, fungsi Recover menjadi fungsi yang paling membutuhkan perhatian karena pemulihan sistem merupakan aspek penting untuk menjaga keberlanjutan pelayanan administrasi kependudukan.

C. Pembahasan

Hasil audit keamanan sistem pengelolaan data kependudukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menunjukkan bahwa seluruh fungsi dalam NIST Cybersecurity Framework 2.0 berada pada kategori Repeatable. Kategori ini menunjukkan bahwa praktik keamanan siber telah dijalankan secara berulang, cukup dikenal oleh organisasi, dan mulai menjadi bagian dari prosedur kerja, meskipun belum sepenuhnya matang sebagai sistem keamanan yang adaptif. Kondisi ini sejalan dengan karakter NIST CSF 2.0 yang menempatkan keamanan siber sebagai proses pengelolaan risiko

yang harus dilaksanakan secara berkelanjutan melalui fungsi Govern, Identify, Protect, Detect, Respond, dan Recover (Moore, 2024). Dalam konteks organisasi publik, capaian Repeatable dapat dipahami sebagai tahap ketika prosedur keamanan sudah berjalan, tetapi masih memerlukan penguatan pada dokumentasi, evaluasi, pengukuran kinerja, serta penyesuaian terhadap perubahan ancaman siber yang terus berkembang (Ross & Pillitteri, 2024).

Capaian rata-rata seluruh fungsi menunjukkan bahwa Disdukcapil Kabupaten Bengkulu Utara telah memiliki fondasi keamanan sistem yang cukup baik, tetapi belum mencapai tingkat kematangan yang optimal. Fungsi Protect memperoleh nilai tertinggi sebesar 3,2 atau 64%, diikuti fungsi Govern sebesar 3,1 atau 62%, fungsi Identify sebesar 3,0 atau 60%, fungsi Detect sebesar 2,8 atau 56%, fungsi Respond sebesar 2,7 atau 54%, dan fungsi Recover sebesar 2,6 atau 52%. Urutan capaian tersebut memperlihatkan bahwa organisasi lebih kuat pada aspek perlindungan teknis dibandingkan kemampuan deteksi, respons, dan pemulihan insiden. Pola ini menunjukkan bahwa sistem keamanan masih cenderung berorientasi pada pencegahan awal, sementara siklus keamanan setelah ancaman muncul belum sepenuhnya kuat. Dalam prinsip keamanan informasi, perlindungan teknis memang penting, tetapi efektivitas keamanan organisasi baru dapat dicapai apabila pencegahan, pemantauan, penanganan insiden, dan pemulihan berjalan sebagai satu kesatuan yang terintegrasi (Whitman & Mattord, 2023).

Temuan tersebut memperlihatkan bahwa Disdukcapil Kabupaten Bengkulu Utara telah memiliki unsur dasar dalam tata kelola keamanan data, terutama pada kebijakan, pembagian peran, pengawasan risiko, dan perlindungan data. Hal ini penting karena data kependudukan merupakan data pribadi yang memiliki nilai strategis dalam pelayanan publik, perencanaan pembangunan, pemberian bantuan sosial, dan penyusunan kebijakan daerah. Data kependudukan juga termasuk informasi yang harus dijaga kerahasiaan, keutuhan, dan ketersediaannya karena berkaitan langsung dengan identitas warga negara. Kewajiban tersebut sejalan dengan Undang-Undang Nomor 27

Tahun 2022 tentang Perlindungan Data Pribadi yang menempatkan perlindungan data sebagai tanggung jawab pengendali data, termasuk instansi pemerintah. Selain itu, Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan juga menegaskan pentingnya perlindungan dan pemanfaatan data kependudukan secara sah, tertib, dan bertanggung jawab.

Pada aspek tata kelola, fungsi Govern memperoleh capaian 62% dan menunjukkan bahwa Disdukcapil telah memiliki dasar pengelolaan keamanan siber yang cukup berjalan. Capaian ini terlihat dari adanya pembagian peran, penerapan kebijakan keamanan, pengawasan risiko, serta perhatian terhadap risiko kerja sama dengan pihak luar. Fungsi Govern dalam NIST CSF 2.0 berperan sebagai fondasi yang mengarahkan seluruh proses keamanan siber karena mencakup strategi, kebijakan, peran, tanggung jawab, dan pengawasan organisasi (Raimondo, 2024). Dalam konteks pemerintahan, tata kelola keamanan tidak hanya berhubungan dengan aspek teknis, tetapi juga berkaitan dengan akuntabilitas birokrasi, kepatuhan hukum, serta komitmen pimpinan dalam menjaga pelayanan publik (Ndraha, 2003).

Namun, capaian fungsi Govern yang masih berada pada kategori Repeatable menunjukkan bahwa tata kelola keamanan belum sepenuhnya bersifat adaptif. Hal ini terlihat dari indikator Organizational Context dan Risk Management Strategy yang masih memperoleh nilai 2,9 atau 58%. Nilai tersebut menunjukkan bahwa pemahaman terhadap konteks organisasi dan strategi pengelolaan risiko belum sepenuhnya merata pada seluruh pegawai. Padahal, keamanan data kependudukan tidak dapat hanya dibebankan kepada unit teknis, karena setiap pegawai yang mengakses, memproses, atau memanfaatkan data memiliki tanggung jawab terhadap keamanan sistem. Dalam tata kelola keamanan informasi, keterlibatan seluruh unsur organisasi menjadi syarat penting agar kebijakan keamanan tidak berhenti sebagai dokumen administratif, tetapi benar-benar menjadi perilaku kerja yang konsisten (Von Solms & Van Niekerk, 2021).

Fungsi Identify memperoleh capaian 60%, yang menunjukkan bahwa proses pengenalan aset, tata

kelola, dan risiko sudah dilakukan, tetapi belum sepenuhnya mendalam. Indikator Asset Management menjadi aspek yang relatif kuat dengan nilai 3,1 atau 68%, yang berarti Disdukcapil telah memiliki pemahaman cukup baik terhadap aset teknologi informasi yang digunakan dalam pelayanan, seperti server, komputer, aplikasi, basis data, dan perangkat biometrik. Identifikasi aset menjadi tahap awal yang sangat penting karena organisasi tidak dapat melindungi sesuatu yang belum dipetakan dengan jelas. Dalam sistem informasi, aset seperti data, perangkat keras, perangkat lunak, jaringan, dan sumber daya manusia merupakan komponen yang saling terhubung untuk menghasilkan informasi yang bermanfaat bagi pengambilan keputusan (Jogiyanto H.M., 2018).

Meskipun demikian, indikator Risk Assessment pada fungsi Identify hanya memperoleh nilai 2,9 atau 58%, sehingga menunjukkan bahwa proses identifikasi risiko kebocoran, penyalahgunaan data, gangguan sistem, dan kerentanan teknis belum sepenuhnya sistematis. Kondisi ini penting diperhatikan karena data kependudukan memiliki tingkat sensitivitas tinggi dan dapat menimbulkan dampak luas jika disalahgunakan. Penilaian risiko yang belum mendalam dapat menyebabkan organisasi tidak mengetahui prioritas perlindungan, titik kerentanan utama, serta skenario ancaman yang paling mungkin terjadi. Dalam pengelolaan keamanan informasi, penilaian risiko harus dilakukan secara berkala karena ancaman siber selalu berubah mengikuti perkembangan teknologi, pola serangan, dan tingkat ketergantungan organisasi terhadap sistem digital (Stallings, 2022).

Capaian tertinggi pada fungsi Protect sebesar 64% menunjukkan bahwa Disdukcapil Kabupaten Bengkulu Utara relatif lebih kuat pada aspek perlindungan sistem dan data. Indikator Maintenance memperoleh nilai 3,6 atau 72%, sedangkan indikator Protect Database memperoleh nilai 3,5 atau 70%. Hasil ini menunjukkan bahwa pemeliharaan sistem dan perlindungan basis data sudah menjadi perhatian organisasi. Kondisi tersebut menjadi temuan positif karena perlindungan terhadap basis data kependudukan merupakan inti dari keamanan layanan administrasi kependudukan. Data kependudukan tidak hanya digunakan untuk menerbitkan dokumen seperti

KTP-el, Kartu Keluarga, dan akta pencatatan sipil, tetapi juga menjadi dasar berbagai layanan lintas sektor. Oleh karena itu, perlindungan basis data harus dilakukan melalui pembatasan akses, pengamanan perangkat, pembaruan sistem, pencadangan, dan prosedur pengendalian yang jelas (Tipton & Krause, 2022).

Walaupun fungsi Protect menjadi aspek terkuat, capaian tersebut belum cukup untuk menyatakan bahwa keamanan sistem sudah matang secara menyeluruh. Indikator Identity Management and Access Control dan Protective Technology masih berada pada nilai 3,1 atau 68%, yang berarti pengelolaan akses dan teknologi pelindung sudah berjalan, tetapi belum sepenuhnya optimal. Hal ini menunjukkan bahwa Disdukcapil masih perlu memperkuat pengaturan hak akses berbasis peran, autentikasi pengguna, pengamanan perangkat kerja, perlindungan jaringan, serta penggunaan teknologi pelindung yang lebih terintegrasi. Dalam keamanan informasi, akses pengguna menjadi salah satu titik rawan karena penyalahgunaan kredensial, kelalaian pegawai, dan lemahnya pembatasan hak akses dapat membuka peluang terjadinya kebocoran data (Whitman & Mattord, 2023).

Fungsi Detect memperoleh capaian 56%, yang menunjukkan bahwa kemampuan deteksi ancaman sudah tersedia tetapi belum optimal. Indikator Continuous Monitoring dan Adverse Event Analysis masing-masing memperoleh nilai tinggi, yaitu 3,5 atau 70% dan 3,6 atau 70%. Hasil ini menunjukkan bahwa aktivitas pemantauan akses dan pengenalan anomali sudah dilakukan dalam batas tertentu. Namun, indikator Detection Processes hanya memperoleh nilai 2,9 atau 58%, sehingga memperlihatkan bahwa prosedur deteksi formal belum sepenuhnya berjalan kuat. Dalam praktik keamanan siber, pemantauan yang dilakukan tanpa prosedur tertulis, sistem log yang memadai, dan alur eskalasi yang jelas dapat menyebabkan keterlambatan dalam mengenali serangan yang lebih kompleks (Ross & Pillitteri, 2024).

Kelemahan pada fungsi Detect menjadi perhatian karena organisasi publik yang mengelola data sensitif harus mampu mengenali tanda awal gangguan sebelum berkembang menjadi insiden besar. Ancaman siber

tidak selalu tampak dalam bentuk serangan langsung, tetapi dapat muncul melalui akses tidak sah, penggunaan akun pegawai, malware tersembunyi, manipulasi data, atau aktivitas tidak wajar pada sistem. Tanpa proses deteksi yang kuat, organisasi dapat baru menyadari adanya gangguan setelah data terdampak atau layanan mengalami kerusakan. Audit keamanan sistem informasi diperlukan untuk menemukan kondisi tersebut sejak awal, menilai kecukupan kontrol keamanan, dan memberikan dasar rekomendasi perbaikan yang sesuai dengan risiko organisasi (Hamzah, 2018).

Fungsi Respond memperoleh capaian 54%, yang menunjukkan bahwa kesiapan Disdukcapil dalam menangani insiden keamanan masih perlu diperkuat. Indikator Response Planning memperoleh nilai 3,0 atau 60%, yang berarti rencana respons insiden sudah mulai tersedia. Akan tetapi, indikator Respond Communication, Respond Mitigation, dan Response Improvements memperoleh nilai yang lebih rendah, yaitu 58%, 56%, dan 54%. Hal ini menunjukkan bahwa mekanisme komunikasi insiden, langkah mitigasi dampak, dan evaluasi setelah insiden belum berjalan optimal. Dalam konteks keamanan informasi, respons insiden harus mencakup pelaporan, analisis, pembatasan dampak, koordinasi antarunit, komunikasi kepada pihak terkait, dan perbaikan pascainsiden (Raimondo, 2024).

Kelemahan fungsi Respond dapat berdampak langsung terhadap kualitas layanan publik apabila terjadi gangguan pada sistem kependudukan. Disdukcapil merupakan instansi yang memberikan layanan langsung kepada masyarakat, sehingga gangguan pada sistem dapat menghambat penerbitan dokumen, pemutakhiran data, dan pelayanan administrasi lainnya. Apabila organisasi belum memiliki mekanisme respons yang jelas, maka insiden kecil dapat berkembang menjadi gangguan layanan yang lebih besar. Dalam penyelenggaraan e-government, kualitas layanan digital tidak hanya dinilai dari kecepatan layanan, tetapi juga dari kemampuan sistem menjaga keandalan, keamanan, dan kesinambungan pelayanan (Indrajit, 2016).

Fungsi Recover menjadi fungsi dengan capaian terendah, yaitu 52%. Indikator Recover Planning

memperoleh nilai 2,6 atau 52%, Recover Communications memperoleh nilai 2,6 atau 52%, dan Recover Improvements memperoleh nilai 2,5 atau 50%. Hasil ini menunjukkan bahwa perencanaan pemulihan, komunikasi selama pemulihan, dan evaluasi setelah pemulihan masih menjadi titik lemah utama. Padahal, fungsi Recover sangat penting karena tidak semua ancaman dapat dicegah sepenuhnya. Organisasi harus tetap mampu memulihkan sistem, mengembalikan layanan, menjaga ketersediaan data, dan menyampaikan informasi yang jelas kepada masyarakat ketika terjadi insiden (Moore, 2024).

Rendahnya capaian Recover menunjukkan bahwa Disdukcapil perlu memperkuat rencana pemulihan bencana atau Disaster Recovery Plan secara lebih operasional. Perencanaan pemulihan tidak cukup hanya berupa pencadangan data, tetapi harus mencakup target waktu pemulihan, batas toleransi kehilangan data, prosedur pemulihan sistem, pihak yang bertanggung jawab, serta mekanisme komunikasi saat layanan terganggu. Jika fungsi pemulihan tidak disiapkan dengan baik, maka gangguan keamanan dapat menyebabkan layanan berhenti lebih lama, data sulit dipulihkan, dan kepercayaan publik menurun. Dalam manajemen keamanan informasi, kemampuan pemulihan merupakan bagian penting dari ketahanan organisasi karena menentukan seberapa cepat layanan dapat kembali berjalan setelah insiden terjadi (Stallings, 2022).

Temuan bahwa fungsi Protect lebih kuat dibandingkan Detect, Respond, dan Recover menunjukkan adanya ketidakseimbangan dalam siklus keamanan siber Disdukcapil Kabupaten Bengkulu Utara. Organisasi sudah memiliki kemampuan dasar dalam melindungi sistem, tetapi belum memiliki kesiapan yang sepadan untuk menghadapi insiden setelah ancaman terjadi. Kondisi ini sering ditemukan pada organisasi yang masih memandang keamanan sebagai urusan teknis, bukan sebagai siklus manajemen risiko yang menyeluruh. Padahal, NIST CSF 2.0 menekankan bahwa keamanan siber harus dipandang sebagai proses terpadu yang dimulai dari tata kelola, identifikasi risiko, perlindungan, deteksi, respons, hingga pemulihan (Moore, 2024).

Jika dikaitkan dengan regulasi, hasil penelitian ini menunjukkan bahwa Disdukcapil Kabupaten Bengkulu Utara telah memiliki dasar implementasi keamanan, tetapi masih perlu meningkatkan kepatuhan terhadap standar keamanan informasi yang diwajibkan. Permendagri Nomor 72 Tahun 2022 menegaskan bahwa keamanan Identitas Kependudukan Digital harus berpedoman pada standar internasional seperti ISO/IEC dan NIST. Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE juga menekankan penyelenggaraan pemerintahan berbasis elektronik yang aman, terpadu, dan berkelanjutan. Dengan demikian, hasil audit yang masih berada pada kategori Repeatable menunjukkan bahwa terdapat kebutuhan untuk memperkuat pengendalian keamanan agar tidak hanya memenuhi kebutuhan teknis, tetapi juga memenuhi tuntutan tata kelola pemerintahan digital.

Selain itu, Peraturan Bupati Bengkulu Utara Nomor 31 Tahun 2023 tentang Arsitektur SPBE memperlihatkan bahwa pemerintah daerah telah memiliki arah kebijakan formal dalam penyelenggaraan SPBE. Namun, hasil penelitian menunjukkan bahwa audit keamanan sistem pengelolaan data masih perlu diperkuat agar pelaksanaan SPBE tidak hanya berorientasi pada penggunaan teknologi, tetapi juga memperhatikan keamanan data dan keberlanjutan layanan. Kondisi ini menunjukkan adanya kesenjangan antara kebijakan dan implementasi di lapangan. Kesenjangan tersebut perlu ditutup melalui pelaksanaan audit berkala, penguatan kapasitas pegawai, peningkatan infrastruktur keamanan, serta penyusunan standar operasional keamanan yang lebih jelas.

Hasil penelitian ini sejalan dengan temuan Gimnastiar dan Nursyanti yang menunjukkan bahwa audit berbasis NIST dapat mengidentifikasi tingkat keamanan dan risiko pada sistem informasi serta menghasilkan rekomendasi perbaikan yang lebih terarah (Gimnastiar & Nursyanti, 2024). Temuan ini juga sejalan dengan Fadila, Mutiah, dan Sari yang menegaskan bahwa penggunaan framework keamanan seperti NIST CSF dapat membantu organisasi mengevaluasi kontrol keamanan siber secara lebih sistematis (Fadila et al., 2023). Perbedaannya, penelitian ini memiliki

konteks yang lebih spesifik karena berfokus pada sistem pengelolaan data kependudukan di instansi pemerintah daerah, sehingga aspek regulasi administrasi kependudukan dan perlindungan data pribadi menjadi bagian penting dari interpretasi hasil.

Hasil penelitian ini juga memperkuat pandangan bahwa NIST CSF relevan digunakan pada lingkungan pemerintahan karena dapat menilai keamanan tidak hanya dari sisi perangkat, tetapi juga dari sisi tata kelola, proses, manusia, dan kesiapan organisasi. Penelitian Muthi'atur Rofi'ah menunjukkan bahwa NIST CSF dapat digunakan dalam perspektif auditor internal Indonesia untuk menilai tata kelola keamanan siber secara lebih terstruktur (Muthi'atur Rofi'ah, 2025). Hal ini sesuai dengan kebutuhan Disdukcapil yang tidak hanya membutuhkan perlindungan teknis, tetapi juga membutuhkan mekanisme audit yang mampu mengukur kesiapan organisasi secara menyeluruh. Dengan demikian, penggunaan NIST CSF 2.0 dalam penelitian ini dapat memberikan gambaran yang lebih lengkap mengenai kondisi keamanan sistem pengelolaan data kependudukan.

Secara praktis, hasil penelitian ini menunjukkan bahwa prioritas perbaikan Disdukcapil Kabupaten Bengkulu Utara sebaiknya diarahkan pada fungsi Recover, Respond, dan Detect. Fungsi Recover perlu diperkuat karena menjadi capaian terendah dan berhubungan langsung dengan keberlanjutan layanan setelah insiden. Fungsi Respond perlu ditingkatkan karena menjadi dasar penanganan insiden agar gangguan tidak meluas. Fungsi Detect juga perlu diperkuat agar organisasi dapat mengenali potensi ancaman lebih cepat. Sementara itu, fungsi Protect, Govern, dan Identify tetap perlu dipertahankan serta ditingkatkan agar perlindungan teknis dan tata kelola keamanan tidak berhenti pada kategori Repeatable.

Dengan demikian, hasil audit menunjukkan bahwa sistem keamanan pengelolaan data di Disdukcapil Kabupaten Bengkulu Utara telah memiliki fondasi yang cukup baik, tetapi belum sepenuhnya tangguh dalam menghadapi ancaman siber yang kompleks. Organisasi sudah memiliki perlindungan teknis, pengelolaan aset, dan tata kelola dasar, tetapi masih memerlukan penguatan pada deteksi ancaman,

respons insiden, dan pemulihan layanan. Apabila perbaikan dilakukan secara bertahap dan berkelanjutan, Disdukcapil dapat meningkatkan posisinya menuju kategori Adaptive, yaitu kondisi ketika keamanan siber tidak hanya dijalankan sebagai prosedur, tetapi menjadi bagian dari budaya kerja, tata kelola risiko, dan kualitas pelayanan publik digital.

D. Kesimpulan

Berdasarkan hasil audit menggunakan NIST Cybersecurity Framework 2.0, keamanan sistem pengelolaan data kependudukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara berada pada kategori Repeatable. Hasil pengukuran menunjukkan bahwa fungsi Protect memperoleh capaian tertinggi sebesar 3,2 atau 64%, diikuti Govern sebesar 3,1 atau 62%, Identify sebesar 3,0 atau 60%, Detect sebesar 2,8 atau 56%, Respond sebesar 2,7 atau 54%, dan Recover sebesar 2,6 atau 52%. Capaian tersebut menunjukkan bahwa sistem keamanan sudah berjalan cukup konsisten, terutama pada aspek perlindungan teknis, pemeliharaan sistem, pengamanan basis data, dan tata kelola dasar keamanan informasi.

Meskipun demikian, hasil penelitian menunjukkan bahwa keamanan sistem belum sepenuhnya matang dan adaptif dalam menghadapi ancaman siber yang semakin kompleks. Kelemahan utama terdapat pada fungsi Detect, Respond, dan Recover, khususnya pada deteksi kejadian keamanan, komunikasi insiden, mitigasi gangguan, perencanaan pemulihan, dan evaluasi pascapemulihan. Dengan demikian, Disdukcapil Kabupaten Bengkulu Utara perlu memperkuat prosedur deteksi, menyusun mekanisme respons insiden yang jelas, menguji rencana pemulihan secara berkala, serta meningkatkan kapasitas pegawai agar perlindungan data kependudukan dapat berjalan lebih aman, andal, dan berkelanjutan.

DAFTAR PUSTAKA

Fadila, V., Mutiah, N., & Sari, R. P. (2023). Audit keamanan siber menggunakan kerangka kerja CIS CSC, NIST CSF, dan COBIT 2019. *Journal of Computing Engineering, System and Science, 8*(2), 271–283.

https://doi.org/10.24114/cess.v8i2.43257

Gimnastiar, R., & Nursyanti, R. (2024). Audit keamanan dan manajemen risiko dengan menggunakan framework NIST (Studi kasus: E-Learning UNIBI). *Seminar Nasional*. https://corisindo.utb-univ.ac.id/index.php/penelitian/article/view/61

Hamzah, M. R. (2018). *Audit keamanan sistem informasi dengan menggunakan standar ISO/IEC 27002:2013 dan ISO/IEC 27001:2013 pada Sub Bagian Data dan Informasi Direktorat Jenderal Kebudayaan Republik Indonesia* [Skripsi, UIN Syarif Hidayatullah Jakarta]. UIN Repository. https://repository.uinjkt.ac.id/dspace/handle/123456789/68155

Handoyo, A., & Nigrum, R. (2024). Implementasi NIST CSF untuk penilaian risiko keamanan siber di perguruan tinggi. *Jurnal Sistem Informasi dan Teknologi, 14*(1), 88–102. https://doi.org/10.37859/coscitech.v4i3.5628

Indrajit, R. E. (2016). *Konsep dan strategi electronic government*. Preinexus.

Jogiyanto, H. M. (2018). *Konsep dasar sistem dan informasi: Sistem informasi manajemen* (Edisi 3). Yayasan Cendikia Mulia Mandiri.

Moore, T. (2024). *The NIST cybersecurity framework 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Muthi'atur Rofi'ah, D. (2025). NIST cybersecurity framework in the lens of Indonesian internal auditors. *Indonesian Interdisciplinary Journal of Sharia Economics, 8*(2), 3349–3367. https://doi.org/10.31538/iijse.v8i2.6027

Ndraha, T. (2003). *Kybernologi: Ilmu pemerintahan*. Rineka Cipta.

Peraturan Bupati Bengkulu Utara Nomor 31 Tahun 2023 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE).

Peraturan Menteri Dalam Negeri Nomor 72 Tahun 2022 tentang Standar dan Spesifikasi Perangkat Keras, Perangkat Lunak, dan Identitas Kependudukan Digital.

Peraturan Menteri Dalam Negeri Nomor 102 Tahun 2019 tentang Pemberian Hak Akses dan Pemanfaatan Data Kependudukan.

Peraturan Menteri Komunikasi dan Informatika Nomor 16 Tahun 2022 tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi dan Komunikasi.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Peraturan Presiden Nomor 82 Tahun 2022 tentang Percepatan Transformasi Digital dan Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik.

Rahman, R., Ananta, A., & Surianti, B. (2025). Analisis perbandingan framework keamanan jaringan (NIST CSF, CIS Controls, ISO 27001). *Technology Sciences Insights Journal, 12*(3), 45–60. https://doi.org/10.60036/z05cpv06

Raimondo, G. M. (2024). *NIST cybersecurity framework 2.0: Small business quick-start guide*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1300

Ross, R., & Pillitteri, V. (2024). *NIST cybersecurity framework 2.0: Managing risk in the digital era*. National Institute of Standards and Technology.

Saputra Rambe, A., & Oktalisa, E. (2021). Inovasi dalam pelayanan publik: Studi kasus implementasi e-government di negara-negara berkembang. *Sengkuni Journal: Social Sciences and Humanities, 2*(2), 165–170. https://doi.org/10.37638/sengkuni.2.2.165-170

Stallings, W. (2022). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley.

Tipton, H. F., & Krause, M. (2022). *Information security management handbook* (Edisi 7). CRC Press.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Von Solms, R., & Van Niekerk, J. (2021). *Information security governance*. Springer.

Whitman, M. E., & Mattord, H. J. (2023). *Principles of information security* (Edisi 7). Cengage Learning.