AUDIT KEAMANAN SISTEM PENGELOLAAN DATA DI DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KABUPATEN BENGKULU UTARA MENGGUNAKAN FRAMEWORK NIST (National Institute of Standard and Technology)

Annisa Rahmadhani.DM
NPP. 33.0256
Program Studi Teknologi Rekayasa Informasi Pemerintahan
Email: annisa.rdm@gmail.com

Pembimbing Skripsi: Muhammad Tosan Bingamawa, M.Kom
Email: tossan@ipdn.ac.id

ABSTRACT

Problem Statement (Kesenjangan Penelitian/Research Gap): *This study focuses on the increasing cyber threats and the limited security infrastructure in the population data management system at the Department of Population and Civil Registration of North Bengkulu Regency. Meanwhile, population data is categorized as sensitive personal data that requires strong protection and proper cybersecurity governance.* ***Purpose:*** *The purpose of this study is to analyze the security level of the data management system at the Population and Civil Registration Service of North Bengkulu Regency using the NIST Cybersecurity Framework 2.0 framework.* ***Method:*** *This study uses a qualitative descriptive approach with data collection techniques through interviews, observations, docum(Mphahlele et al., 2025)entation, and assessment based on the six functions of the NIST CSF 2.0 framework, namely Govern, Identify, Protect, Detect, Respond, and Recover.* ***Result:*** *The results show that all security functions are categorized at the Repeatable level with different achievement scores. 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 has been implemented relatively well, but incident detection, response, and recovery capabilities still require significant improvement. The study also found that governance, policy implementation, and cybersecurity risk management have not been fully optimized.* ***Conclusion:*** *This study concludes that the security system for population data management at the Department of Population and Civil Registration of North Bengkulu Regency has been implemented fairly well, but it is not yet fully mature in addressing complex cyber threats. It is recommended to strengthen the Detect, Respond, and Recover functions to improve sustainable and effective protection of population data.*

Keywords: *cybersecurity; Disdukcapil; NIST CSF 2.0; population data; security audit.*

ABSTRAK

Permasalahan (Kesenjangan Penelitian/Research Gap): Penelitian ini berfokus pada meningkatnya ancaman serangan siber dan keterbatasan infrastruktur keamanan pada sistem pengelolaan data kependudukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara. Sementara itu, data kependudukan merupakan data pribadi yang bersifat sensitif sehingga memerlukan perlindungan keamanan siber dan tata kelola sistem informasi yang baik. **Tujuan:** Tujuan penelitian ini adalah untuk menganalisis tingkat keamanan sistem pengelolaan data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menggunakan framework NIST Cybersecurity Framework 2.0. **Metode:** Penelitian ini menggunakan metode deskriptif kualitatif dengan teknik pengumpulan data melalui wawancara, observasi, dokumentasi, dan penilaian berdasarkan enam fungsi dalam framework NIST CSF 2.0 yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. **Hasil/Temuan:** Temuan penelitian menunjukkan bahwa seluruh fungsi keamanan berada pada kategori Repeatable dengan capaian yang berbeda-beda. Fungsi Protect memperoleh nilai 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%. Hasil tersebut menunjukkan bahwa perlindungan teknis sistem sudah berjalan cukup baik, namun kemampuan deteksi, respons, dan pemulihan insiden siber masih memerlukan peningkatan. Selain itu, tata kelola keamanan, kebijakan, serta pengelolaan risiko keamanan informasi juga belum sepenuhnya optimal. **Kesimpulan:** Penelitian ini menyimpulkan bahwa keamanan sistem pengelolaan data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara telah berjalan cukup baik, namun belum matang secara menyeluruh dalam menghadapi ancaman siber yang kompleks. Adapun saran penelitian ini yaitu perlunya penguatan pada fungsi Detect, Respond, dan Recover guna meningkatkan perlindungan data kependudukan yang lebih efektif dan berkelanjutan.
Kata kunci: audit keamanan; data kependudukan; Disdukcapil; keamanan siber; NIST CSF 2.0.

I. PENDAHULUAN

1.1. Latar Belakang

Pemerintah menurut (Gimnastiar et al., 2024) merupakan organisasi yang dibentuk untuk mengatur kehidupan bersama, menjaga ketertiban, serta mengarahkan masyarakat menuju kondisi yang lebih baik melalui fungsi pemberdayaan, pembangunan, dan pelayanan. Dalam konteks pemerintahan modern, pelayanan publik tidak hanya berkaitan dengan pelayanan administratif secara langsung kepada masyarakat, tetapi juga mencakup pengelolaan data kependudukan yang menjadi dasar berbagai layanan negara (Setiyawati et al., 2025). Data kependudukan digunakan dalam perencanaan pembangunan, distribusi bantuan sosial, pelayanan kesehatan, pendidikan, hingga administrasi pemerintahan lainnya. Oleh karena itu, pengelolaan data kependudukan harus dilakukan secara aman, akurat, dan bertanggung jawab (Mphahlele et al., 2025).

Perkembangan teknologi informasi telah mendorong transformasi digital dalam sistem administrasi pemerintahan, termasuk pada Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil). Sistem Informasi Administrasi Kependudukan (SIAK) menjadi bagian penting dalam mendukung pelayanan publik berbasis digital. Namun, transformasi digital tersebut juga menghadirkan tantangan baru berupa meningkatnya ancaman keamanan siber terhadap data pribadi masyarakat. Data kependudukan merupakan data pribadi yang bersifat sensitif karena memuat identitas individu seperti Nomor Induk Kependudukan (NIK), alamat, status perkawinan, data biometrik, dan informasi penting lainnya yang wajib dilindungi oleh negara (Saputra Rambe et al., 2021).

Pemerintah Indonesia telah menetapkan berbagai regulasi terkait perlindungan data pribadi dan keamanan informasi, di antaranya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan, serta

Permendagri Nomor 72 Tahun 2022 tentang Standar dan Spesifikasi Perangkat Keras, Perangkat Lunak, dan Blangko KTP-el serta Penyelenggaraan Identitas Kependudukan Digital (Ndraha, 2003). Regulasi tersebut menegaskan bahwa pengelola data pribadi wajib menerapkan sistem keamanan informasi sesuai standar nasional maupun internasional guna menjaga kerahasiaan, integritas, dan ketersediaan data (Indrajit, 2016).

Kabupaten Bengkulu Utara dengan jumlah penduduk sebanyak 307.507 jiwa pada tahun 2024 dan laju pertumbuhan penduduk sebesar 1,26% per tahun menghadapi tantangan dalam pengelolaan data kependudukan yang semakin kompleks. Pertumbuhan jumlah penduduk tentu berpengaruh terhadap volume data yang harus dikelola oleh Disdukcapil Bengkulu Utara (Hamzah, 2018). Apabila peningkatan volume data tersebut tidak diimbangi dengan sistem keamanan informasi yang baik, maka risiko kebocoran data, kerusakan data, maupun gangguan layanan publik akan semakin besar.

Tabel 1.1
Jumlah Penduduk Kabupaten Bengkulu Utara Tahun 2021–2024

Tahun	Jumlah Penduduk	Laju Pertumbuhan Penduduk
2021	293.465	1,29%
2022	298.945	1,21%
2023	304.720	1,28%
2024	307.507	1,26%

Selain pertumbuhan jumlah penduduk, tantangan lain terlihat dari kondisi infrastruktur teknologi informasi yang dimiliki Disdukcapil Bengkulu Utara. Infrastruktur yang tersedia masih terbatas baik dari sisi server, perangkat komputer pelayanan, maupun perangkat keamanan jaringan. Keterbatasan tersebut berpotensi menimbulkan gangguan operasional serta meningkatkan kerentanan terhadap ancaman siber (Jogiyanto H.M., 2018).

Tabel 1.2
Infrastruktur Teknologi Informasi Disdukcapil Bengkulu Utara Tahun 2024

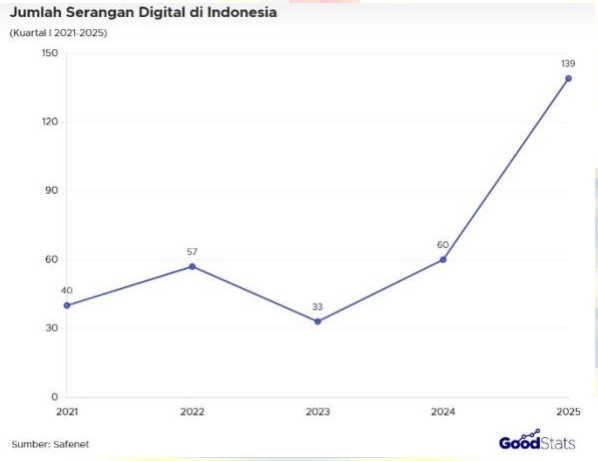
NO	JENIS	NAMA	JUMLAH	KETERANGAN
1	*Software*	SIAK	1	Terpusat
2	*Hardware*	Server	2	- server utama - server backup data
		Personal Computer	14	- 1 unit input data - 1 unit cetak KK - 1 unit cetak akta - 1 unit cetak surat pindah dan datang - 6 unit di ruang pendafataran - 1 unit rekam KTP - 1 unit cetak KTP - 1 unit cetak KIA - 1 unit kendali penghubung ke server
		Signature Pad	1	Merekam tanda tangan
		Finger Print	1	Merekam sidik jari
		Iris Scanner	1	Merekam Biometrik
		Printer cetak	6	- Mencetak KTP

	- Mencetak KIA - Mencetak KK - Mencetak akta pindah dan datang - Mencetak akta kelahiran dan kematian - Scan foto untuk KIA

Berdasarkan kondisi tersebut, diketahui bahwa Disdukcapil Bengkulu Utara hanya memiliki dua unit server yang terdiri dari server utama dan server backup tanpa dukungan redundancy system yang memadai. Selain itu, sebagian besar komputer pelayanan masih menggunakan sistem multi-user dan belum dilengkapi dengan pengamanan berlapis (Muthi'atur Rofi'ah, 2025). Perangkat biometrik seperti fingerprint scanner, iris scanner, dan signature pad juga hanya tersedia satu unit sehingga berisiko menyebabkan bottleneck pelayanan apabila terjadi kerusakan perangkat.

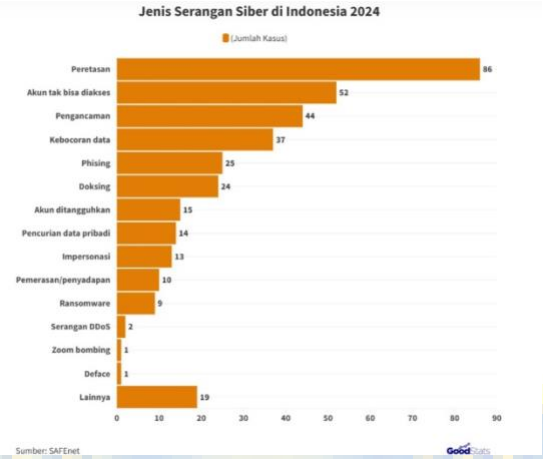
Permasalahan keamanan sistem informasi juga terlihat dari penggunaan jaringan internet umum yang belum sepenuhnya menggunakan jaringan tertutup sebagaimana diatur dalam Permendagri Nomor 102 Tahun 2019. Kondisi ini meningkatkan risiko serangan siber seperti network sniffing, malware, phishing, dan pencurian data. Selain itu, Disdukcapil Bengkulu Utara juga belum memiliki perangkat keamanan tambahan seperti firewall enterprise, intrusion detection system (IDS), intrusion prevention system (IPS), antivirus terpusat, serta sistem log audit yang memadai (Nurdin & Hartati, 2019).

Permasalahan keamanan data semakin relevan dengan meningkatnya kasus kebocoran data di Indonesia dalam beberapa tahun terakhir. Berbagai insiden kebocoran data yang melibatkan lembaga pemerintah maupun sektor swasta menunjukkan bahwa keamanan informasi nasional masih menghadapi tantangan serius. Kebocoran data Dukcapil yang mencakup jutaan data penduduk Indonesia menjadi salah satu contoh nyata lemahnya perlindungan data pribadi (Bakunzibake et al., 2019).



Gambar 1.1
Jumlah Serangan Digital di Indonesia Tahun 2024–2025

Data SAFEnet juga menunjukkan bahwa jenis serangan siber yang paling dominan di Indonesia adalah hacking atau pembobolan sistem. Kondisi ini menunjukkan bahwa instansi pemerintah yang mengelola data sensitif, termasuk Disdukcapil, harus memiliki sistem keamanan informasi yang kuat dan berkelanjutan (Sugiyono, 2018).



Gambar 1.2
Jenis Serangan Siber di Indonesia Tahun 2024

Gambar ini memperlihatkan jenis-jenis serangan siber yang paling banyak terjadi di Indonesia berdasarkan laporan SAFEnet. Dalam rangka meningkatkan keamanan sistem informasi, audit keamanan menjadi salah satu langkah penting yang harus dilakukan oleh instansi pemerintah. Audit keamanan sistem informasi bertujuan untuk menilai tingkat keamanan sistem, mengidentifikasi kerentanan, serta memberikan rekomendasi perbaikan terhadap pengelolaan keamanan informasi. Audit juga menjadi alat evaluasi untuk memastikan bahwa sistem yang digunakan telah sesuai dengan standar keamanan yang berlaku (Hooda et al., 2023).

Permendagri Nomor 72 Tahun 2022 secara tegas mengatur bahwa keamanan identitas kependudukan digital harus mengacu pada standar internasional seperti ISO/IEC maupun National Institute of Standards and Technology (NIST). Namun, berdasarkan Peraturan Bupati Bengkulu Utara Nomor 31 Tahun 2023 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE), audit keamanan SPBE di lingkungan Pemerintah Kabupaten Bengkulu Utara belum pernah dilaksanakan.

Tabel 1.3
Audit Keamanan SPBE Pemerintah Kabupaten Bengkulu Utara

ID	Nama Kegiatan Audit Keamanan SPBE	Deskripsi Kegiatan Audit Keamanan SPBE	Hasil Audit Keamanan SPBE	Jenis Audit Keamanan	Tindak lanjut Audit Keamanan	Tanggal Kegiatan Audit Keamanan	→ Instansi (Dependency)
02.02	Audit Keamanan	melakukan Audit keamanan yang dilakukan secara rutin dalam 2 tahun sekali dan meminimalisir terjadinya permasalahan keamanan dengan implementasi audit kemanan	a. belum/tidak dilaksanakan				

Tabel ini menunjukkan kondisi pelaksanaan audit keamanan SPBE berdasarkan Peraturan Bupati Bengkulu Utara Nomor 31 Tahun 2023. Kondisi tersebut menunjukkan adanya kesenjangan antara regulasi pemerintah pusat yang mewajibkan penerapan audit keamanan berbasis standar internasional dengan implementasi di daerah yang belum melaksanakan audit keamanan secara menyeluruh. Padahal, audit keamanan sangat penting untuk memastikan bahwa sistem pengelolaan data kependudukan mampu melindungi data masyarakat dari ancaman siber (Sharma et al., 2025).

Dalam penelitian ini, peneliti menggunakan framework NIST Cybersecurity Framework (NIST CSF) 2.0 sebagai dasar audit keamanan sistem pengelolaan data di Disdukcapil Bengkulu Utara. Framework NIST dipilih karena memiliki pendekatan yang komprehensif dalam mengukur tingkat keamanan informasi melalui enam fungsi utama yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. Selain itu, framework ini telah banyak digunakan secara nasional maupun internasional sebagai standar audit keamanan siber.

Beberapa penelitian terdahulu telah membahas audit keamanan sistem informasi menggunakan framework NIST, seperti penelitian Nur A mengenai audit keamanan sistem absensi GreatDay menggunakan NIST, penelitian Reynaldy G mengenai audit keamanan dan manajemen risiko berbasis NIST, serta penelitian Bernard N tentang integrasi framework NIST dan ISO dalam audit keamanan siber. Namun demikian, belum terdapat penelitian yang secara spesifik mengkaji audit keamanan sistem pengelolaan data kependudukan di Disdukcapil menggunakan framework NIST CSF 2.0 dalam konteks implementasi regulasi perlindungan data pribadi di Indonesia.

Berdasarkan uraian tersebut, peneliti tertarik untuk melakukan penelitian dengan judul "Audit Keamanan Sistem Pengelolaan Data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara Menggunakan Framework NIST (National Institute of Standards and Technology)" dengan harapan dapat memberikan gambaran mengenai tingkat keamanan sistem pengelolaan data kependudukan serta rekomendasi perbaikan keamanan informasi di Disdukcapil Bengkulu Utara.

1.2. Kesenjangan Masalah yang Diambil (Research Gap)

Penelitian ini berfokus pada permasalahan keamanan sistem pengelolaan data kependudukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara yang masih menghadapi berbagai keterbatasan infrastruktur dan belum dilaksanakannya audit keamanan sistem informasi secara menyeluruh. Di sisi lain, Disdukcapil merupakan instansi yang mengelola data pribadi masyarakat dalam jumlah besar dan bersifat sensitif sehingga membutuhkan sistem keamanan informasi yang kuat dan sesuai standar nasional maupun internasional (Arsento et al., 2022).

Terdapat beberapa permasalahan yang menjadi dasar penelitian ini. Pertama, meningkatnya jumlah penduduk Kabupaten Bengkulu Utara menyebabkan volume data kependudukan yang dikelola Disdukcapil terus bertambah setiap tahun. Kondisi tersebut tidak sepenuhnya diimbangi dengan kesiapan infrastruktur teknologi informasi yang memadai, sehingga meningkatkan risiko gangguan layanan maupun kebocoran data (Gatiningsih, 2022).

Kedua, infrastruktur keamanan informasi di Disdukcapil Bengkulu Utara masih terbatas. Server yang digunakan belum memiliki redundancy system yang optimal, komputer pelayanan masih menggunakan sistem multi-user tanpa pengamanan berlapis, serta belum tersedia perangkat keamanan jaringan seperti firewall enterprise, IDS/IPS, antivirus terpusat, dan audit log system. Selain itu, penggunaan jaringan internet umum juga meningkatkan risiko serangan siber terhadap sistem pengelolaan data kependudukan (Gatiningsih, 2015).

Ketiga, berdasarkan Peraturan Bupati Bengkulu Utara Nomor 31 Tahun 2023 diketahui bahwa audit keamanan SPBE di lingkungan Pemerintah Kabupaten Bengkulu Utara belum pernah dilakukan. Kondisi ini menunjukkan adanya regulatory compliance gap antara ketentuan Permendagri Nomor 72 Tahun 2022 yang mewajibkan penerapan standar keamanan informasi berbasis internasional dengan implementasi di tingkat daerah yang belum melaksanakan audit keamanan (Marthalina et al., 2025).

Keempat, meningkatnya kasus kebocoran data dan serangan siber di Indonesia menunjukkan bahwa instansi pemerintah masih rentan terhadap ancaman keamanan informasi. Kebocoran data Dukcapil nasional yang melibatkan jutaan data penduduk menjadi bukti bahwa pengelolaan data kependudukan masih memiliki kelemahan dalam aspek keamanan system (Suwanda, 2015).

Meskipun berbagai penelitian sebelumnya telah membahas audit keamanan sistem informasi menggunakan framework NIST, masih terdapat keterbatasan penelitian yang secara khusus mengkaji audit keamanan sistem pengelolaan data kependudukan di Disdukcapil menggunakan NIST CSF 2.0 dalam konteks implementasi regulasi perlindungan data pribadi dan administrasi kependudukan di Indonesia. Oleh karena itu, penelitian ini hadir untuk mengisi kesenjangan tersebut dengan memberikan analisis keamanan sistem pengelolaan data kependudukan berdasarkan framework NIST CSF 2.0 (Simangunsong et al., 2019).

1.3. Urgensi Penelitian

Penelitian ini penting dilakukan mengingat meningkatnya ancaman serangan siber terhadap sistem pemerintahan berbasis elektronik, khususnya pada instansi yang mengelola data pribadi masyarakat seperti Dinas Kependudukan dan Pencatatan Sipil. Data kependudukan merupakan data strategis yang digunakan dalam berbagai pelayanan publik sehingga keamanan, kerahasiaan, dan integritas data harus dijaga secara optimal.

Urgensi penelitian ini juga berkaitan dengan belum dilaksanakannya audit keamanan sistem pengelolaan data di Disdukcapil Bengkulu Utara, padahal regulasi nasional telah mewajibkan penerapan standar keamanan informasi berbasis internasional. Penelitian ini diharapkan dapat memberikan gambaran empiris mengenai kondisi keamanan sistem pengelolaan data kependudukan di Disdukcapil Bengkulu Utara berdasarkan framework NIST CSF 2.0 sehingga dapat menjadi dasar evaluasi dan perumusan kebijakan keamanan informasi yang lebih efektif.

Selain itu, penelitian ini penting dilakukan untuk mengidentifikasi area-area yang masih rentan terhadap ancaman siber, khususnya pada fungsi Detect, Respond, dan Recover. Hasil penelitian diharapkan mampu membantu pemerintah daerah dalam meningkatkan tata kelola keamanan informasi, memperkuat infrastruktur keamanan siber, serta meningkatkan kualitas pelayanan publik berbasis digital.

Apabila penelitian ini tidak dilakukan, maka pemerintah daerah dan pengelola sistem informasi akan mengalami keterbatasan data empiris dalam memahami tingkat keamanan sistem yang dimiliki. Akibatnya, kebijakan keamanan informasi berpotensi tidak tepat sasaran, risiko kebocoran data masyarakat semakin tinggi, dan gangguan terhadap pelayanan publik dapat terus terjadi. Selain itu, tidak dilaksanakannya audit keamanan juga dapat menyebabkan rendahnya tingkat kepatuhan terhadap regulasi perlindungan data pribadi dan keamanan sistem pemerintahan berbasis elektronik di Indonesia.

1.4. Penelitian Terdahulu

Penelitian ini terinspirasi oleh beberapa penelitian terdahulu yang berkaitan dengan audit keamanan sistem informasi, manajemen risiko keamanan siber, serta penerapan framework NIST dalam evaluasi keamanan data dan infrastruktur teknologi informasi. Penelitian-penelitian sebelumnya menunjukkan bahwa audit keamanan sistem informasi memiliki variasi fokus, metode, dan pendekatan yang digunakan dalam menilai keamanan sistem pada berbagai sektor, baik pemerintahan, pendidikan, maupun sektor swasta.

Nur Ayu dan Tata Sutabri meneliti pelaksanaan audit keamanan sistem informasi absensi GreatDay menggunakan framework NIST dengan tujuan mengevaluasi keamanan sistem absensi online agar mampu melindungi data pribadi pengguna dari risiko kebocoran sistem. Penelitian tersebut menggunakan metode kuesioner dan wawancara. Hasil penelitian menunjukkan bahwa sistem absensi berada pada level 3, yang berarti prosedur dan pengendalian keamanan sudah diterapkan dengan baik oleh institusi (Wulantari & Sutabri, 2025).

Bernard Ngalim melakukan penelitian mengenai integrasi framework NIST dan ISO dalam audit keamanan siber dan penilaian risiko ke dalam hukum keamanan siber di Cameroon. Penelitian ini menggunakan metode analisis deskriptif dan perbandingan hukum antara standar NIST, ISO, dan regulasi keamanan siber Cameroon. Hasil penelitian menunjukkan bahwa integrasi framework NIST dan ISO mampu memperkuat regulasi keamanan siber nasional serta meningkatkan ketahanan keamanan informasi organisasi (Ngalim, 2023).

Penelitian Reynaldy Gimnastiar, Reni Nursyanti, dan Sardjono membahas audit keamanan dan manajemen risiko pada sistem e-learning UNIBI menggunakan framework NIST. Penelitian ini menggunakan metode kuesioner berbasis NIST SP 800-26 dan NIST SP 800-30 untuk melakukan penilaian keamanan dan risiko sistem. Hasil penelitian menunjukkan tingkat keamanan sistem mencapai 79,14% atau berada pada level 3, meskipun masih ditemukan kerentanan tingkat menengah yang memerlukan perbaikan.

Osama Aljumaiah, Weiwei Jiang, Santosh Reddy Addula, dan Mohammed Amin Almaiah melakukan penelitian mengenai analisis ancaman dan risiko keamanan siber pada infrastruktur teknologi informasi berbasis framework NIST. Penelitian ini menggunakan metode PRISMA terhadap 34 artikel yang berkaitan dengan ancaman pada infrastruktur kritis dan operational technology. Hasil penelitian menunjukkan bahwa faktor manusia menjadi ancaman utama keamanan siber dan implementasi framework NIST dinilai efektif dalam meningkatkan mitigasi risiko keamanan informasi (Aljumaiah et al., 2025).

Selanjutnya, Raiden A.N. Fuy meneliti kesiapan infrastruktur teknologi informasi dalam menunjang penerapan e-government menggunakan framework COBIT 2019. Penelitian ini menggunakan metode mix-method untuk menilai tingkat kapabilitas infrastruktur teknologi informasi. Hasil penelitian menunjukkan sebagian besar domain infrastruktur TI berada pada level kapabilitas rendah, yaitu level 0 hingga level 2, sehingga diperlukan peningkatan signifikan dalam aspek pengelolaan sumber daya, keamanan, monitoring, dan dokumentasi sistem (Tumbade, 2022).

Secara umum, penelitian-penelitian terdahulu menunjukkan bahwa audit keamanan sistem informasi menggunakan framework seperti NIST dan COBIT mampu memberikan gambaran mengenai tingkat keamanan, manajemen risiko, serta kelemahan sistem yang memerlukan perbaikan. Selain itu, sebagian besar penelitian menggunakan pendekatan deskriptif, kuesioner, wawancara, dan analisis risiko dalam mengevaluasi keamanan sistem informasi pada berbagai objek penelitian yang berbeda.

1.5. Pernyataan Kebaruan Ilmiah

Penulis melakukan penelitian yang berbeda dan belum dilakukan oleh penelitian terdahulu. Kebaruan penelitian ini dapat dilihat dari beberapa aspek, yaitu objek penelitian, konteks regulasi, metode analisis, serta framework yang digunakan.

Penelitian ini berfokus pada audit keamanan sistem pengelolaan data kependudukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara yang merupakan instansi pemerintah pengelola data pribadi masyarakat dalam jumlah besar dan bersifat sensitif. Berbeda dengan penelitian Nur Ayu yang berfokus pada sistem absensi perusahaan swasta dan penelitian Reynaldy Gimnastiar yang meneliti sistem e-learning perguruan tinggi, penelitian ini mengkaji keamanan data kependudukan yang memiliki kompleksitas lebih tinggi serta berkaitan langsung dengan perlindungan data pribadi masyarakat.

Selain itu, penelitian ini menggunakan framework NIST Cybersecurity Framework (NIST CSF) 2.0 yang disesuaikan dengan amanat Permendagri Nomor 72 Tahun 2022 mengenai standar keamanan identitas kependudukan digital. Penelitian ini tidak hanya menilai tingkat keamanan sistem, tetapi juga menganalisis kesesuaian implementasi keamanan informasi dengan regulasi nasional

seperti Undang-Undang Perlindungan Data Pribadi dan kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE).

Kebaruan penelitian juga terlihat dari fokus pengkajian pada enam fungsi utama NIST CSF 2.0 yaitu Govern, Identify, Protect, Detect, Respond, dan Recover dalam konteks pelayanan publik dan pengelolaan data kependudukan di pemerintah daerah. Penelitian ini tidak hanya mengidentifikasi tingkat keamanan sistem, tetapi juga mengevaluasi kesiapan tata kelola keamanan informasi, kemampuan deteksi ancaman, respons insiden, serta pemulihan sistem pasca serangan siber.

1.6. Tujuan

Tujuan penelitian ini adalah untuk menganalisis tingkat keamanan sistem pengelolaan data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menggunakan framework NIST Cybersecurity Framework 2.0.

II. METODE

Penelitian ini menggunakan metode statistik deskriptif dengan pendekatan kuantitatif. Pendekatan kuantitatif dipilih karena penelitian ini bertujuan untuk mengukur dan menggambarkan tingkat keamanan sistem pengelolaan data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara berdasarkan framework NIST Cybersecurity Framework (NIST CSF) 2.0 secara objektif dan terukur. Pendekatan ini didasarkan pada filosofi positivisme, di mana proses penelitian dilakukan secara sistematis, terstruktur, dan menggunakan data numerik yang dianalisis melalui teknik statistik deskriptif. Penelitian kuantitatif deskriptif digunakan untuk menjelaskan kondisi keamanan sistem informasi yang sedang berlangsung tanpa melakukan pengujian hipotesis, melainkan menggambarkan tingkat implementasi keamanan siber berdasarkan indikator-indikator yang telah ditentukan.

Metode deskriptif dipilih karena penelitian ini ingin memberikan gambaran nyata mengenai kondisi keamanan sistem pengelolaan data kependudukan di Disdukcapil Bengkulu Utara, khususnya pada aspek Govern, Identify, Protect, Detect, Respond, dan Recover dalam framework NIST CSF 2.0. Dengan pendekatan ini, peneliti dapat mengukur tingkat implementasi keamanan informasi berdasarkan persepsi dan pengalaman responden yang terlibat langsung dalam pengelolaan sistem informasi administrasi kependudukan.

Penelitian ini menggunakan framework NIST Cybersecurity Framework (NIST CSF) 2.0 sebagai dasar operasionalisasi konsep penelitian. Framework tersebut dipilih karena memiliki pendekatan yang komprehensif dalam menilai keamanan sistem informasi dan telah diakui secara internasional sebagai standar pengelolaan risiko keamanan siber. Selain itu, penggunaan NIST CSF 2.0 juga selaras dengan amanat Permendagri Nomor 72 Tahun 2022 yang mewajibkan penerapan standar keamanan informasi berbasis internasional pada pengelolaan data kependudukan.

Sumber data dalam penelitian ini terdiri atas paper atau dokumen, person atau orang, dan place atau tempat. Sumber data dokumen diperoleh melalui peraturan perundang-undangan, laporan instansi, kebijakan keamanan informasi, serta dokumen pendukung lainnya yang berkaitan dengan pengelolaan data kependudukan dan keamanan sistem informasi. Sumber data person diperoleh dari pegawai

Disdukcapil Bengkulu Utara yang menjadi responden penelitian, sedangkan sumber data place berasal dari lokasi penelitian yaitu Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara.

Populasi dalam penelitian ini adalah seluruh pegawai di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara tahun 2025 yang berjumlah 49 orang, terdiri dari 26 orang Aparatur Sipil Negara (ASN), 20 orang Pegawai Pemerintah dengan Perjanjian Kerja (P3K), 2 orang tenaga kebersihan, dan 1 orang tenaga kerja kantor. Populasi tersebut dipilih karena seluruh pegawai memiliki keterkaitan dengan proses pelayanan administrasi kependudukan dan penggunaan sistem informasi dalam aktivitas kerja sehari-hari.

Teknik sampling yang digunakan dalam penelitian ini adalah purposive sampling. Teknik ini dipilih karena penelitian hanya memfokuskan pada responden yang dianggap paling relevan dan memahami pengelolaan sistem informasi di lingkungan Disdukcapil. Sampel penelitian terdiri dari 46 responden, yaitu 26 orang ASN aktif dan 20 orang P3K yang terlibat langsung dalam penggunaan dan pengelolaan sistem informasi administrasi kependudukan. Pemilihan ASN dan P3K sebagai responden dilakukan karena mereka memiliki pengalaman langsung dalam penggunaan sistem pengelolaan data serta memahami prosedur pelayanan administrasi kependudukan, sehingga dinilai mampu memberikan data yang akurat mengenai kondisi keamanan sistem.

Pengumpulan data dilakukan melalui kuesioner dan dokumentasi. Kuesioner digunakan sebagai instrumen utama penelitian untuk memperoleh data primer mengenai tingkat implementasi keamanan sistem berdasarkan framework NIST CSF 2.0. Penyebaran kuesioner dilakukan secara online menggunakan Google Form kepada seluruh responden penelitian. Kuesioner terdiri dari 25 pertanyaan yang disusun berdasarkan indikator pada masing-masing fungsi framework NIST CSF 2.0 dengan menggunakan skala Likert 1–5. Skala tersebut digunakan untuk mengukur tingkat implementasi keamanan sistem mulai dari kondisi belum diterapkan hingga diterapkan secara matang dan berkelanjutan.

III. HASIL DAN PEMBAHASAN

Penulis menganalisis audit keamanan sistem pengelolaan data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menggunakan Framework NIST Cybersecurity Framework (CSF) 2.0 yang terdiri atas enam fungsi utama, yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. Analisis dilakukan berdasarkan hasil penyebaran kuesioner kepada 44 responden yang merupakan ASN dan PPPK aktif di lingkungan Disdukcapil Kabupaten Bengkulu Utara. Data kemudian diolah menggunakan software Microsoft Excel dengan rumus rata-rata (average) untuk mengetahui tingkat implementasi keamanan siber pada setiap fungsi NIST CSF 2.0. Adapun pembahasan hasil audit dapat dilihat pada subbab berikut.

3.1. Hasil Audit Fungsi Govern

Fungsi Govern berfokus pada tata kelola keamanan siber organisasi, termasuk strategi manajemen risiko, kebijakan keamanan, pengawasan, serta pembagian peran dan tanggung jawab dalam menjaga keamanan sistem pengelolaan data.

Tabel 1.

Hasil Audit Fungsi Govern pada Sistem Pengelolaan Data Disdukcapil Bengkulu Utara

No	Indikator	Rata-Rata	Persentase	Tiers Implementation
1	Organizational Context	2,9	58%	Repeatable
2	Risk Management Strategy	2,9	58%	Repeatable
3	Roles, Responsibilities and Authorities	3,1	62%	Repeatable
4	Cybersecurity Policy Implemented	3,1	62%	Repeatable
5	Cybersecurity Supply Chain Risk Managed	3,1	62%	Repeatable
6	Oversight	3,0	60%	Repeatable

Sumber: Hasil Pengolahan Data Penelitian, 2026

Berdasarkan Tabel 1 diketahui bahwa seluruh indikator pada fungsi Govern berada pada kategori Repeatable dengan rata-rata keseluruhan sebesar 3,1 atau 61 persen. Nilai tertinggi terdapat pada indikator Roles, Responsibilities and Authorities, Cybersecurity Policy Implemented, serta Cybersecurity Supply Chain Risk Managed dengan persentase masing-masing sebesar 62 persen. Hal ini menunjukkan bahwa Disdukcapil Bengkulu Utara telah memiliki pembagian tanggung jawab yang cukup jelas terkait keamanan data serta telah menerapkan kebijakan dasar keamanan informasi.

Hasil observasi penulis menunjukkan bahwa pimpinan Disdukcapil telah memberikan perhatian terhadap pengelolaan keamanan data melalui pengawasan rutin terhadap penggunaan sistem SIAK dan pelaksanaan pelayanan administrasi kependudukan. Selain itu, pegawai juga telah memahami pentingnya menjaga kerahasiaan data kependudukan, terutama data Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), dan data biometrik masyarakat.

Namun demikian, indikator Organizational Context dan Risk Management Strategy masih memperoleh nilai 58 persen. Kondisi ini menunjukkan bahwa strategi manajemen risiko keamanan siber belum sepenuhnya berjalan optimal. Berdasarkan hasil dokumentasi dan observasi lapangan, Disdukcapil Bengkulu Utara belum memiliki dokumen audit keamanan informasi secara formal serta belum melaksanakan evaluasi keamanan secara berkala sesuai amanat Permendagri Nomor 72 Tahun 2022.

Penulis menyimpulkan bahwa fungsi Govern pada sistem pengelolaan data Disdukcapil Bengkulu Utara telah berjalan cukup baik dan berada pada kategori Repeatable, namun masih membutuhkan penguatan dalam aspek manajemen risiko, pengawasan berkelanjutan, dan dokumentasi keamanan informasi.

3.2. Hasil Audit Fungsi Identify

Fungsi Identify berfokus pada kemampuan organisasi dalam mengenali aset teknologi informasi, tata kelola keamanan, serta risiko-risiko yang berpotensi mengganggu sistem pengelolaan data.

Tabel 2.
Hasil Audit Fungsi Identify pada Sistem Pengelolaan Data Disdukcapil Bengkulu Utara

No	Indikator	Rata-Rata	Persentase	Tiers Implementation
1	Asset Management	3,1	68%	Repeatable
2	Governance	3,0	60%	Repeatable
3	Risk Assessment	2,9	58%	Repeatable

Sumber: Hasil Pengolahan Data Penelitian, 2026

Berdasarkan Tabel 2 diketahui bahwa fungsi Identify memperoleh rata-rata sebesar 3,0 atau 61 persen dan berada pada kategori Repeatable. Indikator Asset Management memperoleh nilai tertinggi sebesar 68 persen. Hal ini menunjukkan bahwa sebagian besar aset teknologi informasi seperti server utama, server cadangan, komputer pelayanan, serta perangkat biometrik telah dikenali dan diinventarisasi dengan baik oleh Disdukcapil.

Hasil observasi penulis menunjukkan bahwa Disdukcapil Bengkulu Utara memiliki dua server utama yang digunakan untuk mendukung sistem pelayanan administrasi kependudukan, serta 14 unit komputer pelayanan yang digunakan dalam proses perekaman dan pencetakan dokumen kependudukan. Selain itu, perangkat biometrik seperti fingerprint scanner, iris scanner, dan signature pad juga telah digunakan dalam pelayanan KTP elektronik.

Meskipun demikian, indikator Risk Assessment masih memperoleh nilai 58 persen. Hal ini menunjukkan bahwa identifikasi dan analisis risiko keamanan data belum dilakukan secara menyeluruh. Berdasarkan hasil dokumentasi, belum terdapat sistem pemetaan risiko keamanan siber yang terstruktur maupun audit keamanan informasi yang dilakukan secara rutin. Penulis menyimpulkan bahwa fungsi Identify sudah berjalan cukup baik dalam mengenali aset teknologi informasi dan risiko dasar keamanan siber, namun masih memerlukan peningkatan pada aspek penilaian risiko serta tata kelola keamanan informasi secara formal.

3.3. Hasil Audit Fungsi Protect

Fungsi Protect berfokus pada perlindungan sistem, pengendalian akses, keamanan basis data, serta penggunaan teknologi perlindungan untuk menjaga kerahasiaan dan integritas data kependudukan.

Tabel 3.
Hasil Audit Fungsi Protect pada Sistem Pengelolaan Data Disdukcapil Bengkulu Utara

No	Indikator	Rata-Rata	Persentase	Tiers Implementation
1	Identity Management and Access Control	3,1	68%	Repeatable
2	Protect Database	3,5	70%	Repeatable
3	Information Protection Process and Procedures	3,3	66%	Repeatable
4	Maintenance	3,6	72%	Repeatable
5	Protective Technology	3,1	68%	Repeatable

Sumber: Hasil Pengolahan Data Penelitian, 2026

Berdasarkan Tabel 3 diketahui bahwa fungsi Protect memperoleh nilai rata-rata tertinggi dibanding fungsi lainnya, yaitu sebesar 3,3 atau 69 persen dengan kategori Repeatable. Indikator Maintenance memperoleh nilai tertinggi sebesar 72 persen. Hal ini menunjukkan bahwa perawatan sistem dan aplikasi pelayanan kependudukan telah dilakukan secara rutin. Selain itu, indikator Protect Database memperoleh nilai sebesar 70 persen yang menunjukkan bahwa perlindungan data kependudukan melalui sistem keamanan dasar seperti enkripsi dan pembatasan akses sudah diterapkan cukup baik. Berdasarkan hasil observasi, sistem SIAK hanya dapat diakses oleh pegawai tertentu sesuai kewenangan masing-masing.

Namun demikian, hasil observasi lapangan juga menunjukkan bahwa Disdukcapil Bengkulu Utara belum memiliki firewall enterprise, IDS/IPS, antivirus terpusat, maupun segmentasi jaringan yang memadai. Sebagian komputer pelayanan masih menggunakan jaringan umum dan bersifat multi-user sehingga berpotensi meningkatkan risiko kebocoran data.

Hasil wawancara dengan salah satu pegawai bidang operator pelayanan menunjukkan bahwa:

"Untuk keamanan dasar sudah ada seperti password akun dan antivirus biasa, tetapi memang belum ada sistem keamanan yang lebih lengkap seperti firewall khusus atau monitoring otomatis."

Penulis menyimpulkan bahwa fungsi Protect merupakan aspek yang paling kuat dalam sistem keamanan Disdukcapil Bengkulu Utara karena perlindungan teknis dasar telah diterapkan secara rutin. Akan tetapi, penguatan teknologi keamanan modern masih diperlukan agar perlindungan data lebih optimal.

3.4. Hasil Audit Fungsi Detect

Fungsi Detect berfokus pada kemampuan organisasi dalam memantau aktivitas sistem dan mendeteksi ancaman maupun anomali keamanan siber.

Tabel 4.

Hasil Audit Fungsi Detect pada Sistem Pengelolaan Data Disdukcapil Bengkulu Utara

No	Indikator	Rata-Rata	Persentase	Tiers Implementation
1	Continuous Monitoring	3,5	70%	Repeatable
2	Adverse Event Analysis	3,6	70%	Repeatable
3	Continuous Monitoring (Provider)	3,3	66%	Repeatable
4	Detection Processes	2,9	58%	Repeatable

Sumber: Hasil Pengolahan Data Penelitian, 2026

Berdasarkan Tabel 4 diketahui bahwa fungsi Detect memperoleh rata-rata sebesar 3,3 atau 66 persen dan berada pada kategori Repeatable. Indikator Adverse Event Analysis memperoleh nilai tertinggi sebesar 70 persen yang menunjukkan bahwa pegawai cukup mampu mengenali adanya aktivitas mencurigakan pada sistem.

Meskipun demikian, indikator Detection Processes hanya memperoleh nilai sebesar 58 persen. Kondisi ini menunjukkan bahwa prosedur deteksi keamanan siber belum berjalan optimal. Berdasarkan hasil observasi, Disdukcapil Bengkulu Utara belum memiliki sistem SIEM (Security Information and Event Management) maupun mekanisme monitoring otomatis untuk mendeteksi ancaman secara real-time.

Pemantauan aktivitas sistem masih dilakukan secara manual oleh operator dan administrator jaringan. Kondisi ini berpotensi menyebabkan keterlambatan dalam mendeteksi ancaman siber seperti malware, phishing, maupun ransomware. Penulis menyimpulkan bahwa fungsi Detect telah berjalan cukup baik pada aspek pemantauan dasar, namun masih memerlukan peningkatan pada penggunaan teknologi monitoring otomatis dan deteksi ancaman secara real-time.

3.5. Hasil Audit Fungsi Respond

Fungsi Respond berfokus pada kemampuan organisasi dalam merespons insiden keamanan siber serta melakukan mitigasi terhadap dampak gangguan keamanan.

Tabel 5.

Hasil Audit Fungsi Respond pada Sistem Pengelolaan Data Disdukcapil Bengkulu Utara

No	Indikator	Rata-Rata	Persentase	Tiers Implementation
1	Response Planning	3,0	60%	Repeatable
2	Respond Communication	2,9	58%	Repeatable
3	Respond Mitigation	2,8	56%	Repeatable
4	Response Improvements	2,7	54%	Repeatable

Sumber: Hasil Pengolahan Data Penelitian, 2026

Berdasarkan Tabel 5 diketahui bahwa fungsi Respond memperoleh rata-rata sebesar 2,8 atau 57 persen dan berada pada kategori Repeatable. Nilai tertinggi terdapat pada indikator Response Planning sebesar 60 persen. Hasil penelitian menunjukkan bahwa Disdukcapil Bengkulu Utara telah memiliki rencana dasar dalam menangani gangguan sistem. Akan tetapi, belum terdapat simulasi resmi maupun pelatihan penanganan insiden keamanan siber secara berkala.

Berdasarkan hasil wawancara dengan pegawai operator:

"Kalau ada gangguan sistem biasanya langsung koordinasi dengan admin dan pusat, tetapi memang belum pernah ada simulasi khusus penanganan kebocoran data."

Indikator Response Improvements memperoleh nilai terendah sebesar 54 persen. Hal ini menunjukkan bahwa evaluasi terhadap insiden keamanan belum dimanfaatkan secara maksimal untuk memperbaiki sistem keamanan ke depan. Penulis menyimpulkan bahwa fungsi Respond masih

memerlukan peningkatan terutama pada aspek mitigasi, koordinasi penanganan insiden, serta evaluasi pasca-insiden secara sistematis.

3.6. Hasil Audit Fungsi Recover

Fungsi Recover berfokus pada kemampuan organisasi dalam memulihkan sistem dan layanan setelah terjadi gangguan atau insiden keamanan siber.

Tabel 6.
Hasil Audit Fungsi Recover pada Sistem Pengelolaan Data Disdukcapil Bengkulu Utara

No	Indikator	Rata-Rata	Persentase	Tiers Implementation
1	Recover Planning	2,6	52%	Repeatable
2	Recover Improvements	2,5	50%	Repeatable
3	Recover Communications	2,6	52%	Repeatable

Sumber: Hasil Pengolahan Data Penelitian, 2026

Berdasarkan Tabel 6 diketahui bahwa fungsi Recover memperoleh nilai rata-rata terendah yaitu sebesar 2,6 atau 51 persen. Hal ini menunjukkan bahwa kemampuan pemulihan sistem setelah terjadi gangguan keamanan masih belum optimal.

Berdasarkan hasil observasi, Disdukcapil Bengkulu Utara memang telah memiliki server cadangan untuk backup data, namun belum memiliki Disaster Recovery Plan (DRP) yang terstruktur dan teruji secara berkala. Selain itu, belum terdapat penetapan Recovery Time Objective (RTO) maupun Recovery Point Objective (RPO) sebagai standar pemulihan layanan.

Indikator Recover Improvements memperoleh nilai paling rendah sebesar 50 persen. Hal ini menunjukkan bahwa proses evaluasi pasca pemulihan belum dilakukan secara maksimal sebagai bahan perbaikan keamanan sistem. Penulis menyimpulkan bahwa fungsi Recover merupakan aspek yang paling lemah dalam sistem keamanan pengelolaan data Disdukcapil Bengkulu Utara. Oleh karena itu, diperlukan penguatan pada perencanaan pemulihan, simulasi disaster recovery, serta penyusunan standar pemulihan layanan secara formal.

3.7. Pembahasan Hasil Audit Keamanan Sistem Pengelolaan Data Disdukcapil Bengkulu Utara

Secara umum, hasil audit keamanan sistem pengelolaan data Disdukcapil Kabupaten Bengkulu Utara menunjukkan bahwa seluruh fungsi NIST CSF 2.0 berada pada kategori Repeatable dengan rata-rata implementasi pada rentang 51–75 persen. Kondisi ini menunjukkan bahwa prosedur keamanan siber dasar telah diterapkan dan dijalankan secara rutin, namun belum sepenuhnya terdokumentasi secara formal serta belum didukung sistem monitoring dan evaluasi yang matang.

Fungsi Protect menjadi fungsi paling kuat dengan rata-rata sebesar 69 persen karena telah didukung perlindungan dasar seperti pembatasan akses, enkripsi data, antivirus, serta pemeliharaan sistem yang dilakukan secara rutin. Sementara itu, fungsi Recover menjadi fungsi paling lemah dengan rata-rata sebesar 51 persen karena belum adanya Disaster Recovery Plan yang matang dan pengujian pemulihan sistem secara berkala.

Hasil penelitian ini menunjukkan bahwa Disdukcapil Bengkulu Utara telah memiliki fondasi keamanan siber yang cukup baik dalam mendukung pelayanan administrasi kependudukan. Akan tetapi, untuk menghadapi ancaman siber yang semakin kompleks, diperlukan peningkatan pada aspek deteksi ancaman otomatis, respons insiden, serta pemulihan layanan pasca gangguan agar sistem keamanan pengelolaan data dapat berjalan lebih efektif, adaptif, dan berkelanjutan.

3.8. Diskusi Temuan Utama Penelitian

Hasil penelitian menunjukkan bahwa audit keamanan sistem pengelolaan data pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menggunakan framework NIST Cybersecurity Framework (CSF) 2.0 secara umum berada pada kategori *Repeatable*. Kondisi ini

menunjukkan bahwa prosedur keamanan siber dasar telah diterapkan dan dijalankan secara rutin oleh organisasi, meskipun belum sepenuhnya terdokumentasi secara formal dan belum didukung oleh sistem keamanan otomatis yang matang. Penulis menemukan bahwa fungsi Protect menjadi aspek paling kuat dalam sistem keamanan Disdukcapil Bengkulu Utara, sedangkan fungsi Recover menjadi aspek paling lemah karena belum adanya Disaster Recovery Plan (DRP) yang teruji secara berkala serta belum adanya standar Recovery Time Objective (RTO) dan Recovery Point Objective (RPO).

Sama halnya dengan temuan penelitian sebelumnya oleh Nur Ayu dan Tata Sutabri bahwa implementasi framework NIST mampu menunjukkan tingkat keamanan sistem informasi yang sudah berjalan cukup baik pada level operasional organisasi. Penelitian Nur Ayu dan Tata Sutabri menemukan bahwa sistem absensi GreatDay telah berada pada level keamanan yang cukup baik karena prosedur pengendalian keamanan sudah diterapkan secara konsisten oleh institusi. Temuan penelitian ini memperkuat hasil penelitian tersebut karena Disdukcapil Bengkulu Utara juga telah menerapkan prosedur keamanan dasar secara berulang, terutama pada aspek pengendalian akses, pemeliharaan sistem, serta perlindungan data kependudukan melalui pembatasan hak akses pengguna.

Selain itu, temuan penelitian ini juga sejalan dengan penelitian Reynaldy Gimnastiar, Reni Nursyanti, dan Sardjono mengenai audit keamanan sistem e-learning UNIBI menggunakan framework NIST. Penelitian tersebut menunjukkan bahwa sistem keamanan organisasi dapat berada pada kategori cukup baik meskipun masih ditemukan kerentanan yang memerlukan peningkatan. Sama halnya dengan penelitian tersebut, penulis menemukan bahwa Disdukcapil Bengkulu Utara telah memiliki fondasi keamanan siber yang cukup baik, namun masih memiliki kelemahan pada aspek monitoring otomatis, deteksi ancaman real-time, respons insiden, dan pemulihan sistem pasca gangguan keamanan.

Temuan penelitian ini juga memperkuat hasil penelitian Osama Aljumaiah dkk. yang menyatakan bahwa faktor manusia menjadi salah satu aspek penting dalam keamanan siber organisasi. Dalam penelitian ini, penulis menemukan bahwa pemahaman pegawai mengenai pentingnya menjaga kerahasiaan data kependudukan sudah cukup baik. Pegawai telah memahami pentingnya menjaga keamanan data Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), serta data biometrik masyarakat. Akan tetapi, keterbatasan pelatihan keamanan siber dan belum adanya simulasi penanganan insiden menyebabkan kesiapsiagaan organisasi dalam menghadapi ancaman siber masih belum optimal.

Berbeda dengan penelitian Bernard Ngalim yang menitikberatkan pada integrasi framework NIST dan ISO dalam regulasi keamanan siber nasional, penelitian ini lebih berfokus pada implementasi teknis keamanan sistem pengelolaan data kependudukan di lingkungan pemerintah daerah. Penelitian Bernard menunjukkan bahwa integrasi standar keamanan mampu memperkuat ketahanan keamanan informasi secara nasional, sedangkan penelitian ini menemukan bahwa tantangan utama di tingkat pemerintah daerah justru terletak pada implementasi teknis, dokumentasi keamanan, keterbatasan infrastruktur keamanan modern, dan minimnya pengujian pemulihan sistem secara berkala.

Temuan penelitian ini juga memiliki kesamaan dengan penelitian Raiden A.N. Fuy mengenai kesiapan infrastruktur teknologi informasi berbasis COBIT 2019 yang menunjukkan masih rendahnya kapabilitas tata kelola teknologi informasi pada organisasi pemerintah. Dalam penelitian ini, penulis menemukan bahwa Disdukcapil Bengkulu Utara memang telah memiliki infrastruktur dasar keamanan sistem informasi, namun belum didukung oleh perangkat keamanan modern seperti firewall enterprise, IDS/IPS, antivirus terpusat, maupun sistem SIEM untuk monitoring ancaman secara otomatis. Kondisi tersebut menunjukkan bahwa keamanan sistem masih bergantung pada pengawasan manual operator dan administrator jaringan.

Penulis menemukan temuan penting bahwa kekuatan utama keamanan sistem Disdukcapil Bengkulu Utara terletak pada fungsi Protect yang memperoleh persentase tertinggi sebesar 69 persen. Hal ini menunjukkan bahwa perlindungan dasar terhadap sistem dan data kependudukan sudah diterapkan cukup baik melalui pembatasan akses akun, penggunaan password, antivirus dasar, enkripsi

data, serta pemeliharaan sistem secara rutin. Temuan ini memperlihatkan bahwa organisasi telah memiliki kesadaran terhadap pentingnya perlindungan data pribadi masyarakat dalam pelayanan administrasi kependudukan.

Di sisi lain, fungsi Recover memperoleh persentase terendah yaitu sebesar 51 persen. Temuan ini menunjukkan bahwa kemampuan pemulihan sistem setelah terjadi insiden keamanan siber masih menjadi kelemahan utama organisasi. Kondisi tersebut terlihat dari belum adanya Disaster Recovery Plan yang terstruktur, belum adanya simulasi pemulihan data secara berkala, serta belum ditetapkannya standar waktu pemulihan layanan apabila terjadi gangguan sistem. Temuan ini menunjukkan bahwa keamanan siber pada organisasi pemerintah daerah masih cenderung berfokus pada pencegahan dasar, namun belum sepenuhnya siap menghadapi skenario serangan siber berskala besar.

Secara umum, hasil penelitian ini menunjukkan bahwa implementasi framework NIST CSF 2.0 mampu memberikan gambaran yang jelas mengenai tingkat keamanan sistem pengelolaan data kependudukan di Disdukcapil Kabupaten Bengkulu Utara. Penelitian ini juga memperlihatkan bahwa keamanan siber pada sektor pemerintahan daerah memerlukan penguatan tidak hanya pada aspek perlindungan teknis, tetapi juga pada tata kelola, deteksi ancaman otomatis, respons insiden, serta pemulihan layanan agar mampu menghadapi ancaman siber yang semakin kompleks.

3.9. Diskusi Temuan Menarik Lainnya

Penulis menemukan beberapa temuan menarik lain selama pelaksanaan penelitian. Salah satu faktor pendukung implementasi keamanan sistem pengelolaan data di Disdukcapil Bengkulu Utara adalah adanya kesadaran pegawai terhadap pentingnya menjaga kerahasiaan data kependudukan masyarakat. Pegawai memahami bahwa data seperti Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), dan data biometrik merupakan data sensitif yang harus dijaga kerahasiaannya agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Selain itu, keberadaan server cadangan dan pemeliharaan sistem secara rutin juga menjadi faktor pendukung dalam menjaga keberlangsungan pelayanan administrasi kependudukan. Perawatan aplikasi pelayanan yang dilakukan secara berkala membantu meminimalisasi gangguan sistem dan menjaga stabilitas pelayanan publik di lingkungan Disdukcapil Bengkulu Utara.

Namun demikian, penulis juga menemukan beberapa faktor penghambat dalam implementasi keamanan siber. Salah satunya adalah keterbatasan infrastruktur keamanan modern seperti belum tersedianya firewall enterprise, IDS/IPS, antivirus terpusat, dan sistem SIEM untuk monitoring ancaman secara real-time. Kondisi ini menyebabkan proses deteksi ancaman dan monitoring keamanan masih dilakukan secara manual oleh operator dan administrator jaringan.

Faktor penghambat lainnya adalah belum adanya pelatihan keamanan siber dan simulasi penanganan insiden secara berkala bagi pegawai. Akibatnya, kesiapsiagaan organisasi dalam menghadapi ancaman siber seperti ransomware, phishing, maupun kebocoran data masih belum optimal. Selain itu, belum adanya Disaster Recovery Plan yang terstruktur menyebabkan proses pemulihan layanan pasca gangguan belum memiliki standar operasional yang jelas dan terukur.

IV. KESIMPULAN

Penulis menyimpulkan bahwa hasil audit keamanan sistem pengelolaan data di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara menggunakan framework NIST Cybersecurity Framework (CSF) 2.0 menunjukkan bahwa seluruh fungsi keamanan siber berada pada kategori *Repeatable*. Hal ini menunjukkan bahwa prosedur keamanan dasar telah diterapkan dan dijalankan secara rutin dalam mendukung pelayanan administrasi kependudukan.

Fungsi Protect menjadi aspek paling kuat karena telah didukung oleh perlindungan dasar seperti pembatasan akses, pemeliharaan sistem, antivirus, dan enkripsi data. Sementara itu, fungsi Recover menjadi aspek paling lemah karena belum adanya Disaster Recovery Plan, standar pemulihan layanan, serta pengujian pemulihan sistem secara berkala.

Secara umum, Disdukcapil Kabupaten Bengkulu Utara telah memiliki fondasi keamanan siber yang cukup baik, namun masih memerlukan peningkatan pada aspek tata kelola keamanan informasi, deteksi ancaman otomatis, respons insiden, serta pemulihan layanan agar keamanan sistem pengelolaan data dapat berjalan lebih efektif, adaptif, dan berkelanjutan.

Keterbatasan Penelitian. Penelitian ini memiliki keterbatasan pada ruang lingkup penelitian yang hanya dilakukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara serta menggunakan metode kuesioner, observasi, dan wawancara dengan jumlah responden terbatas. Selain itu, penelitian belum melakukan pengujian penetrasi sistem secara teknis karena keterbatasan waktu, akses, dan kebijakan keamanan instansi.

Arah Masa Depan Penelitian (*future work*). Penulis menyarankan agar penelitian selanjutnya dapat melakukan audit keamanan siber dengan cakupan yang lebih luas menggunakan metode penetration testing, vulnerability assessment, maupun integrasi framework keamanan lainnya seperti ISO 27001 dan COBIT. Penelitian selanjutnya juga dapat mengkaji kesiapan implementasi keamanan siber berbasis Artificial Intelligence (AI) dan Security Information and Event Management (SIEM) pada sektor pemerintahan daerah guna meningkatkan ketahanan keamanan informasi secara berkelanjutan.

V. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Kepala Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkulu Utara beserta seluruh jajaran yang telah memberikan izin, dukungan, serta kesempatan kepada penulis untuk melaksanakan penelitian di lingkungan Disdukcapil Kabupaten Bengkulu Utara. Ucapan terima kasih juga penulis sampaikan kepada seluruh pegawai ASN dan PPPK yang telah bersedia menjadi responden dan memberikan informasi selama proses penelitian berlangsung.

VI. DAFTAR PUSTAKA

Aljumaiah, O., Jiang, W., Reddy Addula, S., & Amin Almaiah, M. (2025). Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. *Journal of Cyber Security and Risk Auditing*, *2025*(2). https://doi.org/10.63180/jcsra.thestap.2025.2.2

Arsento, M., Hamdi, M., Ngadisah, & Simangunsong, F. (2022). The Implementation of Waste Management Policy in Creating a Clean, Comfortable and Healty Environment at the City of Jambi Jambi Province. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, *5*(1). https://www.bircu-journal.com/index.php/birci/article/download/3789/pdf

Bakunzibake, P., Klein, G. O., & Islam, S. M. (2019). E-government implementation and monitoring: The case of Rwanda's 'one-stop' E-government. *Electronic Journal of Information Systems in Developing Countries*, *85*(5). https://doi.org/10.1002/isd2.12086

Gatiningsih. (2015). Identifikasi Data Base Kependudukan Sebagai Produk Pelaksanaan Sistem Informasi Administrasi Kependudukan (SIAK) di Kabupaten Bandung. *Jurnal Dukcapil*, *3*(2), 107–126. https://eprints.ipdn.ac.id/2404/

Gatiningsih. (2022). Strategi Peningkatan Kualitas Pelayanan Akte Kematian Berbasis Digital di Kota Medan. In *IPDN* (Number 1). http://eprints2.ipdn.ac.id/id/eprint/1012/

Gimnastiar, R., Nursyanti, R., & ... (2024). Audit Keamanan Dan Manajemen Risiko Dengan Menggunakan Framework NIST (Studi Kasus: E-Learning UNIBI). *Seminar Nasional*

Hamzah, M. (2018). SKRIPSI 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. In *UIN Repository* (Number 1).

Hooda, A., Gupta, P., Jeyaraj, A., & Dwivedi, Y. (2023). Clarifying the Role of E-Government Trust in E-Government Success Models: A Meta-analytic Structural Equation Modeling Approach. *Australasian Journal of Information Systems*, *27*. https://doi.org/10.3127/ajis.v27i0.4079

Indrajit, R. E. (2016). Konsep dan Strategi Electronic Government. *Electronic Government*, *84*, 1–166.

Jogiyanto H.M. (2018). Konsep Dasar Sistem dan Informasi - Sistem Informasi Manajemen (Edisi 3). *Yayasan Cendikia Mulia Mandiri*, 1–32.

Marthalina, M., Dione, F., & Saribulan, N. (2025). Determining Factors of Digital Public Service Management Implementation Policy at Subdistrict Level in South Jakarta City. *Jurnal Manajemen Pelayanan Publik*, *9*(2). https://doi.org/10.24198/jmpp.v9i2.59855

Mphahlele, N. S., Kekwaletswe, R. M., & Seaba, T. R. (2025). Model to explain use of E-Government service change: Use of unified theory of acceptance and use of technology and information systems success model to explain use of E-Government service change: Emerging market case. *Telematics and Informatics Reports*, *17*. https://doi.org/10.1016/j.teler.2025.100190

Muthi'atur Rofi'ah, D. (2025). Nist Cybersecurity Framework in the Lens of Indonesian Internal Auditors. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, *8*(2), 3349–3367.

Ndraha, T. (2003). *KYBERNOLOGI ILMU PEMERINTAHAN.* Jakarta: PT RINEKA CIPTA

Ngalim, B. (2023). Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law. *Journal of Cybersecurity Education Research and Practice*, *2024*(1). https://doi.org/10.32727/8.2023.29

Nurdin, I., & Hartati, S. (2019). *Metodologi Penelitian Sosial*.77-74

Saputra Rambe, A., Oktalisa, E., & Tinggi Ilmu Administrasi, S. (2021). SENGKUNI Journal-Social Sciences and Humanities Inovasi dalam Pelayanan Publik: Studi Kasus Implementasi E-Government di Negara-Negara Berkembang ARTICLE HISTORY. *Sengkuni Journal: Social Sciences and Humanities*, *2*(2), 165–170.

Setiyawati, B. R., Widyarti, M. T. H., & Romangsi, I. N. (2025). Implementation of Good Corporate Governance Principles in Village Fund Management in Jambanan Village Government, Sidoharjo, Sragen. *Data: Journal of Information Systems and Management*. https://journal.idscipub.com/index.php/data/article/view/472

Sharma, S., Kar, A. K., & Gupta, M. P. (2025). Building Accountability in e-government Services: Inputs for Policy. *Australasian Journal of Information Systems*, *29*. https://doi.org/10.3127/ajis.v29.5175

Simangunsong, F., Hutasoit, I., & Sentosa, I. (2019). A strategic framework of good governance, infrastructure development and community empowerment in indonesian public sector management. *African Journal of Hospitality, Tourism and Leisure*, *2019*(Special Issue). https://www.researchgate.net/publication/344397576_A_strategic_framework_of_good_governance_infrastructure_development_and_community_empowerment_in_Indonesian_Public_Sector_Management

Sugiyono. (2018). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Suwanda, D. (2015). Factors Affecting Quality of Local Government Financial Statements to Get Unqualified Opinion (WTP) of Audit Board of the Republic of Indonesia (BPK). *Research Journal of Finance and Accounting*, *6*(4). https://www.researchgate.net/profile/Mohd-

Kadri/post/What-factors-affects-influences-quality-of-financial-reporting-quality-in-the-governmental-sector-other-than-accounting-standardization/attachment/59d62e8179197b807798cb3b/AS%3A354564868984832%401461546

Tumbade, M. O. (2022). SISTEM INFORMASI DALAM MENDUKUNG KEMATANGAN PLANNING SMART CITY E-GOVERNMENT UNTUK PENINGKATAN KAPABILITAS PELAYANAN PEMERINTAH LOMBOK TIMUR TERHADAP MASYARAKAT. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *9*(3). https://doi.org/10.35957/jatisi.v9i3.2225

Wulantari, N. A., & Sutabri, T. (2025). Pelaksanaan Audit Keamanan Sistem Informasi Absensi Greatday Menggunakan Framework NIST. *Jurnal JUPITER*, *17*(1). https://jurnal.polsri.ac.id/index.php/jupiter/article/view/10314/3509