Jurnal Sistem Komputer dan Kecerdasan Buatan
Volume IX Nomor 3 Mei 2026

Implementasi NIST *Cybersecurity Framework* untuk Manajemen Risiko Keamanan Sistem Informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk

Rafif Endra Putra[1], Ikra Novar Rizqi[2]

Institut Pemerintahan Dalam Negeri, Jl. Ir. Soekarno KM 20, Jatinangor, Sumedang, Jawa Barat
rafifendraputra@gmail.com

Diterima : 30 April 2026
Disetujui : 20 Mei 2026

***Abstrak*— Perkembangan *e-government* dan Sistem Pemerintahan Berbasis Elektronik (SPBE) meningkatkan penggunaan layanan publik digital di Kabupaten Nganjuk. Kondisi tersebut juga meningkatkan risiko ancaman siber, kebocoran data, dan gangguan layanan. Dinas Komunikasi dan Informatika Kabupaten Nganjuk telah membentuk *Computer Security Incident Response Team* (CSIRT) dan menerapkan ISO/IEC 27001:2022, namun hasil audit keamanan informasi tahun 2025 menunjukkan tingkat kepatuhan baru mencapai 72% dari standar minimal 80%. Penelitian ini bertujuan mengevaluasi implementasi manajemen risiko keamanan sistem informasi berdasarkan lima fungsi inti NIST *Cybersecurity Framework* versi 1.1. Penelitian menggunakan metode kualitatif deskriptif dengan teknik pengumpulan data melalui wawancara, observasi, dan studi dokumentasi. Hasil penelitian menunjukkan bahwa implementasi keamanan sistem informasi telah berjalan, namun belum optimal pada aspek dokumentasi aset, *monitoring* jaringan, pengelolaan hak akses, pengujian *restore backup*, dan pengelolaan risiko pihak ketiga. Penelitian ini merekomendasikan penguatan tata kelola keamanan informasi melalui peningkatan dokumentasi aset, pemantauan keamanan, dan evaluasi keamanan secara berkala guna mendukung layanan publik digital yang aman dan berkelanjutan.**

***Keywords* — Keamanan sistem informasi, kerangka kerja NIST, manajemen risiko, pemerintah daerah**

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital dalam penyelenggaraan pemerintahan, khususnya pada pelayanan publik berbasis elektronik. Berdasarkan data Badan Pusat Statistik tahun 2024, jumlah pengguna internet di Indonesia mencapai 221,6 juta jiwa atau sekitar 79,5% dari total populasi nasional[1]. Kondisi tersebut menunjukkan bahwa pemanfaatan teknologi digital terus meningkat dan memengaruhi berbagai sektor, termasuk pemerintahan daerah. Implementasi digitalisasi pemerintahan juga ditandai dengan meningkatnya penerapan e-government dan Sistem Pemerintahan Berbasis Elektronik (SPBE) untuk meningkatkan efektivitas pelayanan publik[2].

Dinas Komunikasi dan Informatika Kabupaten Nganjuk sebagai perangkat daerah yang bertanggung jawab dalam pengelolaan teknologi informasi memiliki peran penting dalam mendukung layanan digital pemerintah daerah. Pemanfaatan sistem informasi memberikan manfaat berupa peningkatan efisiensi pelayanan, percepatan akses informasi, dan kemudahan administrasi masyarakat. Namun demikian, peningkatan penggunaan teknologi digital juga

menimbulkan risiko keamanan informasi dan ancaman siber yang semakin kompleks[3]. Sebagai upaya penanganan ancaman siber, Pemerintah Kabupaten Nganjuk telah membentuk *Computer Security Incident Response Team* (CSIRT) berdasarkan Keputusan Bupati Nganjuk Nomor 10 Tahun 2020 untuk mendukung pengelolaan keamanan informasi dan penanganan insiden siber[4].

Ancaman keamanan siber pada sektor pemerintahan menjadi perhatian penting karena dapat memengaruhi keberlangsungan layanan publik dan keamanan data masyarakat. Berdasarkan laporan keamanan siber nasional tahun 2023, terdapat ratusan insiden keamanan siber pada sektor pemerintahan yang didominasi oleh ransomware dan kebocoran data[5]. Selain itu, hasil audit ISO/IEC 27001:2022 pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk menunjukkan tingkat kepatuhan keamanan informasi belum mencapai target optimal sehingga masih diperlukan penguatan tata kelola keamanan sistem informasi[6]. Kondisi tersebut menunjukkan bahwa keamanan sistem informasi tidak hanya menjadi aspek teknis, tetapi juga bagian penting dalam menjaga keberlangsungan layanan pemerintahan digital.

Beberapa penelitian sebelumnya telah membahas manajemen risiko keamanan informasi menggunakan framework seperti NIST *Cybersecurity Framework* (CSF), ISO 27001, dan COBIT. Penelitian oleh Mifta Fadya dan Ditdit Nugraha Utama menunjukkan bahwa integrasi NIST CSF dan COBIT mampu mengidentifikasi gap keamanan dan tingkat kematangan keamanan informasi organisasi publik [7]. Penelitian lain oleh Agus Aminudin dan Aji Supriyanto menemukan bahwa sebagian besar area keamanan informasi pada instansi pemerintah daerah masih berada pada tingkat kematangan awal dan memerlukan penguatan prosedur keamanan[8]. Namun demikian, implementasi NIST CSF secara komprehensif pada pemerintah daerah masih relatif terbatas sehingga penelitian lebih lanjut masih diperlukan[8].

Berbeda dengan penelitian sebelumnya yang umumnya berfokus pada pengukuran tingkat kematangan keamanan informasi atau integrasi beberapa *framework* keamanan, penelitian ini secara khusus mengevaluasi implementasi manajemen risiko keamanan sistem informasi pada instansi pemerintah daerah menggunakan lima fungsi inti NIST *Cybersecurity Framework* versi 1.1 secara menyeluruh. Penelitian ini juga memanfaatkan data audit ISO/IEC 27001:2022, implementasi CSIRT, dan temuan insiden keamanan digital sebagai dasar evaluasi kondisi keamanan informasi di lingkungan Dinas Komunikasi dan Informatika Kabupaten Nganjuk. Selain itu, penerapan NIST *Cybersecurity Framework* pada pemerintah daerah masih relatif terbatas sehingga penelitian ini diharapkan dapat memberikan kontribusi berupa pemetaan *gap* keamanan informasi dan rekomendasi penguatan tata kelola keamanan sistem informasi yang lebih praktis dan sesuai dengan kebutuhan organisasi sektor publik daerah.

Berdasarkan kondisi tersebut, NIST *Cybersecurity Framework* versi 1.1 dipilih karena memiliki pendekatan berbasis risiko yang bersifat fleksibel, adaptif, dan mudah diterapkan pada berbagai jenis organisasi, termasuk instansi pemerintah daerah. Selain itu, NIST *Cybersecurity Framework* menyediakan lima fungsi inti yang mampu membantu organisasi dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan insiden keamanan informasi secara sistematis. Berbeda dengan pendekatan sertifikasi seperti ISO/IEC 27001 yang lebih berfokus pada pemenuhan standar pengelolaan keamanan informasi, NIST *Cybersecurity Framework* lebih menekankan pada evaluasi kondisi implementasi keamanan dan pengelolaan risiko keamanan siber secara operasional. Oleh karena itu, framework ini dinilai sesuai untuk mengevaluasi implementasi manajemen risiko keamanan sistem informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk.

Penelitian ini bertujuan untuk menganalisis manajemen risiko keamanan sistem informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk menggunakan NIST *Cybersecurity Framework* versi 1.1 dengan fokus pada lima fungsi inti, yaitu *Identify, Protect, Detect, Respond,* dan *Recover*. Hasil penelitian

menunjukkan bahwa implementasi keamanan sistem informasi telah berjalan melalui penerapan regulasi keamanan informasi, pembentukan CSIRT, dan pengelolaan sistem keamanan digital. Namun demikian, masih ditemukan beberapa kelemahan seperti belum optimalnya dokumentasi aset, keterbatasan monitoring keamanan, serta perlunya penguatan prosedur respons dan pemulihan insiden. Oleh karena itu, diperlukan penguatan tata kelola keamanan sistem informasi guna mendukung layanan publik digital yang lebih aman, efektif, dan berkelanjutan.

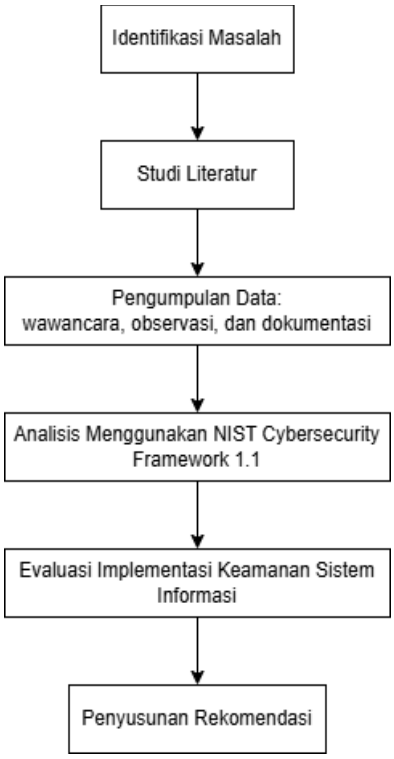
II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk. Pendekatan kualitatif digunakan untuk memahami kondisi implementasi manajemen risiko keamanan sistem informasi secara mendalam berdasarkan situasi dan kondisi nyata organisasi. Menurut Sugiyono, pendekatan kualitatif digunakan untuk memahami fenomena secara holistik dan kontekstual[9].

Fokus penelitian diarahkan pada analisis manajemen risiko keamanan sistem informasi menggunakan NIST *Cybersecurity Framework* (CSF) versi 1.1. Analisis dibatasi pada lima fungsi inti *Framework Core,* yaitu *Identify, Protect, Detect, Respond,* dan *Recover*[10]. Kelima fungsi tersebut digunakan sebagai dasar evaluasi implementasi keamanan sistem informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk.

Teknik pengumpulan data dilakukan melalui wawancara, observasi, dan studi dokumentasi. Wawancara dilakukan terhadap enam informan yang terlibat dalam pengelolaan keamanan sistem informasi di lingkungan Dinas Komunikasi dan Informatika Kabupaten Nganjuk. Observasi dilakukan terhadap implementasi pengamanan sistem informasi dan tata kelola keamanan digital, sedangkan studi dokumentasi dilakukan terhadap regulasi, laporan keamanan informasi, dokumen kebijakan, dan dokumen pendukung lainnya.

Tahapan penelitian dimulai dari identifikasi masalah, pengumpulan data, pemetaan hasil penelitian berdasarkan lima fungsi inti NIST *Cybersecurity Framework* versi 1.1, hingga penyusunan rekomendasi peningkatan tata kelola keamanan informasi. Alur penelitian ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian

Analisis data dilakukan secara deskriptif kualitatif dengan memetakan hasil penelitian ke dalam kategori dan subkategori NIST *Cybersecurity Framework* versi 1.1. Hasil analisis digunakan untuk mengidentifikasi kondisi implementasi keamanan sistem informasi, menemukan kelemahan pengelolaan risiko, serta menyusun rekomendasi peningkatan tata kelola keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk.

III. HASIL DAN PEMBAHASAN

Analisis dalam penelitian ini dilakukan dengan mengadopsi lima fungsi inti NIST *Cybersecurity Framework* (NIST CSF) versi 1.1, yaitu *Identify, Protect, Detect, Respond*, dan *Recover*. Framework tersebut digunakan sebagai dasar

untuk mengevaluasi implementasi manajemen risiko keamanan sistem informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk.

Proses analisis dilakukan melalui beberapa tahapan, yaitu pengumpulan data melalui wawancara, observasi, dan studi dokumentasi, kemudian hasil data dipetakan ke dalam kategori dan subkategori NIST *Cybersecurity Framework* versi 1.1. Selanjutnya, hasil pemetaan dibandingkan dengan standar implementasi keamanan informasi pada masing-masing fungsi NIST CSF untuk mengetahui kondisi penerapan keamanan sistem informasi, menemukan kelemahan pengelolaan keamanan, serta menyusun rekomendasi peningkatan tata kelola keamanan informasi.

Teknik pembuktian hasil penelitian dilakukan melalui triangulasi data, yaitu dengan membandingkan hasil wawancara, observasi lapangan, dan studi dokumentasi agar hasil penelitian lebih valid dan tidak hanya berdasarkan pernyataan informan. Observasi dilakukan terhadap implementasi pengamanan sistem, monitoring jaringan, pengelolaan akses, dan aktivitas operasional keamanan informasi, sedangkan studi dokumentasi dilakukan terhadap SOP keamanan informasi, dokumen kebijakan, log monitoring, risk register, dokumen backup, serta dokumen pendukung lainnya.

Tabel 1. Ringkasan Hasil Analisis Implementasi NIST *Cybersecurity Framework*

Fungsi NIST CSF	Kondisi Implementasi	Bukti Hasil Observasi & Dokumentasi	Gap yang Ditemukan
Identify	Identifikasi aset telah dilakukan	Tersedia SIMASET, daftar aplikasi, label perangkat server dan jaringan	Belum tersedia klasifikasi risiko dan diagram arsitektur sistem lengkap
Protect	Kontrol akses dan perlindungan sistem telah diterapkan	Penggunaan akun pribadi, firewall, antivirus, CCTV, backup NAS, SOP login/logout	SOP password dan dokumen hak akses belum lengkap, pelatihan keamanan belum terdokumentasi
Detect	Monitoring sistem telah berjalan	Monitoring menggunakan Zabbix dan Wazuh, logbook gangguan, ticketing	Logging dan analisis keamanan belum terdokumentasi menyeluruh
Respond	Penanganan insiden telah dilakukan melalui CSIRT	SOP penanganan insiden, logbook gangguan, koordinasi internal	Evaluasi pascainsiden dan dokumentasi analisis akar masalah belum optimal
Recover	Backup dan pemulihan sistem telah dilakukan	NAS backup, SOP recovery, backup harian, Disaster Recovery Center	Pengujian restore berkala belum dilakukan secara menyeluruh

A. Identify

Fungsi *Identify* pada NIST *Cybersecurity Framework* digunakan untuk memahami aset organisasi, sistem informasi, serta risiko keamanan siber yang dimiliki organisasi. Pada penelitian ini, proses identifikasi dilakukan melalui observasi lapangan, wawancara, dan studi dokumentasi terhadap pengelolaan teknologi informasi di Dinas Komunikasi dan Informatika Kabupaten Nganjuk.

Berdasarkan hasil studi dokumentasi, organisasi telah memiliki dokumentasi aset teknologi informasi berupa daftar server fisik pada aplikasi SIMASET BPKAD dan pencatatan perangkat jaringan pada dokumen internal. Selain itu, tersedia pula daftar aplikasi atau sistem informasi yang dikelola oleh tim terkait. Hasil observasi juga menunjukkan bahwa perangkat utama seperti *server, router, switch,* dan *storage* telah diberi label identifikasi sehingga memudahkan pengelolaan aset teknologi informasi.

Organisasi juga telah memiliki kebijakan keamanan informasi berupa SK Bupati tentang Sistem Manajemen Keamanan Informasi serta pembentukan *Computer Security Incident Response Team* (CSIRT) sebagai bentuk penguatan tata kelola keamanan informasi pemerintah daerah. Namun demikian, hasil studi dokumentasi menunjukkan bahwa diagram arsitektur sistem informasi yang lengkap dan resmi belum tersedia. Selain itu, klasifikasi risiko terhadap aset dan prioritas pengamanan sistem informasi juga belum terdokumentasi secara menyeluruh.

Berdasarkan perbandingan dengan kategori *Asset Management* dan *Risk Assessment* pada NIST *Cybersecurity Framework* versi 1.1, kondisi tersebut menunjukkan bahwa proses identifikasi aset dan pengelolaan risiko keamanan informasi masih memerlukan peningkatan, khususnya pada aspek dokumentasi arsitektur sistem, pemetaan risiko keamanan informasi, dan penetapan prioritas pengamanan aset digital[10].

B. Protect

Fungsi *Protect* bertujuan untuk memastikan tersedianya mekanisme perlindungan terhadap sistem informasi dan data organisasi. Implementasi fungsi *Protect* dianalisis melalui observasi terhadap aktivitas operasional serta studi dokumentasi kebijakan keamanan informasi.

Berdasarkan hasil observasi, penerapan kontrol akses telah dilakukan melalui penggunaan akun pribadi pada *workstation* operator dan programmer. Komputer juga dikunci ketika tidak digunakan sementara dan *screen timeout* aktif secara otomatis. Selain itu, ruang server menggunakan pintu besi dengan kartu akses terbatas, dilengkapi CCTV, serta pendingin ruangan yang berfungsi dengan baik. Hasil observasi juga menunjukkan penggunaan perangkat keamanan seperti firewall, antivirus, dashboard monitoring Zabbix dan Wazuh, serta keberadaan NAS dan HDD backup sebagai media cadangan data.

Hasil studi dokumentasi menunjukkan bahwa organisasi telah memiliki beberapa kebijakan keamanan informasi seperti SK Bupati tentang Sistem Manajemen Keamanan Informasi, SOP login/logout sistem, serta SOP penanganan insiden siber. Pembatasan akses terhadap sistem tertentu juga telah diterapkan untuk mengurangi risiko penyalahgunaan akses oleh pihak yang tidak berwenang.

Namun demikian, dokumen khusus terkait pengelolaan password dan pengelolaan hak akses belum ditemukan secara lengkap. Selain itu, dokumen pelatihan atau sosialisasi keamanan informasi bagi pegawai juga belum dapat dikonfirmasi dari hasil studi dokumentasi. Kondisi tersebut menunjukkan bahwa implementasi perlindungan keamanan informasi masih memerlukan penguatan pada aspek dokumentasi keamanan teknis dan peningkatan kesadaran keamanan informasi bagi pengguna sistem.

Berdasarkan kategori *Access Control, Data Security, dan Protective Technology* pada NIST *Cybersecurity Framework* versi 1.1, implementasi fungsi *Protect* telah berjalan cukup baik, namun masih terdapat kelemahan pada aspek dokumentasi pengendalian akses, kebijakan keamanan teknis, dan pelaksanaan pelatihan kesadaran keamanan informasi secara berkala.

C. Detect

Fungsi *Detect* digunakan untuk mengidentifikasi terjadinya insiden keamanan siber secara cepat dan tepat. Pada penelitian ini, analisis fungsi *Detect* dilakukan melalui observasi aktivitas monitoring sistem serta studi dokumentasi pencatatan gangguan dan log keamanan.

Berdasarkan hasil observasi, aktivitas monitoring sistem informasi dan jaringan telah berjalan secara aktif melalui *dashboard* monitoring Zabbix dan Wazuh. Operator terlihat melakukan pemantauan terhadap *alert* sistem, membuka detail notifikasi gangguan, serta mencatat tindak lanjut penanganan pada *logbook* operasional. Jadwal piket monitoring juga terlihat tersedia pada ruang operator sebagai bentuk pengawasan rutin terhadap sistem informasi.

Hasil studi dokumentasi menunjukkan adanya buku catatan gangguan fisik, format laporan insiden standar, serta indikasi penggunaan sistem ticketing digital dalam tindak lanjut gangguan. Selain itu, analisis akar masalah terindikasi

tersedia melalui log sistem walaupun belum ditemukan dokumen analisis yang berdiri sendiri secara khusus.

Namun demikian, hasil observasi dan studi dokumentasi menunjukkan bahwa proses monitoring keamanan belum dilakukan secara optimal dan berkelanjutan. Dokumentasi *logging* dan analisis aktivitas keamanan belum terdokumentasi secara menyeluruh. Selain itu, keterbatasan sumber daya manusia menyebabkan proses pemantauan dan analisis keamanan masih bersifat terbatas.

Berdasarkan kategori *Anomalies and Events* serta *Security Continuous Monitoring* pada NIST *Cybersecurity Framework* versi 1.1, implementasi fungsi *Detect* telah berjalan namun masih memerlukan peningkatan, khususnya pada pengembangan monitoring keamanan yang lebih terintegrasi, penguatan dokumentasi *logging*, dan peningkatan kapasitas sumber daya manusia dalam proses deteksi ancaman keamanan siber.

D. Respond

Fungsi *Respond* bertujuan untuk memastikan organisasi mampu melakukan penanganan terhadap insiden keamanan siber yang terjadi. Implementasi fungsi *Respond* pada penelitian ini dianalisis melalui observasi aktivitas operasional dan studi dokumentasi terkait penanganan insiden keamanan informasi.

Berdasarkan hasil studi dokumentasi, organisasi telah memiliki SOP penanganan insiden siber, format laporan insiden, daftar kontak person darurat Tim CSIRT, serta struktur organisasi pengelola teknologi informasi. Selain itu, pembentukan CSIRT menunjukkan adanya upaya organisasi dalam meningkatkan koordinasi dan respons terhadap gangguan keamanan informasi.

Hasil observasi menunjukkan bahwa operator melakukan tindak lanjut terhadap *alert* yang muncul pada sistem monitoring dan mencatat penanganan gangguan pada *logbook* operasional. Respons awal terhadap gangguan kecil juga terlihat dilakukan dalam waktu relatif cepat melalui koordinasi internal antar petugas.

Namun demikian, penelitian menunjukkan bahwa dokumentasi prosedur respons insiden masih belum lengkap secara rinci, khususnya terkait tahapan eskalasi insiden, evaluasi pascainsiden, dan dokumentasi pembelajaran dari insiden sebelumnya. Selain itu, dokumen analisis akar masalah juga belum ditemukan secara khusus pada hasil studi dokumentasi.

Berdasarkan kategori *Response Planning, Communications*, dan *Improvements* pada NIST *Cybersecurity Framework* versi 1.1, implementasi fungsi Respond telah berjalan namun masih memerlukan penguatan pada aspek dokumentasi prosedur respons, evaluasi pascainsiden, dan pengembangan mekanisme perbaikan berkelanjutan.

E. Recover

Fungsi *Recover* bertujuan untuk memastikan pemulihan layanan dan sistem informasi setelah terjadinya insiden keamanan siber. Analisis fungsi *Recover* dilakukan melalui observasi terhadap sarana *backup* dan studi dokumentasi prosedur pemulihan sistem.

Berdasarkan hasil observasi, terlihat adanya media backup berupa NAS dan HDD *backup* yang diberi label “Backup Daily”. Selain itu, aktivitas monitoring sistem yang berjalan aktif menunjukkan adanya kesiapan awal organisasi dalam menjaga keberlangsungan layanan digital ketika terjadi gangguan sistem.

Hasil studi dokumentasi menunjukkan bahwa organisasi telah memiliki jadwal *backup* harian, *log* hasil *backup* pada sistem, SOP *recovery* atau *restore,* serta penyimpanan *backup* pada NAS lokal dan *Disaster Recovery Center* Provinsi Jawa Timur. Hasil tes *restore* juga tersedia meskipun baru dilakukan pada beberapa layanan tertentu.

Namun demikian, bukti pengujian *restore* secara berkala belum terlihat secara menyeluruh pada seluruh layanan sistem informasi yang dikelola. Selain itu, prosedur pemulihan formal dan strategi keberlangsungan layanan digital juga belum terdokumentasi secara lengkap berdasarkan hasil observasi dan studi dokumentasi.

Berdasarkan kategori *Recovery Planning* dan *Improvements* pada NIST *Cybersecurity Framework* versi 1.1, implementasi fungsi

Recover telah berjalan namun masih memerlukan peningkatan pada aspek pengujian pemulihan berkala, dokumentasi prosedur *recovery,* dan pengembangan strategi keberlangsungan layanan digital setelah terjadinya insiden keamanan siber

IV. KESIMPULAN

Berdasarkan hasil observasi, wawancara, dan studi dokumentasi yang dianalisis menggunakan NIST *Cybersecurity Framework* (NIST CSF) Versi 1.1, dapat disimpulkan bahwa implementasi manajemen risiko keamanan sistem informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk pada dasarnya telah berjalan pada lima fungsi inti NIST CSF, *yaitu Identify, Protect, Detect, Respond,* dan *Recover.* Implementasi tersebut terlihat dari adanya inventarisasi aset teknologi informasi, penggunaan risk register, penerapan pengendalian akses, monitoring sistem dan jaringan, pencatatan gangguan, pembentukan *Computer Security Incident Response Team* (CSIRT), serta dukungan backup dan pemulihan layanan.

Pada fungsi *Identify,* organisasi telah melakukan inventarisasi aset fisik dan aplikasi serta identifikasi ancaman dan risiko keamanan informasi. Namun, dokumentasi aliran data, diagram arsitektur sistem, dan pengelolaan keamanan pihak ketiga masih belum tersedia secara lengkap. Pada fungsi *Protect,* pengamanan telah diterapkan melalui penggunaan akun pribadi, firewall, antivirus, VPN, Wazuh, backup rutin, serta pembatasan akses fisik dan logis. Akan tetapi, audit hak akses berkala, penerapan *multi-factor authentication* (MFA), dan dokumentasi pengelolaan hak akses masih perlu ditingkatkan.

Pada fungsi Detect, aktivitas monitoring keamanan telah berjalan melalui penggunaan log, alert, dashboard monitoring Zabbix dan Wazuh, serta dukungan Tim CSIRT. Namun, monitoring jaringan secara menyeluruh dan dokumentasi pola operasi normal masih belum optimal. Pada fungsi *Respond,* organisasi telah memiliki mekanisme penanganan insiden, koordinasi internal maupun eksternal, serta proses mitigasi gangguan keamanan. Meskipun demikian, dokumentasi analisis akar masalah dan analisis dampak insiden masih memerlukan penguatan. Pada fungsi *Recover,* organisasi telah memiliki dukungan pemulihan berupa SOP recovery/restore, backup harian, Business Continuity Plan, dan Disaster Recovery Center. Namun, pengujian *restore* dan simulasi pemulihan layanan belum dilakukan secara menyeluruh dan berkala.

Secara keseluruhan, penelitian ini menunjukkan bahwa implementasi manajemen risiko keamanan sistem informasi pada Dinas Komunikasi dan Informatika Kabupaten Nganjuk telah berjalan cukup baik, namun masih memerlukan peningkatan pada aspek dokumentasi keamanan, penguatan kontrol akses, monitoring keamanan berkelanjutan, evaluasi insiden, serta pengujian pemulihan sistem. Hasil penelitian ini diharapkan dapat menjadi bahan evaluasi dan rekomendasi dalam meningkatkan tata kelola keamanan informasi guna mendukung keberlangsungan layanan pemerintahan digital yang aman, efektif, dan berkelanjutan.

Penelitian selanjutnya disarankan untuk melakukan pengukuran tingkat kematangan keamanan informasi (maturity level), analisis risiko secara kuantitatif, atau pengujian teknis keamanan sistem seperti *vulnerability assessment* dan *penetration testing* agar hasil evaluasi keamanan informasi menjadi lebih mendalam, terukur, dan komprehensif.

DAFTAR PUSTAKA

[1] F. R. A. Sofyan Mufti Prasetiyo, Rehan Gustiawan, Farhat, "Analisis Pertumbuhan Pengguna Internet Di Indonesia," *BIIKMA Bul. Ilm. Ilmu Komput. dan Multimed.*, vol. 2, no. 1, pp. 65–71, 2024, [Online]. Available: https://jurnalmahasiswa.com/index.php/biikma/article/download/1032/692/2267

[2] L. Q. M. Rumakat, "Analisis Efektivitas Pelayanan Publik dalam Penerapan Sistem Administrasi Berbasis Elektronik di Pemerintah Daerah," *RIGGS J. Artif. Intell. Digit. Bus.*, vol. 4, no. 2, pp. 4282–4289, 2025, doi: 10.31004/riggs.v4i2.1193.

[3] A. MAULANA, "KEAMANAN SIBER DI ERA DIGITAL: ANCAMAN DAN SOLUSI," vol. 2, pp. 306–312, 2024.

[4] BUPATI KABUPATEN NGANJUK, *KEPUTUSAN BUPATI NGANJUK TENTANG PENETAPAN COMPUTER SECURITY INCIDENT RESPONSE TEAM KABUPATEN NGANJUK (NGANJUK-CSIRT)*. INDONESIA, 2023.

[5] Kementerian Komunikasi dan Informatika., "LAPORAN TAHUNAN KOMINFO-CSIRT 2023," 2023. [Online]. Available: https://water.selangor.gov.my/info/penerbitan/laporan-tahunan

[6] humaskabupatennganjuk, "Pemkab Nganjuk Terima Sertifikat ISO 27001:2022," Humas Kabupaten Nganjuk.

[7] M. Fadya and D. N. Utama, "Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019," *TEM J.*, vol. 14, no. 1, pp. 182–191, 2025, doi: 10.18421/TEM141-17.

[8] A. Aminudin and A. Supriyanto, "Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013 (Studi kasus: Bapenda Provinsi Jawa Tengah)," *Aiti*, vol. 21, no. 2, pp. 210–229, 2024, doi: 10.24246/aiti.v21i2.210-229.

[9] P. D. Sugiyono, *METODE PENELITIAN KUALITATIF*. 2022.

[10] N. I. of S. and Technology, "Framework for improving critical infrastructure cybersecurity," *Proc. Annu. ISA Anal. Div. Symp.*, vol. 535, pp. 9–25, 2018, [Online]. Available: file:///C:/Users/thiag/AppData/Local/Mendeley Ltd./Mendeley Desktop/Downloaded/National Institute of Standards and Technology - 2018 - Framework for improving critical infrastructure cybersecurity.pdf