

EVALUASI KOMPARATIF KEAMANAN INFORMASI PDNS 2024 BERDASARKAN ISO/IEC 27001:2022 DAN NIST CSF 2.0

Syahruramadan Kahar^{1*}, Veronika Asri Tandirerung², Risna Asri³, Siti Nurkhalisah⁴, Stevano Moreno Egor⁵, Riswan⁶

^{1,2,3,4,5,6}Universitas Negeri Makassar, Jl. A. P. Pettarani, Makassar, Sulawesi Selatan 90222, Telp. (0411) 861377

Keywords:

ISO/IEC 27001:2022; NIST CSF 2.0; Ransomware; PDNS; Keamanan Siber.

Correspondent Email:

240210501012@student.unm.ac.id

Abstrak. Serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) tahun 2024 mengungkap kelemahan kritis pada keamanan infrastruktur digital pemerintah Indonesia. Penelitian ini bertujuan menganalisis kelemahan keamanan informasi pada kasus serangan ransomware PDNS menggunakan ISO/IEC 27001:2022 dan NIST Cybersecurity Framework (CSF) 2.0 melalui pendekatan Systematic Literature Review (SLR). Sebanyak 24 artikel jurnal ilmiah, laporan keamanan siber, publikasi resmi pemerintah, dan standar keamanan informasi internasional dikaji menggunakan protokol PRISMA. Analisis difokuskan pada identifikasi kesenjangan keamanan pada aspek organisasi, teknologi, dan operasional sistem yang terdampak. Hasil penelitian menunjukkan bahwa serangan terjadi akibat lemahnya pengelolaan akses, patch management, segmentasi jaringan, pemantauan real-time, dan kesiapan respons insiden. ISO/IEC 27001:2022 efektif mengidentifikasi kelemahan tata kelola keamanan informasi, sedangkan NIST CSF 2.0 memberikan analisis operasional terkait kemampuan deteksi, respons, dan pemulihan insiden. Integrasi kedua framework menghasilkan pendekatan keamanan siber yang lebih komprehensif melalui penerapan keamanan berlapis, pemantauan berkelanjutan, dan pengelolaan respons insiden yang terstruktur. Hasil penelitian ini diharapkan dapat menjadi referensi dalam meningkatkan ketahanan siber infrastruktur digital pemerintah.



Copyright © 2026 The Author(s), Published by Jurnal Informatika dan Teknik Elektro Terapan. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Abstract. The ransomware attack on Indonesia's National Temporary Data Center (PDNS) in 2024 revealed critical weaknesses in government digital infrastructure security. This study aimed to analyze information security vulnerabilities in the PDNS ransomware incident using ISO/IEC 27001:2022 and the NIST Cybersecurity Framework (CSF) 2.0 through a Systematic Literature Review (SLR) approach. A total of 24 academic journals, cybersecurity reports, official government publications, and international security standards were reviewed using the PRISMA protocol. The analysis focused on identifying security gaps in organizational, technological, and operational aspects of the affected infrastructure. The results indicated that the attack exploited weaknesses in access management, patch management, network segmentation, real-time monitoring, and incident response readiness. ISO/IEC 27001:2022 effectively identified governance and information security management deficiencies, while NIST CSF 2.0 provided operational analysis related to detection, response, and recovery capabilities. The integration of both frameworks provides a more comprehensive cybersecurity approach through layered defense implementation, continuous monitoring, and structured incident response management. The findings are expected to contribute to improving cybersecurity resilience within government digital infrastructure environments.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai sektor, termasuk pemerintahan, pendidikan, kesehatan, dan layanan publik. Digitalisasi memberikan kemudahan dalam pengelolaan data dan layanan, namun di sisi lain meningkatkan risiko ancaman keamanan siber seperti kebocoran data, malware, dan ransomware [1]. Pada era Society 5.0, integrasi teknologi Internet of Things (IoT), Artificial Intelligence (AI), dan Big Data menjadikan data sebagai aset strategis yang memiliki nilai tinggi sehingga membutuhkan perlindungan yang memadai [3].

Pada Juni 2024, Indonesia mengalami serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) yang berdampak pada terganggunya ratusan layanan publik nasional. Serangan tersebut menggunakan varian ransomware Brain Cipher yang merupakan turunan dari LockBit 3.0. Penyerang mengenkripsi data penting dan meminta tebusan sebesar delapan juta dolar Amerika Serikat [4]. Insiden ini memperlihatkan bahwa keamanan infrastruktur digital pemerintah masih memiliki berbagai kelemahan mendasar, baik dari sisi tata kelola maupun operasional keamanan sistem.

Keamanan informasi merupakan upaya perlindungan informasi untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data atau dikenal sebagai CIA Triad [3]. Dalam implementasinya, organisasi membutuhkan standar dan kerangka kerja keamanan yang dapat membantu mengelola risiko secara sistematis. Salah satu standar internasional yang banyak digunakan adalah ISO/IEC 27001:2022 yang berfokus pada Sistem Manajemen Keamanan Informasi (SMKI) [5]. Selain itu, terdapat NIST Cybersecurity Framework (CSF) 2.0 yang menyediakan pendekatan operasional dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan sistem dari insiden keamanan siber [2].

Penelitian sebelumnya menunjukkan bahwa ISO/IEC 27001:2022 efektif dalam meningkatkan tata kelola keamanan informasi organisasi [6][7], sedangkan NIST CSF lebih menekankan pada kesiapan operasional dalam menghadapi insiden siber [8]. Selain itu, Sishuba & Edoun [9] merekomendasikan

pendekatan *defense-in-depth* sebagai strategi berlapis dalam menghadapi ancaman kompleks seperti ransomware. Ribeiro et al. [10] juga menemukan bahwa banyak layanan publik daring di berbagai negara masih memiliki postur keamanan yang lemah. Namun demikian, penelitian yang secara khusus mengintegrasikan kedua framework dalam konteks kasus ransomware PDNS 2024 masih sangat terbatas.

Kebaruan penelitian ini terletak pada sintesis sistematis yang menggabungkan audit berbasis ISO/IEC 27001:2022 dengan evaluasi operasional NIST CSF 2.0 secara terpadu pada satu kasus nyata serangan ransomware terhadap infrastruktur kritis pemerintah Indonesia. Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk: (1) menganalisis proses serangan ransomware pada PDNS 2024; (2) mengevaluasi keamanan informasi berdasarkan ISO/IEC 27001:2022 dan NIST CSF 2.0; serta (3) menyusun rekomendasi peningkatan ketahanan siber bagi infrastruktur digital pemerintah.

2. TINJAUAN PUSTAKA

2.1 Keamanan Informasi

Keamanan informasi merupakan disiplin yang berfokus pada perlindungan aset informasi dari berbagai ancaman, baik internal maupun eksternal. Konsep dasar keamanan informasi dikenal sebagai CIA Triad yang mencakup tiga aspek utama, yaitu confidentiality (kerahasiaan), integrity (integritas), dan availability (ketersediaan) [3]. Dalam konteks digital, keamanan informasi mencakup penerapan kebijakan, prosedur, dan teknologi untuk melindungi data dari akses tidak sah, modifikasi, dan gangguan layanan. Ancaman siber seperti malware, ransomware, dan phishing terus berkembang sehingga membutuhkan pendekatan keamanan yang komprehensif dan adaptif [1].

2.2 ISO/IEC 27001:2022

ISO/IEC 27001:2022 adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI) yang diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC). Standar ini memberikan kerangka sistematis untuk mengelola risiko keamanan informasi melalui

empat kategori kontrol utama, yaitu *organizational controls*, *people controls*, *physical controls*, dan *technological controls* [5]. ISO/IEC 27001:2022 merupakan pembaruan dari versi 2013 dengan penambahan kontrol keamanan baru yang relevan dengan perkembangan ancaman digital terkini, termasuk keamanan cloud, intelijen ancaman siber, dan manajemen konfigurasi [6]. Implementasi standar ini memungkinkan organisasi untuk memperoleh sertifikasi formal sebagai bukti komitmen terhadap keamanan informasi [7].

2.3 NIST Cybersecurity Framework (CSF) 2.0

NIST Cybersecurity Framework (CSF) 2.0 adalah kerangka kerja keamanan siber yang dikembangkan oleh National Institute of Standards and Technology (NIST) Amerika Serikat. CSF 2.0 merupakan pembaruan dari versi 1.1 yang memperluas cakupan dari sektor infrastruktur kritis ke semua jenis organisasi. Framework ini terdiri dari enam fungsi utama, yaitu *Govern*, *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*, yang memberikan panduan operasional komprehensif dalam mengelola risiko keamanan siber [2]. Pendekatan NIST CSF 2.0 bersifat fleksibel dan adaptif sehingga dapat disesuaikan dengan kebutuhan berbagai jenis organisasi tanpa memerlukan sertifikasi formal [8].

2.4 Ransomware dan Ancaman Siber

Ransomware adalah jenis malware yang mengenkripsi data korban dan meminta tebusan sebagai syarat pemulihan akses. Serangan ransomware modern menggunakan pendekatan multi-tahap yang mengacu pada MITRE ATT&CK Framework, meliputi *initial access*, *privilege escalation*, *lateral movement*, dan *execution* [13]. Varian Brain Cipher yang menyerang PDNS merupakan turunan dari LockBit 3.0 yang memiliki kemampuan enkripsi tingkat lanjut dan mekanisme penghindaran deteksi [14]. Analisis sentimen terhadap isu ancaman siber di media sosial menunjukkan bahwa insiden seperti PDNS memiliki dampak signifikan terhadap kepercayaan publik terhadap layanan digital pemerintah [1].

2.5 Penelitian Terkait

Beberapa penelitian telah mengkaji implementasi ISO/IEC 27001 dan NIST CSF dalam berbagai konteks. Setyoso et al. [7] menunjukkan efektivitas ISO 27001:2022 dalam desain keamanan informasi untuk transformasi digital UMKM. Apriany & Wibowo [6] menganalisis implementasi ISO 27001:2022 dan Indeks KAMI pada perusahaan konsultan. Di sisi lain, Marotta & Madnick [8] mengkategorikan regulasi keamanan siber yang berkembang dan mengidentifikasi kesenjangan kapabilitas pada tahap penanganan insiden. Sishuba & Edoun [9] merekomendasikan pendekatan *defense-in-depth* untuk sistem kontrol industri. Ribeiro et al. [10] mengevaluasi postur keamanan layanan publik daring di berbagai negara dan menemukan kelemahan yang signifikan pada aspek teknologi dan operasional.

3. METODE PENELITIAN

Penelitian ini menggunakan metode *Systematic Literature Review (SLR)* dengan pendekatan kualitatif deskriptif. Metode SLR digunakan untuk mengidentifikasi, mengevaluasi, dan mensintesis berbagai penelitian ilmiah secara sistematis dan transparan [3]. Proses penelitian mengacu pada protokol PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) untuk memastikan validitas dan reproduibilitas hasil penelitian.

Tahapan penelitian dilakukan melalui beberapa langkah sebagai berikut: (1) identifikasi topik penelitian; (2) penentuan kata kunci pencarian; (3) penelusuran literatur; (4) seleksi artikel; (5) ekstraksi data; dan (6) sintesis hasil penelitian. Kata kunci yang digunakan meliputi "information security", "ransomware", "ISO 27001:2022", "NIST CSF", "PDNS", dan "cybersecurity framework".

Literatur diperoleh dari berbagai sumber akademik dan publikasi resmi, yaitu Google Scholar, IEEE Xplore, ScienceDirect, Springer, ACM Digital Library, laporan keamanan siber resmi, serta dokumen standar internasional. Artikel dipilih berdasarkan kriteria inklusi berikut:

- 1) Membahas keamanan informasi, ransomware, atau tata kelola keamanan siber.

2) Menggunakan ISO/IEC 27001 atau NIST CSF sebagai kerangka analisis.

3) Dipublikasikan pada rentang tahun 2020–2026.

4) Berasal dari jurnal ilmiah, laporan teknis, atau dokumen resmi yang dapat diverifikasi.

Artikel yang tidak relevan, tidak memiliki sumber yang jelas, atau tidak memiliki pembahasan metodologis yang memadai dikeluarkan dari penelitian. Proses seleksi literatur menggunakan protokol PRISMA disajikan pada Tabel 1.

Tabel 1. Proses Seleksi Literatur Menggunakan Protokol PRISMA

Tahap Seleksi	Jumlah Artikel
Identifikasi awal dari seluruh database	87
Setelah duplikasi dihapus	61
Setelah seleksi judul dan abstrak	38
Setelah seleksi teks penuh (final)	24

4. HASIL DAN PEMBAHASAN

4.1 Analisis Proses Serangan Ransomware pada PDNS 2024

Serangan ransomware pada PDNS 2024 menunjukkan pola serangan siber yang terstruktur dan sistematis berdasarkan tahapan MITRE ATT&CK Framework [13]. Serangan tidak terjadi secara acak, melainkan berlangsung melalui empat tahap yang saling berkaitan dan memanfaatkan kelemahan sistem secara bertahap.

Tahap pertama adalah initial access, yaitu proses masuknya penyerang ke dalam sistem melalui eksploitasi kerentanan yang belum diperbarui serta kebocoran kredensial pengguna. Kondisi ini mengindikasikan bahwa patch management dan manajemen identitas belum diterapkan secara optimal [14]. Tahap kedua adalah privilege escalation, yaitu peningkatan hak akses penyerang hingga memperoleh kontrol administratif terhadap sistem. Keberhasilan tahap ini menunjukkan bahwa prinsip least privilege dan pemantauan aktivitas pengguna belum diterapkan secara optimal [16]. Tahap ketiga adalah lateral

movement, yaitu penyebaran malware ke berbagai server dalam jaringan yang dapat terjadi dengan cepat karena tidak adanya segmentasi jaringan yang memadai [17].

Pada tahap keempat, yaitu execution, ransomware Brain Cipher dijalankan untuk menonaktifkan sistem keamanan endpoint dan mengenkripsi data penting. Sistem monitoring yang tidak mampu mendeteksi aktivitas berbahaya secara dini menunjukkan kelemahan serius pada endpoint protection dan mekanisme pemantauan keamanan [18]. Tahap terakhir berupa permintaan tebusan sebesar delapan juta dolar AS yang ditolak oleh pemerintah Indonesia, sehingga pemulihan sistem dilakukan secara mandiri [20].

Dari keseluruhan tahapan tersebut, keberhasilan serangan merupakan hasil dari kombinasi kelemahan teknis, manajerial, dan operasional. Hal ini sejalan dengan temuan Sishuba & Edoun [9] bahwa sistem tanpa lapisan pertahanan yang memadai akan sangat rentan terhadap serangan multi-tahap seperti ransomware.

4.2 Audit Keamanan Berdasarkan ISO/IEC 27001:2022

Audit keamanan dilakukan dengan mengevaluasi penerapan kontrol keamanan berdasarkan empat kategori utama ISO/IEC 27001:2022, yaitu organizational controls, people controls, physical controls, dan technological controls [5][7]. Hasil audit disajikan pada Tabel 2.

Tabel 2. Hasil Audit Keamanan Berdasarkan ISO/IEC 27001:2022

Kategori Kontrol	Temuan Utama	Analisis
Organizational Controls	Kebijakan keamanan belum efektif	Manajemen risiko belum diterapkan secara konsisten sehingga ancaman ransomware tidak teridentifikasi sejak awal [12].

People Controls	Kesadaran keamanan rendah	Kurangnya pelatihan menyebabkan lambatnya deteksi dan respons insiden di tingkat pengguna [15].
Physical Controls	Pengamanan fisik belum optimal	Kontrol akses terhadap infrastruktur server masih lemah dan berpotensi membuka celah manipulasi [16].
Technological Controls	Proteksi sistem lemah	Endpoint protection, patch management, dan sistem backup belum berjalan optimal sehingga sistem mudah dieksploitasi [17].

Tabel 2 menunjukkan bahwa kelemahan paling dominan terdapat pada aspek organizational controls dan technological controls. Kebijakan yang tidak diterapkan secara konsisten menyebabkan sistem tidak memiliki pertahanan yang memadai. Selain itu, tidak adanya audit berkala dan security testing memperburuk kondisi karena kerentanan tidak teridentifikasi lebih awal [11]. Hal ini juga sejalan dengan temuan Apriany & Wibowo [6] bahwa organisasi yang belum mengimplementasikan SMKTI secara penuh memiliki tingkat kematangan keamanan yang rendah.

4.3 Evaluasi Menggunakan NIST Cybersecurity Framework (CSF) 2.0

Evaluasi keamanan dilakukan menggunakan lima fungsi utama NIST CSF 2.0, yaitu Identify, Protect, Detect, Respond, dan Recover [2]. Hasil evaluasi disajikan pada Tabel 3.

Tabel 3. Evaluasi Menggunakan NIST Cybersecurity Framework (CSF) 2.0

Fungsi NIST	Kondisi PDNS	Analisis
Identify	Belum optimal	Inventarisasi aset dan identifikasi risiko belum terstruktur sehingga sistem tidak siap menghadapi ancaman yang berkembang [18].
Protect	Lemah	Kontrol akses, enkripsi data, dan proteksi endpoint tidak memadai untuk mencegah penetrasi awal penyerang [19].
Detect	Terlambat	Tidak adanya monitoring real-time menyebabkan serangan berkembang tanpa terdeteksi selama beberapa jam [20].
Respond	Kurang efektif	Penanganan insiden belum memiliki prosedur dan playbook yang terstruktur sehingga koordinasi menjadi lambat [21].
Recover	Belum siap	Sistem backup dan pemulihan belum dirancang memadai sehingga proses recovery

		memakan waktu lama [22].
--	--	--------------------------

Tabel 3 menunjukkan bahwa kelemahan paling signifikan terdapat pada fungsi Detect, Respond, dan Recover. Ketidakmampuan sistem dalam mendeteksi serangan secara dini menyebabkan dampak serangan semakin luas. Koordinasi respons insiden yang tidak terstruktur memperlambat proses pemulihan layanan publik. Hal ini sejalan dengan temuan Marotta & Madnick [8] bahwa kelemahan pada regulasi operasional keamanan siber menghasilkan kesenjangan kapabilitas yang signifikan pada tahap penanganan insiden.

4.4 Integrasi ISO/IEC 27001:2022 dan NIST CSF 2.0

ISO/IEC 27001:2022 dan NIST CSF 2.0 memiliki pendekatan yang berbeda namun saling melengkapi. Perbandingan keduanya disajikan pada Tabel 4.

Tabel 4. Perbandingan ISO/IEC 27001:2022 dan NIST CSF 2.0

Aspek	ISO/IEC 27001:2022	NIST CSF 2.0	Relevansi pada PDNS
Pendekatan	Tata kelola dan manajemen risiko	Operasional dan respons insiden	PDNS lemah pada keduanya
Fokus Utama	Pengendalian keamanan informasi	Deteksi dan pemulihan serangan	Kesenjangan terjadi di aspek operasional
Implementasi	Formal dan terstruktur	Fleksibel dan adaptif	Keduanya dibutuhkan
Sertifikasi	Dapat disertifikasi	Tidak disertifikasi	Pemerintah perlu sertifikasi ISO
Peran	Pencegahan dan	Respons dan	Saling melengkapi

	pengendalian	pemulihan	
--	--------------	-----------	--

Tabel 4 memperlihatkan bahwa ISO/IEC 27001:2022 berperan dalam membangun fondasi tata kelola keamanan melalui kebijakan dan kontrol yang terstruktur, sedangkan NIST CSF 2.0 memastikan kesiapan sistem dalam menghadapi dan merespons serangan secara operasional [6][7]. Pada kasus PDNS, kelemahan terjadi pada kedua aspek tersebut secara bersamaan, sehingga penerapan satu framework saja tidak cukup untuk menghadapi ancaman siber yang kompleks. Integrasi kedua pendekatan menjadi solusi yang lebih efektif dalam meningkatkan ketahanan sistem keamanan informasi.

4.5 Rekomendasi Peningkatan Keamanan

Berdasarkan hasil sintesis 24 literatur, rekomendasi disusun dalam tiga prioritas waktu sebagaimana disajikan pada Tabel 5.

Tabel 5. Rekomendasi Peningkatan Keamanan Berdasarkan Sintesis Literatur

Prioritas	Rekomendasi	Referensi
Jangka Pendek (0–6 bulan)	Patch management menyeluruh, implementasi MFA, segmentasi jaringan, dan backup terenkripsi dengan metode 3-2-1	[14]; [9]
Jangka Menengah (6–18 bulan)	Implementasi SOC dan SIEM, penyusunan incident response playbook, pelatihan keamanan siber rutin bagi seluruh pegawai	[21]; [15]
Jangka Panjang (>18 bulan)	Sertifikasi ISO/IEC 27001:2022, audit keamanan berkala, dan penerapan Security by	[6]; [8]

	Design pada sistem baru	
--	-------------------------	--

Tabel 5 menunjukkan bahwa rekomendasi jangka pendek berfokus pada penguatan teknis dasar yang dapat segera dilaksanakan. Penerapan Multi-Factor Authentication (MFA) dan segmentasi jaringan yang ketat akan secara langsung mengurangi risiko privilege escalation dan lateral movement [9]. Untuk jangka menengah, implementasi Security Operations Center (SOC) dan Security Information and Event Management (SIEM) akan memperkuat fungsi Detect dalam NIST CSF yang saat ini menjadi kelemahan terbesar PDNS [21]. Adapun untuk jangka panjang, sertifikasi ISO/IEC 27001:2022 memberikan legitimasi formal dan kerangka audit berkelanjutan yang dibutuhkan oleh institusi pemerintah [6].

5. KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, diperoleh beberapa kesimpulan sebagai berikut:

- Serangan ransomware pada PDNS 2024 terjadi akibat kombinasi kelemahan pada pengelolaan akses, patch management, segmentasi jaringan, sistem monitoring, dan kesiapan respons insiden yang berlangsung melalui empat tahap terstruktur berdasarkan MITRE ATT&CK Framework.
- Audit menggunakan ISO/IEC 27001:2022 menunjukkan adanya kelemahan pada aspek organizational controls dan technological controls, sedangkan evaluasi menggunakan NIST CSF 2.0 memperlihatkan defisiensi kritis pada fungsi Detect, Respond, dan Recover.
- Integrasi ISO/IEC 27001:2022 dan NIST CSF 2.0 menghasilkan pendekatan keamanan siber yang lebih komprehensif karena mampu menggabungkan aspek tata kelola keamanan informasi dan kesiapan operasional sistem secara bersamaan. Penerapan kedua framework secara terpadu sangat penting dalam meningkatkan ketahanan siber infrastruktur digital pemerintah.
- Penelitian selanjutnya disarankan untuk mengembangkan model penilaian kematangan keamanan siber yang menggabungkan metrik kuantitatif dari

kedua framework, serta melakukan validasi empiris melalui studi kasus implementasi langsung pada instansi pemerintah di Indonesia.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Ibu Veronika Asri Tandirerung, S.Pd., M.Pd. selaku dosen pengampu mata kuliah Keamanan Informasi Program Studi Teknik Komputer Universitas Negeri Makassar atas arahan, bimbingan, dan masukan dalam penyusunan artikel ini.

DAFTAR PUSTAKA

- [1] R. F. Setiawan, "Analisis Sentimen Isu Ancaman Siber Menggunakan Algoritma Multi-layer Perceptron," *Jurnal Informatika dan Teknik Elektro Terapan (JITET)*, vol. 13, no. 3, pp. 1296–1302, Jul. 2025.
- [2] J. L. Salas-Riega, Y. Riega-Viru, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the NIST framework," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 16, no. 6, 2025.
- [3] Nurbojatmiko, M. S. Khatami, N. M. Asnadi, and R. Anisyah, "ISO 27001 as information security solution in Society 5.0 era: Systematic literature review," *Sinkron: Jurnal dan Penelitian Teknik Informatika*, vol. 9, no. 1, 2025.
- [4] BSSN, Laporan insiden keamanan siber PDNS 2024. Badan Siber dan Sandi Negara, 2024.
- [5] F. C. Arumdiya and C. Rudianto, "Implementasi ISO 27001:2022 dalam manajemen risiko keamanan informasi," *Jurnal PETISI*, vol. 6, no. 2, 2025.
- [6] A. Apriany and A. Wibowo, "Analysis of the implementation of ISO 27001:2022 and KAMI Index in enhancing the information security management system in consulting firms," *Indonesian Journal of Computing and Cybernetics Systems (IJCCS)*, vol. 18, no. 4, pp. 417–428, 2024.
- [7] F. A. A. Setyoso, R. Mulyana, and R. A. Nugraha, "Utilizing ISO 27001:2022 in information security design for SME digital transformation," *Ranah Research*, vol. 6, no. 6, 2024.
- [8] A. Marotta and S. Madnick, "Analyzing and categorizing emerging cybersecurity regulations," *ACM Computing Surveys*, vol. 58, no. 2, 2025.
- [9] T. Sishuba and E. I. Edoun, "Cyber security standards for applying the defense-in-depth approach for industrial control systems," *AIP Conference Proceedings*, vol. 3416, 2026.

- [10] D. Ribeiro, V. Fonte, L. F. Ramos, and J. M. Silva, "Assessing the information security posture of online public services worldwide," *Government Information Quarterly*, vol. 42, 2025.
- [11] E. Liyanto, "Analisis penerapan sistem manajemen keamanan informasi pada website official STT NF dengan SNI ISO/IEC 27001:2022," *Sekolah Tinggi Teknologi Terpadu Nurul Fikri*, 2024.
- [12] A. Muzakky, "Perancangan sistem manajemen keamanan informasi menggunakan framework ISO/IEC 27001:2022 pada sistem informasi peminjaman ruangan kampus," *STT Terpadu Nurul Fikri*, 2024.
- [13] MITRE, "ATT&CK framework: Tactics, techniques and procedures for ransomware attacks," The MITRE Corporation, 2024. [Online]. Available: <https://attack.mitre.org>
- [14] Sangfor, "Brain Cipher ransomware: Technical analysis and mitigation strategies," Sangfor Technologies Security Blog, 2024.
- [15] M. Salam, K. A. A. Bakar, A. T. A. Ghani, and A. H. M. Aman, "Cybersecurity in higher education institutions digitalisation," *SAGE Open*, pp. 1–14, 2026.
- [16] D. Primacs, "Technical forensics report: Brain Cipher ransomware attack on Indonesian PDNS," *Security Research Publication*, 2024.
- [17] Lockheed Martin, "Cyber kill chain framework: Advanced threat analysis," Lockheed Martin Corporation, 2025.
- [18] Kumparan Tech, "Begini cara Brain Cipher ransomware sandera data korban," *Kumparan*, Jun. 30, 2024. [Online]. Available: <https://kumparan.com>
- [19] CSIRT Magelang Kota, "Analisis teknis serangan ransomware Brain Cipher pada PDNS," *CSIRT Kota Magelang Technical Report*, 2024.
- [20] Antara News, "Menkominfo jelaskan kronologi serangan siber PDNS 2," *Antara News*, Jun. 26, 2024. [Online]. Available: <https://www.antaranews.com>
- [21] ASIS International, *Incident response and business continuity management standards*. ASIS International Publications, 2024.
- [22] RRI, "Update pemulihan PDNS pasca serangan ransomware," *Radio Republik Indonesia News*, 2024.