Contents lists available at MID Publisher International

Technology Sciences Insights Journal

Journal homepage: https://journal.midpublisher.com/index.php/tsij

Analisis Perbandingan Framework Keamanan Jaringan (NIST CSF, CIS Controls, ISO 27001)

Rakhmadi Rahman, Asti Ananta, Besse Surianti
Program Studi Sistem Informasi, Institut Teknologi Bacharuddin Jusuf Habibie

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima: Juni 2025
Revisi: Juni 2025
Diterima: Juli 2025
Dipublikasi: Juli 2025

Kata Kunci:
Keamanan Jaringan, NIST CSF, CIS Controls, ISO/IEC 27001, Framework.

*Penulis Korespondensi:
rakhmadi.rahman@ith.ac.id

ABSTRAK

Keamanan jaringan menjadi elemen krusial dalam mendukung keberlangsungan operasional organisasi pada era digital saat ini. Riset ini mengkaji dan membandingkan tiga framework keamanan informasi terkemuka: NIST Cybersecurity Framework (CSF), CIS Controls, dan ISO/IEC 27001, untuk menentukan pendekatan yang paling sesuai berdasarkan skala dan kebutuhan organisasi. Metode deskriptif-komparatif digunakan dalam penelitian ini dengan mengandalkan data sekunder dari standar resmi, literatur akademik, dan studi kasus. Hasil studi menunjukkan bahwa NIST CSF unggul dalam fleksibilitas dan dapat diterapkan secara modular, CIS Controls efektif secara teknis untuk organisasi dengan sumber daya terbatas, sementara ISO/IEC 27001 menawarkan sistem manajemen keamanan informasi yang komprehensif dan bersertifikasi. Penelitian ini menyarankan kombinasi penggunaan framework agar dapat membentuk strategi keamanan informasi yang berkelanjutan dan kontekstual

ABSTRACT

Network security is a crucial element in supporting the operational sustainability of organisations in today's digital age. This research examines and compares three leading information security frameworks: NIST Cybersecurity Framework (CSF), CIS Controls, and ISO/IEC 27001, to determine the most appropriate approach based on organisational scale and needs. The descriptive-comparative method was used in this research by relying on secondary data from official standards, academic literature, and case studies. The study results show that NIST CSF excels in flexibility and can be implemented in a modular manner, CIS Controls is technically effective for organisations with limited resources, while ISO/IEC 27001 offers a comprehensive and certified information security management system. This research suggests a combination of frameworks to form a sustainable and contextualised information security strategy

PENDAHULUAN

Seiring meningkatnya transformasi digital di berbagai sektor, risiko keamanan siber juga meningkat. Laporan dari Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa Indonesia mengalami serangan siber dalam jumlah masif tiap tahun. Dalam konteks tersebut, organisasi membutuhkan sistem perlindungan informasi yang tidak hanya reaktif tetapi proaktif, terstruktur, dan berkelanjutan. Framework keamanan informasi berfungsi sebagai panduan terstruktur dalam membangun, mengelola, dan mengevaluasi sistem keamanan informasi yang sesuai dengan tujuan dan kapasitas organisasi. Di tengah beragam pilihan yang tersedia, seperti NIST CSF, CIS Controls, dan ISO/IEC 27001, organisasi perlu melakukan penyesuaian berdasarkan risiko, sumber daya, serta kebutuhan sertifikasi atau kepatuhan regulasi yang berlaku. Tiga framework keamanan yang paling banyak diadopsi secara global NIST CSF, CIS Controls, dan

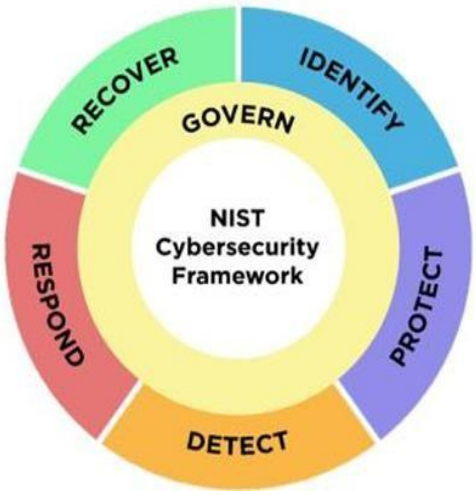
ISO/IEC 27001 masing-masing menyuguhkan pendekatan yang berbeda terhadap keamanan jaringan. Namun, tidak semua organisasi mengetahui bagaimana memilih framework yang paling sesuai berdasarkan konteks dan kapasitasnya. Oleh sebab itu, riset ini disusun untuk memberikan gambaran menyeluruh sekaligus analisis perbandingan ketiga framework tersebut.

LANDASAN TEORI

Keamanan Jaringan

Keamanan jaringan merupakan langkah strategis yang bertujuan menjaga kerahasiaan, integritas, dan ketersediaan data yang ditransmisikan dalam jaringan komputer. Di era digital, jaringan tidak hanya menjadi sarana komunikasi internal, tetapi juga penghubung utama ke layanan cloud, aplikasi, dan perangkat pengguna. Oleh karena itu, ancaman terhadap jaringan seperti malware, DDoS, sniffing, dan zero-day attack terus berkembang dan membutuhkan pendekatan perlindungan yang adaptif. Pendekatan modern meliputi arsitektur Zero Trust (ZTA), segmentasi jaringan, serta penggunaan kecerdasan buatan (AI) untuk deteksi dan respons ancaman secara real-time. Selain teknologi, aspek nonteknis seperti budaya keamanan, kepatuhan terhadap kebijakan, dan pelatihan pengguna juga sangat penting. Kesadaran pengguna dan kebijakan yang jelas dapat meminimalkan kesalahan manusia yang sering menjadi celah serangan. Dengan demikian, keamanan jaringan tidak hanya bersifat teknis, tetapi juga mencerminkan tata kelola organisasi dalam menghadapi risiko digital secara menyeluruh dan berkelanjutan.

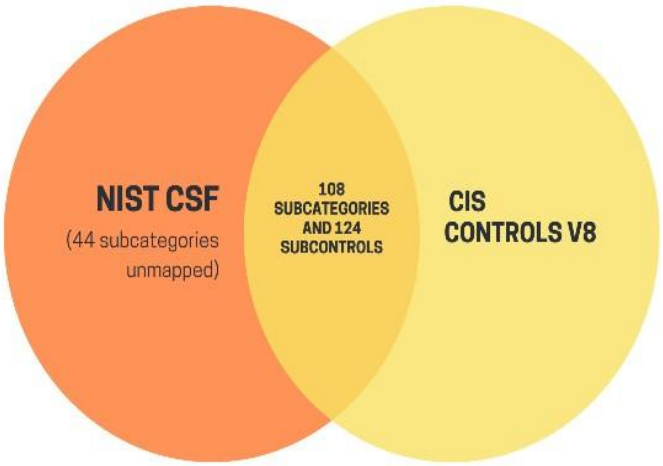
NIST Cybersecurity Framework (CSF)



Gambar 1 NIST Cybersecurity Framework (CSF)

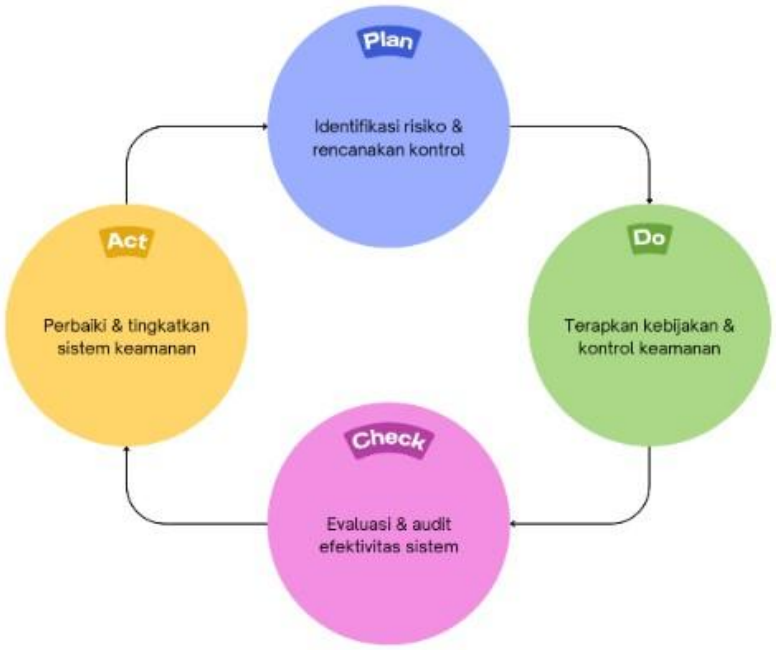
NIST CSF dikembangkan oleh National Institute of Standards and Technology dan terdiri dari enam fungsi utama: Govern, Identify, Protect, Detect, Respond, dan Recover. Pendekatan berbasis risiko ini memungkinkan organisasi memulai implementasi dari aspek paling mendesak. Framework ini bersifat fleksibel dan dapat diadaptasi oleh organisasi dari berbagai sektor dan skala. Selain menyediakan struktur fungsional, NIST CSF juga menyediakan Implementation Tiers untuk mengukur tingkat kematangan keamanan dan Profile untuk memetakan kondisi aktual dan target keamanan siber organisasi.

CIS Controls



Gambar 2 CIS Controls

Framework ini berfokus pada kontrol teknis dan operasional. CIS Controls v8 menyusun 18 kontrol berdasarkan tingkat kematangan organisasi, yakni IG1 hingga IG3. CIS Controls dikembangkan berdasarkan analisis empiris dari ribuan insiden keamanan nyata. Oleh karena itu, framework ini menawarkan panduan praktis untuk pengamanan teknis yang dapat segera diterapkan. Implementasi bertahap melalui Implementation Groups (IGs) memudahkan organisasi dalam menyesuaikan kontrol dengan sumber daya dan risikonya. 2.4 ISO/IEC 27001



Gambar 3 Siklus PDCA ISO/IEC 27001

Informasi berbasis siklus Plan-Do-Check-Act (PDCA). Standar ini mencakup 93 kontrol keamanan dalam Annex A. ISO/IEC 27001 sangat cocok untuk organisasi besar dan teregulasi yang membutuhkan sistem manajemen keamanan informasi yang formal, terdokumentasi, dan terukur. Proses sertifikasinya meningkatkan kredibilitas organisasi di mata mitra, regulator, dan pelanggan.

METODE

Jenis Penelitian

Jenis penelitian ini adalah deskriptif-komparatif dengan pendekatan kualitatif. Tujuan utamanya adalah untuk memahami karakteristik dan keefektifan masing-masing framework berdasarkan parameter implementasi di lapangan.

Teknik Pengumpulan Data

Data diperoleh dari dokumen standar resmi, jurnal ilmiah, white papers, dan studi kasus implementasi. Studi literatur dilakukan secara sistematis untuk menilai efektivitas dan relevansi framework dalam konteks organisasi dengan skala berbeda.

Teknik Analisis

Analisis dilakukan dengan membandingkan ketiga framework berdasarkan struktur, pendekatan implementasi, kompleksitas, serta kesesuaian terhadap tipe organisasi. Data kemudian dipetakan ke dalam bentuk tabel dan narasi untuk memudahkan interpretasi dan rekomendasi.

HASIL DAN PEMBAHASAN

Perbandingan Umum Framework

Tabel 1 Perbandingan Umum NIST CSF, CIS Controls, dan ISO/IEC 27001

Aspek	NIST CSF	CIS Controls v8	ISO/IEC 27001:2022
Pendekatan	Berbasis fungsi manajemen risiko	Berbasis kontrol teknis	Berbasis manajemen keamanan informasi (ISMS)
Struktur	6 fungsi inti: Govern, Identify, Protect, dll.	18 kontrol dibagi dalam 3 implementation groups	10 klausul + 93 kontrol dalam Annex A
Tujuan Utama	Meningkatkan ketahanan dan manajemen risiko siber	Mitigasi ancaman nyata berbasis teknis	Membangun sistem keamanan informasi formal & terukur
Fleksibilitas	Sangat fleksibel, dapat dikustomisasi	Fleksibel dan mudah diterapkan	Moderat; bersifat formal dan mengikat
Dokumentasi & Struktur	Ringan, tidak mengharuskan dokumentasi formal	Dokumentasi minimal	Dokumentasi sangat tinggi
Sertifikasi Resmi	Tidak tersedia	Tidak tersedia	Tersedia (audit dan sertifikasi ISO)
Skalabilitas Organisasi	Menengah – besar, sektor kritis	Kecil – menengah, fleksibel	Besar dan kompleks
Kompatibilitas Framework	Mudah diintegrasikan dengan ISO & CIS	Dapat melengkapi NIST atau ISO	Menjadi fondasi ISMS; dapat dikombinasi dengan NIST
Biaya Implementasi	Rendah hingga sedang	Sangat rendah	Tinggi (termasuk pelatihan dan sertifikasi)
Ketersediaan Publik	Gratis dan open source	Gratis, open source	Berbayar (standar dan pelatihan resmi)

Tabel ini membandingkan aspek fundamental dari setiap framework, mulai dari struktur, fleksibilitas, biaya implementasi, hingga ketersediaan sertifikasi. Dapat disimpulkan bahwa NIST CSF unggul dalam fleksibilitas, CIS Controls dalam kemudahan teknis, dan ISO/IEC 27001 dalam aspek formalitas dan pengakuan internasional.

Rekomendasi Berdasarkan Jenis Organisasi

Tabel 2 Rekomendasi Framework Berdasarkan Organisasi

Skala Organisasi	**Framework Rekomendasi**	**Alasan**
Kecil (Startup/UMKM)	CIS Controls	Ringan, mudah diterapkan, fokus pada keamanan teknis
Menengah	NIST CSF + CIS Controls	Kombinasi strategis dan teknis, fleksibel dan modular
Besar/Multinasional	ISO/IEC 27001	Perlukan pengelolaan risiko formal dan audit eksternal

Tabel ini menyajikan rekomendasi framework yang paling sesuai untuk organisasi kecil, menengah, dan besar. CIS Controls sangat direkomendasikan untuk organisasi kecil dan menengah karena ringan dan praktis, sedangkan ISO/IEC 27001 lebih cocok untuk organisasi besar dan multinasional.

Pemetaan Fungsi Framework

Tabel 3 Tabel Pemetaan Fungsi Antar Framework

Fungsi NIST CSF	**CIS Controls v8 (Contoh)**	**ISO/IEC 27001:2022 (Contoh Domain)**
Identify (ID)	Control 1: Inventory & Asset Management	A.5: Organizational Controls, A.6: People Controls
Protect (PR)	Control 4: Secure Config, Control 6: Access	A.7: Physical Security, A.8: Technological Controls
Detect (DE)	Control 8: Audit Log Management	A.12: Operations Security, A.13: Communication
Respond (RS)	Control 17: Incident Response	A.16: Incident Management
Recover (RC)	Control 11: Data Recovery	A.17: Information Security Continuity
Govern (GV)	Control 2 & 14: Awareness & Training	A.5.2: Policy and Responsibilities

Pemetaan ini menunjukkan bagaimana fungsi atau domain utama dari setiap framework dapat saling melengkapi. Kombinasi NIST CSF sebagai kerangka strategis dengan CIS Controls untuk kontrol teknis dan ISO/IEC 27001 untuk manajemen formal dapat menciptakan sistem keamanan yang holistik.

Diagram Alur Integrasi Strategis

Gambar 4 Alur Strategi Implementasi Framework Gabungan

Diagram ini menunjukkan bagaimana ketiga framework dapat diintegrasikan secara strategis untuk mencapai sistem keamanan informasi yang adaptif dan berkelanjutan.

Checklist Implementasi Framework

Tabel 4 Checklist Implementasi Kontrol Keamanan Informasi

No.	Kontrol/Praktik	Framework	Status	Bukti/Dokumen	Tindak Lanjut
1	Inventarisasi AseT	CIS Control ✓1 / ISO A.5.9	Sudah	Excel + Tag QR	Perbarui setiap 3 bulan
2	Penggunaan MFA	CIS Control X 6.3 / ISO A.8.3	-	Implementasi dengan Google Authenticator	Belum
3	Pelatihan Keamanan untuk Karyawan Baru	CIS Control ~ 14 / NIST GV	LMS Dalam Proses	Log + Modul Pelatihan	Uji pemahaman tiap pelatihan
4	Backup Otomatis	Data CIS Control ✓11 / ISO A.17	Sudah	Log backup dari AWS	Simulasi restore tiap 6 bulan

5	Kebijakan puncak Tertulis	ISO A.5.1 / X	Buat dan sahkan oleh Keamanan	NIST GV	Belum manajemen

Checklist ini menjadi panduan implementasi langkah demi langkah dari masing-masing framework, memungkinkan organisasi untuk melakukan evaluasi diri dan perencanaan strategis.

KESIMPULAN

Penelitian ini menyimpulkan bahwa setiap framework memiliki kekuatan dan keterbatasan masing-masing. NIST CSF sangat fleksibel dan cocok untuk tahap awal, CIS Controls memberikan solusi teknis langsung, sedangkan ISO/IEC 27001 ideal untuk organisasi besar dan teregulasi.

Daftar Pustaka

[1] National Institute of Standards and Technology. (2024). Framework for Improving Critical Infrastructure Cybersecurity Version 2.0. NIST, U.S. Department of Commerce.

[2] Center for Internet Security. (2021). CIS Controls v8: Critical Security Controls for Effective Cyber Defense. Center for Internet Security, Inc.

[3] ISO/IEC. (2022). ISO/IEC 27001:2022 – Information Security Management Systems – Requirements. International Organization for Standardization.

[4] Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of Cybersecurity Maturity Assessment Framework Using NIST CSF v1.1 and CIS Controls v8. Jurnal Inovtek Polbeng – Seri Informatika, 9(1), 125–140.

[5] Alghamdi, F. (2023). Comparative Study of ISO/IEC 27001 and NIST CSF in Large Organizations. International Journal of Information Security and Privacy, 17(2), 1–12.

[6] Aminudin, A., Afiansyah, H. G., & Nugroho, H. A. (2024). Implementing ISO 27001 and NIST CSF for Cyber Risk Evaluation in Public Sector. Journal of Cybersecurity and Governance, 12(4), 67–78.

[7] International Journal of Innovative Science and Research Technology (IJISRT). (2024).