

Published online on the page: https://journal.upp.ac.id/index.php/rjti/index

**R J T I**
Riau Jurnal Teknik Informatika
| E - ISSN (*Online*) 2829-2529 |

# Manajemen Risiko Serangan Siber Menggunakan Framework *NIST Cybersecurity Framework* 2.0 pada Layanan *Website* di Kampus XYZ

Kevin Fryfo Winstone Rimper[1,*], Sherwin Reinaldo U. A. Sompie[2], Daniel Febrian Sengkey[3]

[1,2,3] Dept. of Electrical Engineering, Sam Ratulangi University Manado, Kampus Bahu St., 95115, Indonesia

**Informasi Artikel**

*Sejarah Artikel:*
*Submit:* 07 September 2026
Revisi: 03 November 2026
Diterima: 05 November 2026
Diterbitkan: 08 November 2026

**Kata Kunci**

Manajemen Risiko Keamanan Siber, NIST Cybersecurity Framework 2.0, Vulnerability Assessment, CVSS v3.1.

**Korespondensi**

E-mail:
kevinrimper026@student.unsrat.ac.id

**A B S T R A C T**

*The digitalization of academic services in Indonesian higher education has widened cybersecurity exposure, as reflected in the rising national network traffic anomalies reported by Indonesia's National Cyber and Crypto Agency (BSSN). A large public university, anonymized here as Campus XYZ, has experienced several real incidents, from academic-portal data exposure and website defacement to a Distributed Denial of Service (DDoS) attack that disrupted its server infrastructure for nearly a week. This study develops a cybersecurity risk management profile for the university's website services using the NIST Cybersecurity Framework (CSF) 2.0, combined with authorized technical testing through OWASP ZAP and Nikto and vulnerability scoring based on CVSS v3.1. The research follows the seven-step NIST CSF 2.0 implementation process, from Prioritize and Scope to Implementation Action Plan, with data collected through purposive interviews with six UPT TIK informants, field observation, document review, and an unauthenticated vulnerability assessment of the institution's public domains conducted with institutional permission. The study produces a Current Profile at an average of Tier 1.17 (Partial), a Target Profile of Tier 2.33, a risk-prioritized gap analysis (average gap of 1.17 Tier, largest on the Govern function), and a three-phase roadmap (0-24 months) of 22 action items. The roadmap is formulated as a target to help raise the institution's cybersecurity posture; its actual implementation and post-implementation evaluation are beyond the scope of this study. To protect the institution, specific domain names and vulnerability identifiers are anonymized.*

***Abstrak***

Digitalisasi layanan akademik di perguruan tinggi Indonesia memperluas celah keamanan siber, sebagaimana tercermin dari meningkatnya anomali trafik jaringan nasional yang dilaporkan Badan Siber dan Sandi Negara (BSSN). Sebuah universitas negeri besar, yang dianonimkan sebagai Kampus XYZ, telah mengalami sejumlah insiden nyata, mulai dari keterbukaan data portal akademik, defacement website, hingga serangan Distributed Denial of Service (DDoS) yang mengganggu infrastruktur servernya selama hampir sepekan. Penelitian ini menyusun profil manajemen risiko keamanan siber layanan website universitas tersebut menggunakan NIST Cybersecurity Framework (CSF) 2.0, dipadukan dengan pengujian teknis terotorisasi melalui OWASP ZAP dan Nikto serta penilaian kerentanan berbasis CVSS v3.1. Penelitian mengikuti tujuh langkah implementasi NIST CSF 2.0, dari Prioritize and Scope hingga Implementation Action Plan, dengan data dihimpun melalui wawancara purposif enam narasumber UPT TIK, observasi lapangan, studi dokumentasi, dan vulnerability assessment unauthenticated terhadap domain publik institusi yang dilaksanakan atas izin institusi. Penelitian menghasilkan Current

Creative Commons Attribution-ShareAlike 4.0 International License. *Some rights reserved*

Profile pada rata-rata Tier 1,17 (Partial), Target Profile Tier 2,33, gap analysis terprioritas berbasis risiko (rata-rata gap 1,17 Tier, terbesar pada fungsi Govern), serta roadmap tiga fase (0-24 bulan) berisi 22 action item. Roadmap dirumuskan sebagai target untuk membantu meningkatkan postur keamanan siber institusi; implementasi dan evaluasi pascapenerapannya berada di luar cakupan penelitian ini. Demi melindungi institusi, nama domain dan identitas kerentanan spesifik dianonimkan.

This is an open access article under the CC–BY-SA license

## 1. Pendahuluan

Transformasi digital yang berlangsung di lingkungan perguruan tinggi Indonesia dalam satu dekade terakhir telah mengubah secara mendasar cara institusi pendidikan menjalankan operasionalnya. Layanan yang dahulu bersifat manual dan tatap muka kini beralih menjadi layanan berbasis web yang dapat diakses kapan saja dan dari mana saja, mulai dari pendaftaran mahasiswa baru, proses perkuliahan, hingga administrasi kepegawaian. Perubahan ini tidak dapat dilepaskan dari dua sisi yang saling berkaitan. Di satu sisi, transformasi ini mempercepat dan mempermudah jalannya layanan akademik. Di sisi lain, transformasi ini memperluas permukaan serangan (*attack surface*) yang harus dihadapi institusi. Semakin banyak sistem yang terhubung ke jaringan publik, semakin besar pula peluang munculnya titik lemah yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

Data yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) memperkuat gambaran ini. Sepanjang tahun 2023, tercatat ratusan juta anomali trafik jaringan yang mengarah pada aktivitas serangan siber seperti malware, trojan, dan ransomware, dan tren tersebut tetap berlanjut hingga pertengahan tahun 2024 dengan jumlah anomali yang juga besar. Angka-angka ini menunjukkan bahwa ancaman siber bukan lagi persoalan yang bersifat insidental atau jarang terjadi, melainkan sebuah kondisi yang berlangsung terus-menerus dan memerlukan perhatian serius dari setiap institusi yang mengelola sistem informasi, termasuk perguruan tinggi.

Lingkungan kampus memiliki karakteristik yang khas dibandingkan organisasi pada umumnya, dan karakteristik inilah yang justru membuatnya rentan terhadap serangan. Sebuah kajian sistematis yang mensintesis aset kritis, ancaman rutin, serta model ancaman generik di lingkungan pendidikan tinggi menegaskan bahwa kebutuhan akan manajemen risiko keamanan informasi di sektor ini akan terus meningkat seiring bertambahnya kompleksitas sistem yang dikelola, dan bahwa insiden kebocoran data sangat mungkin terulang apabila institusi tidak memiliki tata kelola risiko yang memadai [1]. Universitas pada umumnya mengelola jaringan yang sangat terbuka dan harus dapat diakses secara bersamaan oleh ribuan pengguna dengan peran dan hak akses yang berbeda-beda, mulai dari mahasiswa, dosen, staf administrasi, hingga pihak eksternal seperti mitra dan alumni. Kondisi infrastruktur yang cenderung terdesentralisasi, dikembangkan secara bertahap oleh unit-unit yang berbeda, dan tidak jarang menggunakan teknologi yang beragam, secara otomatis memperluas area yang berpotensi disalahgunakan.

Gambaran serupa juga ditemukan pada konteks pendidikan tinggi di kawasan lain. Kajian terhadap institusi pendidikan tinggi di Balkan Barat mendapati bahwa peningkatan insiden kebocoran data akademik erat kaitannya dengan struktur *e-learning* yang terdesentralisasi serta keragaman pengguna yang tinggi, ditambah dengan masih minimnya keberadaan rencana respons insiden yang formal di banyak institusi [2], [3]. Temuan-temuan lintas negara ini memperlihatkan bahwa persoalan yang dihadapi Kampus XYZ bukanlah kasus yang berdiri sendiri, melainkan bagian dari pola yang lebih luas di sektor pendidikan tinggi secara global, sebuah pola yang membuka ruang

bagi penelitian berbasis studi kasus lokal untuk memberikan kontribusi yang relevan secara lebih luas.

Kampus XYZ, sebagai salah satu perguruan tinggi terbesar di kawasan Indonesia Timur dengan lebih dari 24.000 mahasiswa, sangat bergantung pada sistem informasi berbasis web dalam menjalankan operasionalnya sehari-hari. Sejumlah layanan kritis berjalan secara daring, mulai dari portal akademik, *website* masing-masing fakultas, sistem keuangan, hingga platform pembelajaran. Besarnya volume data sensitif yang tersimpan di dalam sistem-sistem tersebut membuat Kampus XYZ menjadi sasaran yang cukup menarik bagi pelaku kejahatan siber, baik yang bermotif finansial, iseng, maupun kepentingan lain.

Ancaman yang dihadapi Kampus XYZ bukan sekadar kemungkinan teoritis, melainkan sesuatu yang telah benar-benar terjadi dan berulang. Pada tahun 2023, misalnya, terjadi insiden pencurian data tabel username di Portal Akademik (Portal Inspire). Di samping itu, beberapa *website* di lingkungan kampus juga kerap mengalami *defacement* berupa sisipan iklan judi online, yang terjadi karena adanya celah keamanan pada sistem manajemen konten yang jarang diperbarui secara berkala. Puncaknya terjadi pada Mei 2025, ketika Kampus XYZ mengalami serangan *Distributed Denial of Service* (DDoS) yang berasal dari luar negeri. Secara teknis, dampak serangan DDoS memang dikenal dapat bersifat fatal terhadap ketersediaan layanan, karena serangan jenis ini bekerja dengan cara menghabiskan sumber daya jaringan target melalui banjir permintaan palsu yang dikirim secara terdistribusi, dan apabila tidak terdeteksi sejak dini dapat menimbulkan gangguan operasional yang berkepanjangan [4]. Hal ini sejalan dengan apa yang dialami Kampus XYZ, di mana seluruh layanan server kampus lumpuh total dan tidak dapat diakses selama hampir sepekan penuh, dengan proses pemulihan yang panjang hingga harus melibatkan konsultasi dengan pihak eksternal.

Di luar aspek teknis, terdapat pula persoalan lain yang tidak kalah penting, yaitu keterbukaan institusi pendidikan dalam mengungkap detail insiden yang mereka alami. Sebuah studi terhadap perguruan tinggi di Inggris menemukan bahwa keterbatasan pengungkapan detail serangan menjadi persoalan utama, karena informasi yang lengkap sering kali ditahan oleh institusi dengan alasan keamanan, sehingga menyulitkan pihak lain, termasuk peneliti dan sesama institusi, untuk melakukan penilaian kerentanan secara menyeluruh dan belajar dari kejadian tersebut [5]. Pola tertutup semacam ini turut dirasakan pada konteks Kampus XYZ, di mana dokumentasi insiden yang tersedia untuk keperluan evaluasi dan penelitian masih sangat terbatas, sehingga menyulitkan proses pembelajaran organisasi dari insiden-insiden yang pernah terjadi sebelumnya.

Selain tekanan dari sisi ancaman teknis, terdapat pula tuntutan dari sisi kepatuhan regulasi yang tidak dapat diabaikan. Sejak disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), setiap instansi di Indonesia memiliki kewajiban hukum yang mengikat untuk menjaga keamanan data yang mereka kelola. Data ribuan mahasiswa dan pegawai yang tersimpan dalam sistem Kampus XYZ jelas termasuk dalam kategori data pribadi yang dilindungi oleh undang-undang tersebut. Apabila institusi gagal menjamin keamanan data ini, dampaknya tidak hanya terbatas pada reputasi kelembagaan, tetapi juga berpotensi menimbulkan sanksi administratif maupun konsekuensi hukum lainnya. Dengan mempertimbangkan seluruh kondisi tersebut, baik dari sisi ancaman teknis, riwayat insiden, maupun kewajiban regulasi, penguatan postur keamanan siber di Kampus XYZ pada saat ini bukan lagi sekadar pilihan, melainkan sebuah kebutuhan yang mendesak.

Untuk mengelola kerumitan tata kelola keamanan siber di lingkungan kampus, dibutuhkan sebuah standar atau kerangka kerja yang terstruktur namun tetap realistis untuk diterapkan sesuai dengan kapasitas institusi. Kerangka kerja standar seperti ISO/IEC 27001 pada dasarnya sangat baik dan siap sertifikasi (*certification-ready*), namun penerapannya kerap terhambat oleh kebutuhan investasi finansial yang besar, tenaga ahli khusus, serta proses dokumentasi yang cukup

memberatkan bagi institusi publik dengan sumber daya terbatas. Di sisi lain, penerapan COBIT 2019 sangat menitikberatkan pada integrasi tata kelola teknologi informasi (*governance-aligned*), yang mensyaratkan adanya struktur kepemimpinan yang matang serta koordinasi lintas departemen yang kuat, sesuatu yang belum tentu tersedia secara ideal di seluruh institusi pendidikan tinggi negeri. Bertolak dari kondisi tersebut, penelitian ini menjadikan NIST Cybersecurity Framework (NIST CSF) 2.0 sebagai kerangka kerja utama. NIST CSF dinilai lebih modular, lebih fleksibel, dan menggunakan pendekatan berbasis risiko, sehingga lebih mudah disesuaikan dengan kapasitas sumber daya maupun tingkat kematangan suatu institusi. Nilai tambah lainnya, pembaruan pada versi 2.0 menghadirkan fungsi "Govern" yang secara eksplisit mengintegrasikan keamanan siber dengan manajemen risiko tingkat institusi dan kepatuhan regulasi, termasuk kepatuhan terhadap UU PDP. Karakteristik yang adaptif inilah yang menjadikan NIST CSF 2.0 ideal untuk dipadukan dengan pengujian teknis, demi menghasilkan penilaian yang berlapis dan lebih komprehensif. Perbandingan karakteristik ISO/IEC 27001, COBIT 2019, dan NIST CSF untuk konteks negara berkembang dibahas dalam beberapa studi terdahulu [6], [7].

Meskipun studi mengenai implementasi NIST CSF telah cukup banyak dilakukan di berbagai belahan dunia, masih terdapat sejumlah kesenjangan penelitian (research gap) yang dapat diisi melalui penelitian ini. Pertama, penelitian yang secara spesifik menggunakan standar terbaru NIST CSF 2.0 untuk mengevaluasi infrastruktur *website* pendidikan tinggi di Indonesia masih sangat minim ditemukan, meskipun kajian mengenai infrastruktur dan kinerja layanan *website* pada sektor publik di Indonesia telah mulai berkembang, termasuk pada jurnal ini [8]. Kedua, sebagian besar penelitian terdahulu lebih banyak berfokus pada penilaian kualitatif melalui wawancara atau kuesioner semata, tanpa membuktikan celah keamanan secara langsung menggunakan pengujian teknis berbasis *scanning tools* maupun sistem penilaian kerentanan standar seperti CVSS, sehingga *Current Profile* yang dihasilkan cenderung kurang didukung oleh bukti teknis yang kuat. Ketiga, integrasi yang komprehensif antara evaluasi manajemen organisasi melalui NIST CSF dan uji teknis keamanan aplikasi web melalui OWASP dan CVSS, dalam satu paket penelitian yang utuh, masih jarang ditemukan, terutama untuk konteks wilayah Indonesia Timur. Pemetaan posisi penelitian ini terhadap studi-studi terdahulu dirangkum pada Tabel 1 [9], [10], [11]. Berbagai penerapan NIST CSF di Indonesia maupun lintas negara juga menegaskan relevansinya untuk penilaian kematangan dan manajemen risiko keamanan siber [12], [13], [14], [15], [16], [17], [18].

Kesenjangan-kesenjangan inilah yang menjadi pijakan dilaksanakannya penelitian ini di Kampus XYZ. Melalui penggabungan NIST Cybersecurity Framework 2.0 dari sisi tata kelola organisasi dengan evaluasi teknis melalui OWASP ZAP, Nikto, serta CVSS v3.1, penelitian ini diharapkan dapat memberikan gambaran postur keamanan siber yang lebih riil dan berbasis bukti, sekaligus merumuskan strategi mitigasi yang solid untuk melindungi aset digital Kampus XYZ. Lebih jauh lagi, pendekatan manajemen risiko yang dikembangkan dalam penelitian ini diharapkan tidak hanya memberikan manfaat langsung bagi Kampus XYZ, tetapi juga dapat dijadikan referensi implementasi bagi kampus-kampus lain di Indonesia yang menghadapi tantangan serupa dalam pengelolaan keamanan siber layanan *website* mereka

**Tabel 1. Perbandingan Penelitian Terdahulu dan Posisi Penelitian**

| Penulis (Tahun) | Objek | Metode / Tools | Kelebihan | Kekurangan |
|---|---|---|---|---|
| Delgado dkk. (2021) [9] | Organisasi pemerintah | NIST CSF; kuesioner + uji statistik | Fokus manajerial dan kebijakan | Hanya survei kepatuhan; tanpa uji kerentanan teknis |
| Nugroho dkk. (2024) [10] | Website tunggal | NIST CSF; Nikto, Nmap, nslookup | Implementasi teknis kuat | Ruang lingkup sempit; tanpa tata kelola makro |
| Mahendra & Soewito | Infrastruktur kementerian | NIST + CIS Controls; | Menggabung dua kerangka | NIST versi lama; fungsi tata kelola belum |

| | | | | |
|---|---|---|---|---|
| (2023) [11] | | CVSS | | eksplisit |
| Penelitian ini | Layanan *website* perguruan tinggi | NIST CSF 2.0 + OWASP ZAP/Nikto + CVSS v3.1 | Integrasi tata kelola (termasuk Govern) dengan uji teknis dalam satu penelitian | Hanya rekomendasi (tanpa eksekusi); scan *unauthenticated*; batas pada lapisan web/server |

*Sumber: Hasil olahan penulis (2026)*

## 2. Metode Penelitian

### 2.1. Tahapan Penelitian

Penelitian ini merupakan studi kasus terapan yang dilaksanakan di Unit Pengelola Teknologi Informasi Kampus (UPT TIK) Kampus XYZ, dengan waktu pelaksanaan selama enam bulan. Penelitian ini mengadopsi pendekatan metode campuran (*mixed-methods*), yang menggabungkan analisis kualitatif terhadap tata kelola organisasional dengan pengujian kuantitatif berbasis kerentanan teknis pada aplikasi web.

Data primer dikumpulkan melalui tiga teknik utama: (1) Wawancara mendalam (*in-depth interview*) semi-terstruktur dengan enam pemangku kepentingan kunci di UPT TIK, termasuk Kepala Unit, Penanggung Jawab Sistem, Penanggung Jawab Jaringan, Pengembang Aplikasi, Pengelola Web, dan Bagian Keuangan; (2) Observasi langsung terhadap arsitektur infrastruktur jaringan; dan (3) Pemindaian kerentanan teknis (Vulnerability Assessment).

Keenam narasumber dipilih secara purposif berdasarkan relevansi tugas pokoknya dengan keenam fungsi inti NIST CSF 2.0, sehingga setiap fungsi memiliki sumber data yang kompeten. Wawancara dilakukan semi-terstruktur, direkam atas persetujuan narasumber, lalu ditranskripsikan untuk dianalisis. Penentuan tingkat kematangan tiap fungsi tidak ditetapkan dari satu sumber, melainkan melalui triangulasi antara hasil wawancara, observasi lapangan, studi dokumentasi, dan temuan *vulnerability assessment*. Penilaian kematangan menggunakan rubrik *Implementation Tier* NIST CSF 2.0 pada skala Tier 1 (Partial) hingga Tier 4 (Adaptive), yang diterapkan konsisten pada setiap fungsi [19]. Seluruh kegiatan *vulnerability assessment* dilaksanakan atas izin dan koordinasi resmi dengan UPT TIK; pemindaian bersifat *unauthenticated*, dibatasi pada domain publik institusi, dan *Web Application Firewall* dinonaktifkan sementara atas persetujuan institusi agar kondisi lapisan aplikasi dan server terpindai akurat. Sesuai prinsip *responsible disclosure*, identitas institusi, nama domain, dan identitas kerentanan spesifik dianonimkan dalam artikel ini.

Penilaian tingkat kematangan setiap fungsi dilakukan oleh peneliti dengan mengacu pada rubrik *Implementation Tier* NIST CSF 2.0 dan ditetapkan melalui triangulasi lintas sumber, yaitu wawancara enam narasumber purposif, observasi lapangan, studi dokumentasi, dan temuan *vulnerability assessment*, kemudian dikonfirmasi bersama Kepala UPT TIK sebagai bentuk *member checking* untuk mengurangi subjektivitas. Perlu ditegaskan bahwa Tier NIST bersifat ordinal; nilai rata-rata Tier yang dilaporkan dalam penelitian ini digunakan semata-mata sebagai indikator agregat untuk mengomunikasikan postur keseluruhan secara ringkas, bukan sebagai pengukuran berskala interval. Oleh karena itu, dasar analisis utama tetap berupa Tier per fungsi sebagaimana disajikan pada Tabel 3, dan analisis kesenjangan dihitung per fungsi, bukan dari nilai rata-rata. Penelitian ini belum menerapkan uji reliabilitas antar-penilai formal, misalnya dengan melibatkan dua penilai atau menghitung koefisien Cohen's Kappa. Penggunaan rubrik yang terstandardisasi, triangulasi sumber data, serta konfirmasi dengan pemangku kepentingan utama menjadi strategi untuk menjaga konsistensi penilaian, sementara pelibatan beberapa penilai independen direkomendasikan sebagai agenda penelitian lanjutan.

**2.2. Alur prosedur penelitian**

Alur prosedur penelitian mengikuti tujuh langkah baku implementasi NIST CSF 2.0:

1. Prioritize and Scope:

Mengidentifikasi pendorong bisnis utama dan membatasi ruang lingkup pengujian pada layanan *website* publik.

2. Orient:

Menginventarisasi aset digital melalui fase *reconnaissance* menggunakan pendekatan multi-alat (pemetaan subdomain, DNS brute-force, dan inspeksi Certificate Transparency logs).

3. Create *Current Profile*:

Menyusun postur keamanan saat ini ke dalam enam fungsi NIST CSF 2.0 (Govern, Identify, Protect, Detect, Respond, Recover) dengan skala penilaian kematangan (Tier 1: Partial, Tier 2: Risk Informed, Tier 3: Repeatable, Tier 4: Adaptive).

4. Conduct Risk Assessment:

Melaksanakan pengujian keamanan teknis *unauthenticated* menggunakan tools pemindai konfigurasi server dan *Dynamic Application Security Testing* (DAST), yaitu Nikto v2.6.0 dan OWASP ZAP yang dijalankan pada lingkungan sistem operasi Kali Linux. Temuan celah keamanan diverifikasi untuk mengeliminasi *false positive*, kemudian dihitung tingkat keparahannya menggunakan kalkulator *Common Vulnerability Scoring System* (CVSS) v3.1 untuk membentuk *Risk Register*.

5. Create *Target Profile*:

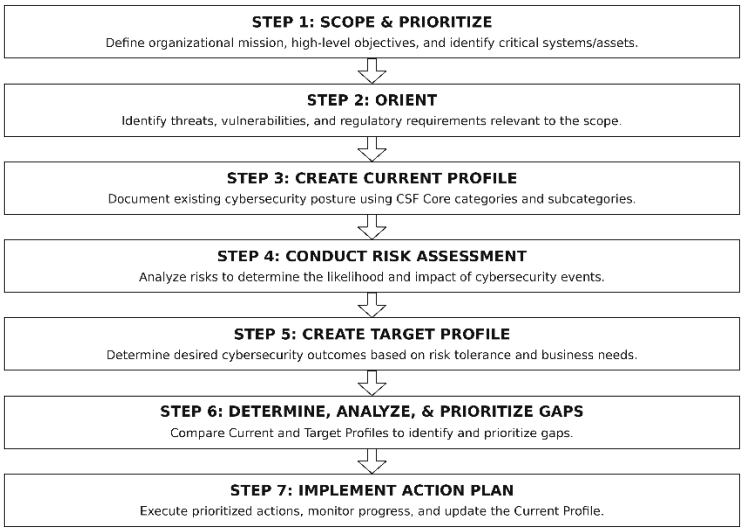
Menetapkan target tingkat kematangan organisasional yang realistis untuk dicapai dalam 1-2 tahun ke depan berdasarkan kapasitas sumber daya dan toleransi risiko institusi.

6. Determine, Analyze, and Prioritize Gaps:

Mengalkulasi selisih tingkat kematangan (Tier) antara kondisi saat ini dan kondisi target pada setiap fungsi untuk menentukan akar permasalahan.

7. Implement Action Plan:

Merumuskan rancangan tindakan strategis (*roadmap*) yang diprioritaskan berdasarkan urgensi risiko operasional.[10]




**Gambar. *1*. Langkah Implementasi NIST CSF 2.0**

## 3. Hasil dan Pembahasan

### 3.1. Identifikasi Ruang Lingkup dan Prioritas Sistem

Proses *reconnaissance* awal menghasilkan temuan yang mengejutkan terkait luasnya permukaan serangan nyata (*attack surface*) institusi. Berdasarkan wawancara, pihak pengelola mengasumsikan hanya terdapat sekitar 80 layanan *website* aktif. Namun, hasil inventarisasi teknis berhasil memetakan lebih dari 150 subdomain aktif yang memiliki DNS A record, di mana sebagian besar terkonsentrasi pada dua blok IP publik utama yang menciptakan risiko kegagalan tunggal (*single point of failure*). Kesenjangan pengetahuan aset ini menunjukkan belum berjalannya kontrol *Asset Management* (ID.AM) dengan baik. Melalui proses penyaringan, ditetapkan 13 sistem domain publik utama sebagai target pengujian *vulnerability assessment* (Lihat Tabel 2). Kriteria penetapan prioritas ini dinilai berdasarkan besaran volume data sensitif (seperti data pribadi dan data transaksi finansial mahasiswa) serta potensi dampak kelumpuhan operasional.

**Tabel 2. Prioritas Sistem Layanan Website Kampus XYZ**

| No | Domain Target | Komponen Utama | Prioritas |
|---|---|---|---|
| 1 | domain_pembayaran.xyz.ac.id | Apache / OpenSSL | Kritis |
| 2 | domain_keuangan.xyz.ac.id | Apache HTTP Server | Kritis |
| 3 | domain_admisi.xyz.ac.id | CodeIgniter | Kritis |
| 4 | panel_infrastruktur.xyz.ac.id | VMware vCenter | Tinggi |
| 5 | domain_pelaporan2.xyz.ac.id | Apache HTTP Server | Tinggi |
| 6 | domain_anggaran.xyz.ac.id | CodeIgniter | Tinggi |
| 7 | domain_tracerstudy.xyz.ac.id | Apache | Tinggi |
| 8 | domain_website_utama.xyz.ac.id | WordPress | Sedang |
| 9 | domain_dashboard.xyz.ac.id | Apache | Sedang |
| 10 | domain_rto.xyz.ac.id | Apache | Sedang |
| 11 | domain_pelaporan.xyz.ac.id | Nginx | Sedang |
| 12 | domain_fakultas_A.xyz.ac.id | WordPress | Sedang |
| 13 | domain_pascasarjana.xyz.ac.id | Joomla | Sedang |

### 3.2. Analisis Postur Keamanan Saat Ini (Current Profile)

Berdasarkan sintesis data kualitatif (wawancara operasional) dan data kuantitatif (pemindaian keamanan), postur keamanan siber Kampus XYZ secara keseluruhan teridentifikasi berada pada rata-rata agregat Tier 1,17 (Partial). Penilaian ini mengindikasikan bahwa manajemen risiko keamanan institusi masih bersifat amat kasuistik, tidak terencana secara strategis, dan sepenuhnya bersifat reaktif. Berikut adalah pemaparan rinci profil pada keenam fungsi NIST CSF 2.0:

1. Fungsi Govern (GV) - Tier 1:

Pada pilar tata kelola, institusi saat ini belum memiliki dokumen Kebijakan Keamanan Siber formal yang disahkan sebagai pedoman utama. Selain itu, belum terdapat struktur atau unit kerja yang secara spesifik didedikasikan untuk mengelola keamanan informasi; tanggung jawab tersebut saat ini masih dirangkap oleh Admin Jaringan di samping tugas rutin pemeliharaan infrastruktur operasional. Evaluasi terhadap postur keamanan juga cenderung dilakukan sebagai bentuk penanganan pasca-insiden (seperti pengadaan kapabilitas Cloud Armor setelah serangan DDoS 2025), dan belum menggunakan pendekatan *risk register* yang proaktif.

2. Fungsi Identify (ID) - Tier 1:

Pengelolaan aset digital dan inventaris perangkat lunak belum terdokumentasi secara terpusat, sehingga menyulitkan organisasi dalam memetakan keseluruhan luas permukaan serangan (*attack surface*). Pelaksanaan identifikasi kerentanan (risk assessment) juga masih mengacu pada dokumen laporan pengujian terdahulu yang belum diperbarui secara periodik, sehingga gambaran risiko belum sepenuhnya merepresentasikan kondisi terkini.

3. Fungsi Protect (PR) - Tier 1:

Terdapat ruang untuk peningkatan yang cukup signifikan pada aspek proteksi. Lapisan perimeter jaringan sudah memiliki pelindungan yang memadai dengan diterapkannya segmentasi VLAN dan *Web Application Firewall* (WAF) berbasis cloud. Namun, pengamanan pada lapisan aplikasi (Platform Security) masih perlu diperkuat. Hasil pengujian menunjukkan bahwa ke-13 target uji belum mengimplementasikan konfigurasi HTTP Security Headers (seperti HSTS, CSP, X-Frame-Options) secara optimal, dan masih ditemukan pengoperasian komponen *End-of-Life* (EOL) pada lingkungan produksi.

4. Fungsi Detect (DE) - Tier 1:

Proses pemantauan indikator anomali (*Continuous Monitoring*) saat ini masih terfokus pada jam operasional kerja dan sangat bergantung pada pelaporan dari pengguna layanan. Di sisi infrastruktur, pencatatan log pada perangkat *firewall* utama sedang dinonaktifkan sementara untuk mengoptimalkan efisiensi ruang penyimpanan (storage). Kondisi ini menyebabkan keterbatasan ketersediaan data historis yang sangat dibutuhkan untuk visibilitas dan analisis forensik secara menyeluruh ketika terjadi anomali.

5. Fungsi Respond (RS) - Tier 1:

Dalam menghadapi krisis keamanan berskala tinggi seperti serangan DDoS, tim teknis belum memiliki panduan *Incident Response Plan* (IRP) baku yang dapat dijadikan rujukan. Alur koordinasi penanganan darurat saat ini masih memanfaatkan jalur komunikasi non-formal, yang pada praktiknya membuat waktu pemulihan membutuhkan waktu hingga satu pekan. Langkah analisis akar masalah pasca-insiden juga masih perlu dirumuskan guna mencegah vektor serangan serupa di kemudian hari.

6. Fungsi Recover (RC) - Tier 2 (Risk Informed):

Fungsi ini menunjukkan tingkat kematangan yang paling baik. Tim teknis telah secara konsisten menjalankan prosedur pencadangan otomatis (automated daily *backup*) lintas klaster server menuju media penyimpanan cloud. Sistem *backup* ini telah terbukti efektif dalam memulihkan situs saat terjadi insiden *defacement*. Untuk mencapai level selanjutnya, parameter waktu pemulihan seperti Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) perlu segera diformalkan ke dalam dokumen institusional.

**Tabel 3. Rekapitulasi *Current Profile* NIST CSF 2.0**

| Fungsi | Kategori | Tier | Ringkasan Kondisi |
|---|---|---|---|
| Govern (GV) | GV.OC, GV.RM, GV.RR, GV.PO, GV.OV, GV.SC | 1 - Partial | Tidak ada kebijakan keamanan formal, tidak ada unit keamanan tersendiri, tidak ada *risk register* aktif, tidak ada manajemen komponen pihak ketiga |
| Identify (ID) | ID.AM, ID.RA, ID.IM | 1 - Partial | Tidak ada inventaris aset tertulis, tidak ada risk assessment sistematis, tidak ada proses improvement terstruktur |
| Protect (PR) | PR.AA, PR.AT, PR.DS, PR.PS, PR.IR | 1 – Partial | 13/13 *website* tanpa *security headers*, cookie tidak aman, Apache EOL aktif, tidak ada enkripsi data di database, tidak ada training keamanan rutin |
| Detect (DE) | DE.CM, DE.AE | 1 - Partial | Monitoring hanya jam kerja, log *firewall* tidak aktif, tidak ada analisis log rutin, notifikasi Telegram jarang dipantau |
| Respond (RS) | RS.MA, RS.AN, RS.CO, RS.MI | 1 – Partial | Tidak ada IRP atau SOP insiden, respons sepenuhnya reaktif, tidak ada analisis pasca insiden, mitigasi hanya bersifat sementara |
| Recover (RC) | RC.RP, RC.CO | 2 - Risk Informed | Backup otomatis harian di cloud sudah berjalan konsisten, pernah dilakukan uji pemulihan, namun tidak ada RTO/RPO formal dan komunikasi pemulihan masih informal |

### 3.3. Penilaian Risiko Teknis (Conduct Risk Assessment)

Pengujian kerentanan aplikasi web dilakukan melalui tahapan *spidering* untuk memetakan seluruh topologi URL yang terekspos publik, dilanjutkan dengan pemindaian *Dynamic Application*

*Security Testing* dan inspeksi konfigurasi web server. Proses deduplikasi data berhasil memvalidasi 31 tipe kerentanan otentik yang bebas dari *false positive*. Penilaian skor *Common Vulnerability Scoring System* (CVSS) v3.1 menyoroti dua celah kategori Kritis (Ekstrem) dan beberapa kategori Tinggi (High) yang berpotensi menyebabkan kelumpuhan triad CIA (Confidentiality, Integrity, Availability). Tabel 4 merangkum *risk register* pada penemuan paling berdampak. Penilaian keparahan kerentanan mengacu pada standar *Common Vulnerability Scoring System* (CVSS) v3.1 [20].

**Tabel 4. Rangkuman Daftar Kerentanan**

| No | Identifikasi Risiko | CVSS Score | Fungsi Terkait |
|---|---|---|---|
| 1 | Penggunaan Web Server & Modul Kriptografi Usang (*End-of-Life*) pada layanan transaksi (domain_pembayaran) | 9.8 (Kritis) | Protect (PR.PS) |
| 2 | Kerentanan Prototype Pollution (CVE-XXXX-01) pada pustaka JavaScript (Chart.js) di domain_dashboard | 9.8 (Kritis) | Protect (PR.PS) |
| 3 | Kerentanan Eksekusi Kode Berbahaya (CVE-XXXX-02) pada komponen pembaca dokumen PDF | 8.8 (Tinggi) | Protect (PR.PS) |
| 4 | Miskonfigurasi Lintas Domain (CORS Misconfiguration) | 7.1 (Tinggi) | Protect (PR.PS) |
| 5 | Ketiadaan Proteksi Anti-CSRF Token pada seluruh formulir transmisi data | 7.1 (Tinggi) | Protect (PR.AA) |
| 6 | Antarmuka Panel Manajemen Infrastruktur (Virtualisasi, CI/CD, SIEM) terekspos ke internet publik | N/A | Protect (PR.IR) |

Kombinasi kerentanan ini sangat berbahaya. Sebagai contoh, beroperasinya perangkat lunak web server legacy tanpa tambalan keamanan pada domain_pembayaran membuka peluang eksploitasi *Remote Code Execution* (RCE) langsung ke dalam database finansial, tanpa interaksi pengguna sama sekali. Di samping itu, terbukanya portal panel instrumen keamanan (SIEM) ke internet publik berisiko membocorkan tata letak dan aturan deteksi internal kampus kepada pihak peretas [21]. Perlu ditekankan bahwa tingkat prioritas pada Tabel 2 mencerminkan prioritas ruang lingkup yang ditetapkan sebelum pemindaian berdasarkan sensitivitas data dan potensi dampak operasional, sehingga merupakan dimensi yang berbeda dari tingkat keparahan teknis (skor CVSS) yang baru ditemukan pada saat pengujian. Oleh karena itu, sebuah domain dengan prioritas ruang lingkup Sedang, seperti domain_dashboard, tetap dapat memuat kerentanan berkategori Kritis pada lapisan teknisnya.

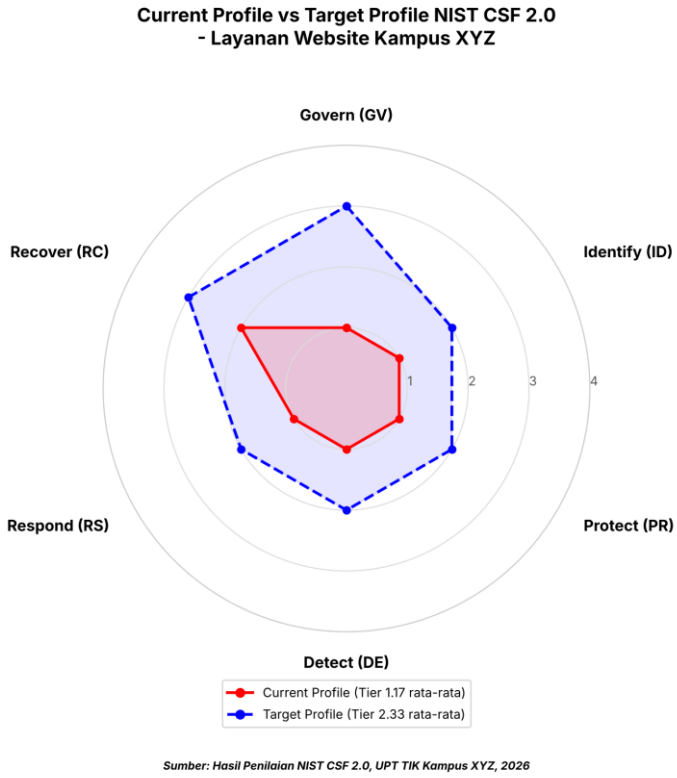
Dominannya Tier 1 pada hampir seluruh fungsi, dengan fungsi Govern sebagai akar kelemahan, sejalan dengan temuan bahwa risiko keamanan di perguruan tinggi berakar pada lemahnya tata kelola dan terbatasnya sumber daya, bukan semata persoalan teknis [1], [22]. Kajian terdahulu juga menegaskan bahwa kerangka manajemen risiko sering belum disesuaikan dengan struktur sosio-teknis kampus [22], sehingga pendekatan berbasis kematangan seperti NIST CSF 2.0 relevan untuk memetakan prioritas perbaikan secara bertahap [19], [23]. Implikasinya, penguatan postur keamanan institusi perlu dimulai dari pembenahan tata kelola (kebijakan, kepemilikan aset, dan kompetensi SDM) sebelum intervensi teknis dapat berkelanjutan. Apabila diposisikan sebagai tolok ukur sektoral, dominasi Tier 1 (Partial) ini selaras dengan temuan berbagai kajian sistematis yang menempatkan mayoritas perguruan tinggi pada tingkat kematangan keamanan siber yang rendah, khususnya pada aspek tata kelola, sehingga kondisi Kampus XYZ bukan merupakan anomali melainkan cerminan pola umum di sektor pendidikan tinggi.

### 3.4. Penentuan Target Profile dan Analisis Kesenjangan (Gap Analysis)

Target kematangan (*Target Profile*) ditetapkan pada rentang agregat Tier 2,33, yang dirancang realistis mengingat keterbatasan tenaga ahli keamanan siber tersertifikasi di unit tersebut.

Nilai kesenjangan (gap) diperoleh dengan mengurangkan Current Tier dari Target Tier. Pada Gambar 2, Fungsi Govern menjadi akar kelemahan yang membutuhkan penanganan terberat dengan

Gap 2 (menargetkan Tier 3 - Repeatable). Institusi harus melompati dua tingkat kematangan dengan segera menetapkan kebijakan resmi, otoritas tugas, dan prosedur. Sementara kelima fungsi lainnya (Identify, Protect, Detect, Respond, Recover) masing-masing memiliki Gap 1.




**Gambar 2. Spider Chart Analisis Kesenjangan (Gap) Profil Kematangan NIST CSF 2.0**

### 3.5. Rencana Aksi Implementasi (Implementation Action Plan)

Berdasarkan hasil Determine, Analyze, and Prioritize Gaps pada Langkah sebelumnya, dirumuskan *Implementation Action Plan* berupa *roadmap* intervensi yang difokuskan khusus pada penutupan risiko kategori Ekstrem dan Tinggi, sementara risiko kategori Sedang dan Rendah dijadwalkan dalam siklus *vulnerability assessment* berkelanjutan pada Fase 3. Sebanyak 22 *action item* dipetakan secara sekuensial ke dalam tiga fase implementasi berdasarkan urgensi risiko operasional dan ketergantungan antar tindakan (dependency), yaitu Fase 1: Tindakan Darurat dan Fondasi Awal (0–6 bulan), Fase 2: Formalisasi dan Konsistensi (6–12 bulan), serta Fase 3: Institusionalisasi dan Pematangan (12–24 bulan).

Penempatan suatu *action item* pada fase tertentu tidak semata bergantung pada tingkat prioritas risikonya, melainkan juga pada kesiapan fondasi yang menjadi prasyaratnya. Sebagai contoh, *action item* pengintegrasian solusi keamanan lanjutan yang berprioritas Tinggi baru ditempatkan pada Fase 3 karena membutuhkan kebijakan konfigurasi formal dari Fase 2 serta tenaga ahli tersertifikasi yang baru tersedia pada awal Fase 3. Fase 1 memprioritaskan penanganan segera komponen *End-of-Life* (EOL) pada layanan bertransaksi finansial dan pembatasan akses publik terhadap panel infrastruktur kritis, sekaligus meletakkan fondasi non-teknis berupa inventarisasi aset dan struktur koordinasi keamanan siber. Fase 2 berfokus pada formalisasi tata kelola melalui Kebijakan Keamanan Siber dan *Incident Response Plan* (IRP), didukung aktivasi kembali logging *firewall* dan penyusunan risk assessment sistematis. Fase 3 diarahkan pada pematangan kapabilitas jangka panjang melalui peningkatan kompetensi SDM, *vulnerability assessment* berkala, mekanisme pengawasan tingkat pimpinan, dan simulasi insiden. Tabel 5 merangkum keseluruhan *action item* pada *roadmap* implementasi tersebut

**Tabel 5. Rekapitulasi *Implementation Action Plan***

| No | Fase | Action Item | Fungsi NIST | Prioritas |
|---|---|---|---|---|
| 1 | Fase 1 | Pembaruan Apache HTTP Server & OpenSSL EOL pada domain_pembayaran | Protect (PR) | Kritis |
| 2 | Fase 1 | Pembaruan nginx usang pada domain_pelaporan | Protect (PR) | Tinggi |
| 3 | Fase 1 | Pembaruan pustaka pdf.js pada domain_website_utama | Protect (PR) | Tinggi |
| 4 | Fase 1 | Pembaruan Vue.js & perbaikan CORS pada domain_pelaporan | Protect (PR) | Tinggi |
| 5 | Fase 1 | Implementasi Anti-CSRF Token pada 8 host terdampak | Protect (PR) | Tinggi |
| 6 | Fase 1 | Penyusunan inventaris aset *website* tertulis | Identify (ID) | Tinggi |
| 7 | Fase 1 | Pembatasan akses publik panel infrastruktur kritis | Protect (PR) | Tinggi |
| 8 | Fase 1 | Pembentukan struktur koordinasi keamanan siber | Govern (GV) | Tinggi |
| 9 | Fase 2 | Penyusunan Kebijakan Keamanan Siber formal | Govern (GV) | Kritis |
| 10 | Fase 2 | Penyusunan *Incident Response Plan* (IRP) | Respond (RS) | Kritis |
| 11 | Fase 2 | Formalisasi RTO/RPO & prosedur komunikasi pemulihan | Recover (RC) | Tinggi |
| 12 | Fase 2 | Penerapan jadwal *patch management* terdokumentasi | Protect (PR) | Tinggi |
| 13 | Fase 2 | Reaktivasi logging *firewall* & perluasan retensi log | Detect (DE) | Tinggi |
| 14 | Fase 2 | Prosedur review log keamanan berkala | Detect (DE) | Tinggi |
| 15 | Fase 2 | Risk assessment sistematis berbasis inventaris aset | Identify (ID) | Tinggi |
| 16 | Fase 2 | Uji coba pemulihan (*recovery drill*) | Recover (RC) | Sedang |
| 17 | Fase 3 | Sertifikasi & pelatihan keamanan siber lanjutan SDM | Govern (GV) | Tinggi |
| 18 | Fase 3 | Vulnerability assessment berkala (tahunan) | Identify (ID) | Tinggi |
| 19 | Fase 3 | Mekanisme pengawasan (*oversight*) tingkat pimpinan | Govern (GV) | Tinggi |
| 20 | Fase 3 | Integrasi solusi keamanan lanjutan ke arsitektur jaringan | Protect (PR) | Tinggi |
| 21 | Fase 3 | Peninjauan menyeluruh dokumen kebijakan, IRP, RTO/RPO | Govern (GV) | Sedang |
| 22 | Fase 3 | Simulasi insiden (*tabletop exercise*) | Respond (RS) | Sedang |

## 4. Kesimpulan

Postur manajemen risiko keamanan siber pada layanan *website* Kampus XYZ saat ini dinilai belum optimal, dengan rata-rata profil kematangan berada pada Tier 1,17 (Partial) terhadap *Target Profile* Tier 2,33. Melalui pemindaian teknis objektif terhadap 13 sistem prioritas, ditemukan 31 risiko valid yang mengancam integritas sistem informasi institusi, termasuk dua celah keamanan berkategori Kritis (CVSS 9,8) yaitu penggunaan komponen web server dan modul kriptografi yang telah melewati masa dukungan vendor (*End-of-Life*) pada domain_pembayaran, serta kerentanan *prototype pollution* pada pustaka JavaScript (Chart.js) di domain_dashboard. Analisis kesenjangan menunjukkan bahwa Fungsi Govern memiliki jarak terjauh dari kondisi target ideal (*Gap* 2), menegaskan bahwa kerentanan teknis yang tersebar merata pada dasarnya berakar dari belum

terlembagakannya struktur kebijakan keamanan siber, pemetaan kepemilikan aset digital yang valid, serta keterbatasan kompetensi khusus sumber daya manusia di bidang pertahanan siber.

Sebagai luaran utama, penelitian ini merumuskan *Implementation Action Plan* berupa *roadmap* 22 *action item* yang terbagi ke dalam tiga fase implementasi, yaitu Fase 1: Tindakan Darurat dan Fondasi Awal (0–6 bulan), Fase 2: Formalisasi dan Konsistensi (6–12 bulan), dan Fase 3: Institusionalisasi dan Pematangan (12–24 bulan). Apabila dilaksanakan secara konsisten, *roadmap* ini diproyeksikan mampu mengangkat postur kematangan keamanan siber institusi dari kondisi Partial menuju Repeatable (Tier 3) dalam kurun waktu dua tahun.

Sebagai langkah perbaikan struktural, direkomendasikan kepada pihak UPT TIK Kampus XYZ untuk segera mengadopsi dokumen rencana aksi tiga fase yang telah dirumuskan secara inkremental dalam penelitian ini. Prioritas penanganan mutlak diarahkan pada pembaruan komponen server EOL dan pembatasan akses publik terhadap panel manajemen infrastruktur kritis pada enam bulan pertama operasional. Tahapan tersebut kemudian harus diikuti secara simultan dengan formalisasi dokumen Kebijakan Keamanan Siber dan *Incident Response Plan* (IRP) agar manajemen penanganan insiden tidak lagi bersifat reaktif-paliatif, sekaligus diperkuat melalui peningkatan kompetensi SDM dan pelaksanaan *vulnerability assessment* berkala pada Fase 3. Penelitian ini terbatas pada tahap evaluasi dan penyusunan rekomendasi; *roadmap* yang dihasilkan merupakan target yang belum diimplementasikan dan belum dievaluasi efektivitasnya pascapenerapan, sehingga pengujian dampak nyata rekomendasi menjadi agenda penelitian lanjutan. Keterbatasan lain mencakup cakupan uji yang hanya bersifat *unauthenticated* pada lapisan web/server dan tidak meliputi jaringan internal institusi. Terkait generalisasi, Kampus XYZ dipilih sebagai kasus karena merupakan salah satu perguruan tinggi negeri terbesar di kawasan Indonesia Timur dengan karakteristik infrastruktur dan keterbatasan sumber daya yang lazim dijumpai pada institusi sejenis, sehingga profil dan *roadmap* yang dihasilkan bersifat dapat dialihkan (transferable) secara analitis bagi institusi dengan konteks serupa. Meskipun demikian, generalisasi statistik lintas institusi memerlukan studi multi-kasus, dan kontribusi penelitian ini difokuskan pada luaran berupa artefak diagnostik, yaitu profil kematangan dan rencana aksi terprioritas, bukan pada pembuktian efektivitas pascapenerapan.

## Daftar Pustaka

[1] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," Future Internet, vol. 13, no. 2, p. 39, 2021, doi: 10.3390/fi13020039.

[2] O. Afolalu and M. S. Tsoeu, "Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions," Future Internet, vol. 17, no. 12, p. 575, 2025, doi: 10.3390/fi17120575.

[3] M. Salam, N. A. A. Bakar, N. Maarop, and G. N. Samy, "Cybersecurity in Higher Education Institutions Digitalisation: Addressing Threats and Vulnerabilities," SAGE Open, vol. 16, no. 1, 2026.

[4] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," Journal of Sensor and Actuator Networks, vol. 12, no. 4, p. 51, 2023, doi: 10.3390/jsan12040051.

[5] H. S. Lallie, A. Thompson, E. Titis, and P. J. Stephens, "Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector," Computers, vol. 14, no. 2, p. 49, 2025, doi: 10.3390/computers14020049.

[6] T. M. Rambau, W. Munyoka, L. J. Phahlamohlaka, and A. Kadyamatimba, "Evaluating cyber resilience frameworks for e-government: applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in developing country contexts," Information and Computer Security, pp. 1-22, 2026, doi: 10.1108/ICS-09-2025-0376.

[7] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," JOIV: International Journal on Informatics Visualization, vol. 4, no. 4, pp. 225-230, 2020, doi: 10.30630/joiv.4.4.482.

[8] D. Hadinata and A. Zulfan, "Analisis Komparatif HTTP/1.1 vs HTTP/2 dan Klasifikasi Prioritas Migrasi pada Website Pemerintah Kepulauan Riau Menggunakan Ensemble Machine Learning," Riau Jurnal Teknik Informatika, vol. 4, no. 3, pp. 475-482, 2025, doi: 10.30606/rjti.v4i3.4061.

[9] M. Frayssinet Delgado, D. Esenarro, F. F. Juarez Regalado, and M. Diaz Reategui, "Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations," 3C TIC, vol. 10, no. 2, pp. 123-141, 2021, doi: 10.17993/3ctic.2021.102.123-141.

[10] F. R. Nugroho, F. N. Afiana, and A. P. Kuncoro, "NIST Cyber Security Framework Development for Website Information Collection," Jurnal Teknologi Sistem Informasi dan Aplikasi, vol. 7, no. 3, pp. 1335-1342, 2024, doi: 10.32493/jtsi.v7i3.41541.

[11] V. Mahendra and B. Soewito, "Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber," Jurnal Teknik Informatika dan Sistem Informasi, vol. 22, no. 3, 2023.

[12] M. M. Chaikin, "Problems and Prospects of Implementing Assessment of the Level of Maturity of Cyber Security Processes of Critical Infrastructure Objects of the Energy Sector of Ukraine in Accordance with the NIST Cybersecurity Framework," Elektronnoe Modelirovanie, vol. 45, no. 5, pp. 81-88, 2023, doi: 10.15407/emodel.45.05.081.

[13] S. Balafif, "Penyesuaian Model Ketahanan Siber UMKM di Indonesia Dengan NIST Cybersecurity Framework," Jurnal Sistem Informasi dan Teknologi, vol. 8, no. 3, 2023.

[14] H. Ghozie Afiansyah, N. Annisa, and K. Febriyani, "Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022," Jurnal Teknik Informatika, 2023.

[15] M. O. Hoshmand and S. Ratnawati, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," AICOMS, vol. 2, no. 2, 2023.

[16] E. H. Ramadhani, I. K. A. Enriko, and E. L. I. P. Sari, "Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional," Jurnal Indonesia: Manajemen Informatika dan Komunikasi (JIMIK), vol. 6, no. 1, 2025.

[17] K. Bwiino, D. Ssemaluulu, and J. Businge, "A Systematic Literature Review of Information Security Practices in Higher Education Contexts," IET Information Security, 2026.

[18] B. Barruga, "Systematic Review of Cybersecurity Frameworks for Higher Education Institutions: Characteristics, Components, and Challenges," International Journal of Applied Mathematics, vol. 38, no. 3, 2025.

[19] L. Bernardo, A. Grilo, and P. Carreira, "An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF," Electronics, vol. 14, no. 7, p. 1364, 2025, doi: 10.3390/electronics14071364.

[20] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System," IEEE Security & Privacy, vol. 4, no. 6, pp. 85-89, 2006, doi: 10.1109/MSP.2006.145.

[21] M. Akbar, R. Munadi, and S. H. Supangkat, "Faculty Academic Web Security Assessment via Grey-Box VAPT and CVSS v3.1," Journal of Embedded Systems, Security and Intelligent Systems, 2026.

[22] B. Owino, G. Wanyembi, and C. Makori, "Systematic Literature Review of Cybersecurity Risk Assessment and Management Frameworks in Higher Education Institutions," The University Journal, vol. 7, no. 1, 2025.

[23] I. Bongiovanni, "The least secure places in the universe? A systematic literature review on information security management in higher education," Computers & Security, vol. 86, pp. 350-357, 2019, doi: 10.1016/j.cose.2019.07.003.