Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

Evaluasi Postur Keamanan Siber Sistem RME: Pendekatan Tingkatan (Tiers) NIST CSF 2.0 pada RS Radjak Salemba

Hasan Shofiyyur Rahman[1], Fadilla Putra Karnasyah[2], Regina Juliyanti Manalu[3], Zaskia Maharani[4], I Gede Susrama[5], Intan Hesti Indriana[6], Kraugusteeliana Kraugusteeliana[7*]
[1,2,3,4,6,7]Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta
[5]Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur
Email: kraugusteeliana@upnvj.ac.id
[1,2,3,4,6,7]Jl. Rs. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta
[5]Jl. Rungkut Madya, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur

Keywords:

NIST CSF 2.0, Implementation Tiers, Electronic Medical Record, Cybersecurity Governance, Risk Management.

Abstract

The implementation of the Electronic Medical Record (EMR) system at Radjak Salemba Hospital enhances efficiency but introduces patient data security risks. This study evaluates the RME cybersecurity posture using the latest NIST Cybersecurity Framework (CSF) 2.0 through the Implementation Tiers approach. Utilizing a qualitative case study method, data was collected based on six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Results indicate the organization's overall posture is at Tier 1 (Partial), reflecting reactive risk management. Although technical functions (Protect, Recover) reached Tier 2 (Risk-Informed) due to encryption and backups, fundamental weaknesses in governance (Govern) and detection (Detect) create significant disparities. The study recommends formulating a formal Risk Register and Incident Response Playbook to transform the security posture towards Tier 3 (Repeatable) within 12 months, ensuring standardized and adaptive patient data protection.

Kata Kunci:

NIST CSF 2.0, Tingkatan Implementasi, Rekam Medis Elektronik, Tata Kelola Keamanan Siber, Manajemen Risiko.

Abstrak

Penerapan Sistem Rekam Medis Elektronik (RME) di RS Radjak Salemba meningkatkan efisiensi namun memunculkan risiko keamanan data pasien. Penelitian ini mengevaluasi postur keamanan siber RME menggunakan standar terbaru NIST *Cybersecurity Framework* (CSF) 2.0 melalui pendekatan Tingkatan Implementasi (*Implementation Tiers*). Menggunakan metode studi kasus kualitatif, data dikumpulkan berdasarkan enam fungsi inti: G*overn, Identify, Protect, Detect, Respond,* dan *Recover*. Hasil analisis menunjukkan postur organisasi secara umum berada pada *Tier* 1 (*Partial*), mencerminkan pengelolaan risiko yang reaktif. Meski fungsi teknis (*Protect, Recover*) mencapai *Tier* 2 (*Risk-Informed*) berkat enkripsi dan *backup*, kelemahan fundamental pada tata kelola (*Govern*) dan deteksi (*Detect*) menciptakan disparitas signifikan. Penelitian ini merekomendasikan penyusunan *Risk Register* formal dan *Incident Response Playbook* untuk mentransformasi postur keamanan menuju *Tier* 3 (*Repeatable*) dalam 12 bulan, menjamin perlindungan data pasien yang terstandar dan adaptif.

1. Pendahuluan

Digitalisasi layanan kesehatan melalui Sistem Rekam Medis Elektronik (RME) di RS Radjak Salemba telah meningkatkan efisiensi operasional, namun juga memunculkan kerentanan baru terhadap keamanan data pasien. Meskipun kontrol teknis seperti enkripsi dan backup rutin telah diterapkan, observasi awal menunjukkan adanya disparitas pada tata kelola keamanan yang masih bersifat reaktif dan belum terstruktur. Hal ini sejalan dengan temuan Gusni dkk. (2021) pada studi kasus di RS Bhayangkara Sespima Polri, yang menyatakan bahwa kelemahan tata kelola keamanan sering kali menjadi celah utama meskipun infrastruktur teknis sudah tersedia. Kondisi ini menciptakan risiko signifikan

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

terhadap kebocoran data dan ketidakpatuhan regulasi jika tidak segera dikelola dengan kerangka kerja yang komprehensif (Zahra dkk., 2021).

Penelitian ini bertujuan mengevaluasi postur keamanan siber RME menggunakan pendekatan terbaru NIST *Cybersecurity Framework* (CSF) 2.0. Dengan fokus pada enam fungsi inti, termasuk fungsi baru *Govern*, analisis ini tidak hanya mengukur celah keamanan teknis, tetapi juga memetakan tingkatan implementasi (*Tiers*) organisasi dari status Partial menuju *Risk-Informed* (NIST, 2024). Evaluasi ini sangat krusial untuk merumuskan rekomendasi perbaikan tata kelola yang adaptif demi menjamin keberlanjutan perlindungan informasi pasien secara menyeluruh.

Penelitian terdahulu mengenai evaluasi keamanan sistem informasi rumah sakit umumnya berfokus pada pengukuran tingkat kepatuhan administratif menggunakan instrumen seperti Indeks KAMI dan ISO/IEC 27001 (Khamil dkk., 2022; Wicaksono dan Putra, 2022; Zaini dkk., 2024), atau audit kapabilitas tata kelola TI menggunakan COBIT 2019 (Gusni dkk., 2021). Berbeda dengan pendekatan berbasis kepatuhan (*compliance-based*) tersebut, penelitian ini menawarkan kebaruan (*novelty*) melalui penerapan standar terkini NIST CSF 2.0 dengan fokus spesifik pada Tingkatan Implementasi (*Implementation Tiers*). Kontribusi utama penelitian ini terletak pada pergeseran perspektif evaluasi: dari sekadar audit daftar periksa (*checklist* audit) menjadi analisis kedalaman budaya manajemen risiko. Melalui pendekatan *Tiering*, penelitian ini mendiagnosis sejauh mana praktik keamanan siber telah melembaga (*institutionalized*) dalam proses bisnis rumah sakit sehingga memberikan wawasan fundamental yang sering terlewatkan oleh audit keamanan konvensional.

2. Metodologi Penelitian

2.1. Metode dan Objek Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus tunggal (*single-case study*) untuk mengeksplorasi dinamika tata kelola keamanan siber pada ekosistem digital RS Radjak Salemba. Mengingat struktur tim TI pada cabang ini yang ringkas (terdiri dari dua personel) serta batasan akses fisik selama periode penelitian, pengumpulan data dipusatkan pada metode wawancara mendalam (*in-depth interview*) secara intensif. Narasumber ditentukan melalui teknik purposive sampling, yakni satu informan kunci (*key informant*) yang menjabat sebagai Kepala Unit Teknologi Informasi. Pemilihan ini didasarkan pada otoritas responden yang memegang kendali penuh atas kebijakan strategis sekaligus operasional teknis sistem RME.

Untuk menjamin keabsahan data tanpa observasi lapangan langsung, penelitian ini menerapkan teknik validasi internal melalui pertanyaan pendalaman (*probing*) dan pengecekan konsistensi (*consistency check*). Peneliti mengajukan pertanyaan verifikasi berulang terkait indikator NIST CSF 2.0 untuk memastikan jawaban responden mengenai ketersediaan dokumen (seperti SOP dan log) serta konfigurasi teknis adalah akurat dan tidak kontradiktif. Selain itu, instrumen wawancara dirancang terstruktur berdasarkan standar NIST untuk meminimalkan subjektivitas interpretasi (Creswell & Creswell, 2018).

2.2. Tahapan Penelitian

Pelaksanaan penelitian dilakukan melalui alur kerja sistematis yang dimulai dari identifikasi kesenjangan tata kelola, studi literatur mendalam mengenai standar NIST CSF

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

2.0, pengumpulan data lapangan, hingga analisis penentuan tingkatan implementasi (*tiering*) yang diakhiri dengan perumusan rekomendasi strategis, sebagaimana digambarkan secara rinci pada Gambar 1 dibawah ini:

Gambar 1. Tahapan Penelitian

Kerangka tahapan ini dirancang menggunakan pendekatan berbasis risiko (*risk-based approach*) untuk memastikan bahwa setiap langkah audit—mulai dari persiapan instrumen hingga validasi temuan yang terfokus pada area-area kritis yang memiliki dampak terbesar terhadap kerahasiaan dan ketersediaan data pasien, sehingga hasil akhirnya dapat memberikan peta jalan perbaikan yang konkret dan terukur bagi manajemen rumah sakit.

2.3. Kerangka Analisis dan Instrumen Penelitian

Analisis postur keamanan dalam penelitian ini berlandaskan pada NIST *Cybersecurity Framework* (CSF) versi 2.0 yang membedah kapabilitas organisasi melalui enam fungsi inti (*Govern, Identify, Protect, Detect, Respond, Recover*), di mana instrumen wawancara disusun berdasarkan kategori-kategori tersebut seperti yang dirincikan dalam Tabel 1 berikut:

Tabel 1: Instrumen Pertanyaan NIST CSF 2.0

NIST Core Function	**Pertanyaan**
Govern	Secara umum, bagaimana tim IT mengidentifikasi dan mengelola risiko-risiko

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

	keamanan pada Sistem RME?
	Apakah ada mekanisme pencatatan risiko seperti *Risk Register*, atau bagaimana temuan risiko dikomunikasikan ke manajemen?
Protect	Bisa tolong jelaskan langkah-langkahnya, bagaimana proses pemberian hak akses untuk pengguna baru (misalnya dokter/perawat) pada sistem RME?
	Bagaimana proses pencabutan hak akses jika ada pengguna yang sekiranya bukan lagi seorang staf atau pegawai rumah sakit? Berapa lama jangkauan waktu yang dibutuhkan hingga aksesnya benar-benar dicabut?
	Bagaimana tim IT memastikan setiap pengguna hanya bisa mengakses data sesuai kewenangannya saja (prinsip *least privilege*)?
	Bagaimana data RME pasien dilindungi saat disimpan di server (data *at rest*)? Apakah ada teknologi seperti enkripsi yang digunakan?
	Bagaimana data RME dilindungi saat diakses melalui jaringan rumah sakit (data in transit) untuk mencegah adanya penyadapan data?
	Bagaimana prosedur pencadangan (*backup*) data RME dilakukan? Seberapa sering dilakukan, dan apakah pernah diuji untuk memastikan datanya bisa dipulihkan (*restore*)?
	Apakah ada sosialisasi atau pelatihan yang diberikan kepada para pengguna (dokter/perawat) tentang pentingnya menjaga kerahasiaan data pasien?
Detect	Setelah hak akses diberikan, bagaimana tim IT memantau atau mencatat (*logging*) aktivitas pengguna di dalam sistem RME untuk mendeteksi aktivitas yang tidak wajar?
	Selain perlindungan seperti enkripsi, adakah sistem yang memantau jaringan atau server secara aktif untuk mendeteksi potensi ancaman keamanan (seperti upaya peretasan atau *malware*) secara *real-time*?
Respond	Jika terjadi insiden (misalnya Sistem RME error), apa langkah pertama yang biasanya dilakukan oleh tim IT?
Recover	Setelah sistem terganggu, bagaimana secara garis besar proses pemulihan dilakukan untuk memastikan layanan kembali normal dan data pasien tetap aman?

3. Hasil dan Pembahasan

Pengumpulan data dilaksanakan melalui wawancara terstruktur dengan tim IT RS Radjak Salemba menggunakan checklist audit berbasis NIST CSF 2.0 yang mencakup enam fungsi utama (*Govern, Identify, Protect, Detect, Respond, Recover*). Data kualitatif yang diperoleh mencakup prosedur operasional, ketersediaan dokumentasi kebijakan, serta mekanisme respons insiden. Selanjutnya, temuan tersebut dipetakan ke dalam fungsi inti NIST CSF 2.0 untuk menentukan posisi organisasi dalam hierarki Tingkatan Implementasi (*Implementation Tiers*). Pemetaan temuan kunci audit terhadap fungsi NIST disajikan pada Tabel 2.

Tabel 2: Pemetaan Temuan Wawancara ke NIST CSF 2.0 Core Functions

NIST CSF	Jawaban Responden	Implementasi Status
Govern	Identifikasi risiko bersifat reaktif (hanya saat insiden). Kebijakan	*Tier 1 (Partial)*

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

	keamanan terfragmentasi dalam berbagai SOP terpisah. Tidak ada *Risk Register* formal yang dikelola secara berkala.	
Identify	Inventarisasi aset dilakukan manual menggunakan *spreadshee*t terpisah (silo). Penilaian risiko (*risk assessment*) dilakukan secara *ad-hoc* tanpa metodologi standar yang konsisten.	*Tier 1 (Partial)*
Protect	Kontrol teknis cukup memadai: *Role-Based Access Control* (RBAC) diterapkan, enkripsi data aktif, dan VPN digunakan untuk akses jarak jauh. Namun, belum ada kebijakan *Multi-Factor Authentication* (MFA) menyeluruh.	*Tier 2 (Risk-Informed)*
Detect	Pemantauan anomali bergantung pada tinjauan log manual (*manual log review*) yang tidak real-time. Tidak ada sistem deteksi intrusi (IDS) otomatis atau SIEM untuk korelasi event.	*Tier 1 (Partial)*
Respond	Penanganan insiden sangat bergantung pada mekanisme berbasis individu (*person-centric response*), di mana keberhasilan respons ditentukan oleh keahlian personel tertentu tanpa panduan prosedur standar. Belum tersedia *Incident Response Playbook* formal untuk skenario siber spesifik (misal: *ransomware*).	*Tier 1 (Partial)*
Recover	Prosedur *backup* harian berjalan konsisten, namun pengujian pemulihan (*recovery drills*) jarang dilakukan. RTO (*Recovery Time Objective*) belum didefinisikan secara metrik bisnis.	*Tier 2 (Risk-Informed)*

3.1. Hasil Penilaian dan Analisis Tingkatan Implementasi (*Tier Analysis*)

Berbeda dengan pengukuran tingkat kematangan konvensional, penelitian ini menggunakan Tingkatan Implementasi (*Tiers*) NIST CSF 2.0 untuk mengukur sejauh mana praktik manajemen risiko keamanan siber telah melembaga dalam organisasi. Skala tingkatan yang digunakan dijelaskan pada Tabel 3.

Tabel 3: Definisi Tingkatan Implementasi (*Implementation Tiers*) NIST CSF 2.0

Level	Kategori	Deskripsi
1	*Partial*	Praktik manajemen risiko keamanan siber tidak teratur (*ad-hoc*) dan reaktif. Kesadaran risiko terbatas di tingkat organisasi dan tidak ada kolaborasi formal.
2	*Risk-Informed*	Praktik manajemen risiko disetujui manajemen namun belum ditetapkan sebagai kebijakan organisasi menyeluruh. Prioritas risiko mulai terbentuk namun pelaksanaan belum konsisten.
3	*Repeatable*	Praktik manajemen risiko diperbarui secara berkala dan ditetapkan sebagai kebijakan formal. Terdapat proses standar yang konsisten di seluruh organisasi.
4	*Adaptive*	Organisasi mengadaptasi praktik keamanannya secara aktif berdasarkan pengalaman masa lalu dan indikator prediktif. Manajemen risiko menjadi bagian budaya organisasi.

Evaluasi terhadap enam fungsi NIST CSF 2.0 di RS Radjak Salemba menunjukkan bahwa organisasi secara dominan masih berada pada *Tier* 1 (*Partial*), yang mengindikasikan pengelolaan risiko masih bersifat reaktif. Rincian hasil penilaian per fungsi disajikan pada Tabel 4.

Tabel 4: Hasil Penilaian Current Tier Setiap Fungsi NIST CSF 2.0

Fungsi NIST CSF	*Current Tier*	Deskripsi Temuan	Status
Govern	1	Tata kelola keamanan *ad-hoc*. Tidak ada struktur manajemen	Partial

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

		risiko formal, keputusan keamanan tidak berbasis data risiko.	
Identify	1	Inventarisasi aset tidak terpusat, menyulitkan identifikasi kerentanan secara holistik.	Partial
Protect	2	Kontrol teknis (enkripsi, akses) sudah berjalan dengan kesadaran risiko yang baik, namun belum diformalkan dalam kebijakan terpadu.	Risk Informed
Detect	1	Kemampuan deteksi terbatas pada tinjauan manual pasca-insiden, tidak ada kemampuan *real-time*.	Partial
Respond	1	Tidak ada panduan penanganan insiden (*playbook*). Respons sangat bergantung pada mekanisme penanganan berbasis individu (*person-centric response*).	Partial
Recover	2	Prosedur backup disadari kepentingannya dan dijalankan, namun uji pemulihan belum menjadi standar prosedur operasi.	Risk Informed

Berdasarkan pemetaan temuan pada Tabel 4, penentuan tingkatan implementasi dilakukan dengan mencocokkan kondisi faktual lapangan terhadap taksonomi NIST CSF 2.0. Fungsi *Govern* ditetapkan pada Tier 1 (*Partial*) bukan tanpa alasan; temuan menunjukkan bahwa pengelolaan risiko masih bersifat *ad-hoc* dan sangat bergantung pada inisiatif reaktif saat insiden terjadi, tanpa adanya *Risk Register* formal maupun kebijakan tingkat organisasi yang mengatur manajemen risiko secara terstruktur. Sesuai definisi NIST, kondisi di mana "kesadaran risiko terbatas dan tidak ada proses formal" secara mutlak menempatkan fungsi ini di Tier 1.

Sebaliknya, fungsi *Protect* dan *Recover* dinilai telah mencapai Tier 2 (*Risk-Informed*). Hal ini didasari oleh bukti bahwa praktik perlindungan data seperti penerapan enkripsi, manajemen akses (RBAC), dan backup rutin yang telah dijalankan dengan kesadaran penuh terhadap risiko siber, meskipun belum dilembagakan dalam kebijakan tertulis yang baku. Pembedaan ini krusial untuk menunjukkan bahwa secara teknis operasional, RS Radjak Salemba memiliki kapabilitas pertahanan yang cukup baik (*Risk-Informed*), namun fondasi tata kelolanya masih rapuh (*Partial*). Disparitas ini menegaskan bahwa kelemahan utama bukan pada alat teknologi, melainkan pada ketidakhadiran strategi manajerial yang mengikat.

Selain tata kelola, kelemahan pada fungsi *Identify* (*Tier* 1) memiliki implikasi operasional yang serius. Ketiadaan manajemen aset terpusat meningkatkan risiko *shadow* IT, di mana perangkat atau aplikasi tidak berizin dapat terhubung ke jaringan rumah sakit tanpa sepengetahuan tim TI, membuka celah masuk bagi malware. Lebih lanjut, inventarisasi yang masih manual (*silo*) menyebabkan rumah sakit tidak memiliki visibilitas utuh terhadap ketergantungan sistem dengan vendor pihak ketiga (*supply chain risks*). Dalam konteks RME yang menyimpan data sensitif pasien, kegagalan mengidentifikasi di mana saja data tersimpan dan siapa saja vendor yang memiliki akses dapat berakibat fatal pada ketidakpatuhan terhadap regulasi pelindungan data pribadi (Pemerintah Republik Indonesia, 2022).

3.2. Analisis Kesenjangan (*Gap Analysis*) dan Identifikasi Prioritas

Analisis kesenjangan dilakukan untuk membandingkan kondisi postur saat ini (*Current Tier*) terhadap target yang diharapkan. Dalam penelitian ini, target ditetapkan pada Tier 3 (*Repeatable*). Penetapan target ini didasarkan pada karakteristik kritis data rekam medis yang membutuhkan standar perlindungan tinggi sesuai regulasi kesehatan (Kementerian Kesehatan Republik Indonesia, 2022). Institusi layanan kesehatan tidak dapat bergantung

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

pada manajemen risiko yang berbasis individu atau pengetahuan informal (*Tier* 2), karena rentan terhadap inkonsistensi saat terjadi pergantian personel. Oleh karena itu, pencapaian *Tier* 3 yang di mana kebijakan keamanan telah diformalkan, didokumentasikan, dan diperbarui secara berkala sebagai standar organisasi akan menjadi syarat mutlak untuk menjamin kerahasiaan data pasien secara berkelanjutan, sekaligus merupakan target yang realistis untuk dicapai dalam jangka pendek dibandingkan Tier 4 (*Adaptive*) yang memerlukan investasi teknologi prediktif yang kompleks (Gordon dkk., 2020). Ringkasan analisis kesenjangan antara kondisi saat ini dan target Tier 3 disajikan pada Tabel 5.

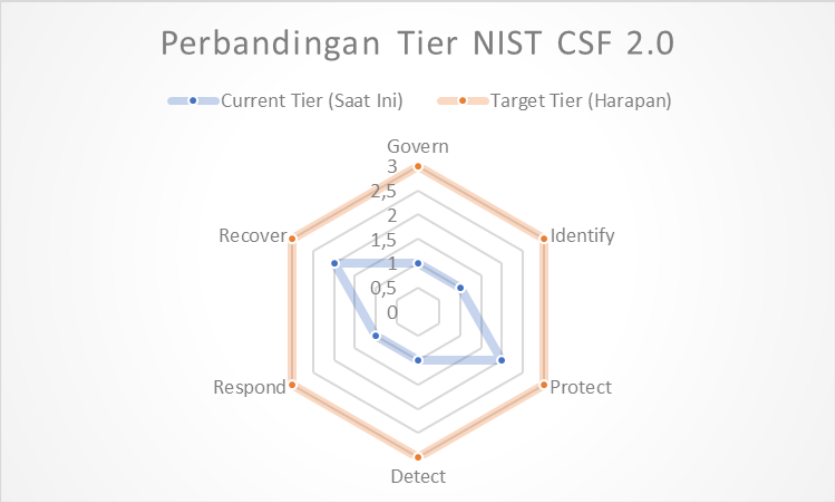
Tabel 5: Analisis Kesenjangan *(Gap Analysis*) dan Prioritas Perbaikan

Fungsi NIST CSF	*Current Tier*	Target *Tier*	Gap	Prioritas	Deskripsi Kesenjangan Utama
Govern	1	3	2	*URGENT*	Ketiadaan kebijakan formal membuat manajemen risiko tidak terarah dan bergantung pada individu.
Identify	1	3	2	*High*	Manajemen aset manual (silo) meningkatkan risiko *shadow* IT dan kerentanan tak terdeteksi.
Protect	2	3	1	*Medium*	Kontrol teknis perlu ditingkatkan menjadi kebijakan baku dan diaudit secara berkala.
Detect	1	3	2	*URGENT*	Ketidakmampuan mendeteksi serangan *real-time* memperbesar dampak insiden siber.
Respond	1	3	2	*URGENT*	*Respons* insiden tanpa prosedur baku berpotensi memperparah kebocoran data pasien.
Recover	2	3	1	*Medium*	Rencana pemulihan belum teruji efektivitasnya melalui simulasi rutin.

Dari Tabel 5, teridentifikasi tiga area prioritas Urgent dengan celah terbesar (*Gap* 2 *Level*), yaitu pada fungsi *Govern, Detect, dan Respond.* Kegagalan menutup celah ini dapat mengakibatkan ketidakpatuhan regulasi dan gangguan operasional fatal pada layanan RME.

Untuk memperjelas disparitas antara postur keamanan saat ini dengan kondisi ideal yang diharapkan, visualisasi kesenjangan disajikan pada Gambar 2. Grafik radar tersebut menunjukkan secara visual area-area kritis yang mengalami "kempis" (Tier 1), khususnya pada fungsi strategis Govern dan Identify, dibandingkan dengan fungsi operasional seperti Protect yang sedikit lebih unggul.

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi



Gambar 2. Visualisasi Perbandingan Current Tier vs Target Tier pada Enam Fungsi NIST CSF 2.0

3.3. Rekomendasi Perbaikan Berbasis NIST CSF 2.0

Rekomendasi perbaikan disusun secara bertahap untuk mentransformasi postur keamanan dari *Partial* menuju *Repeatable*, dengan fokus utama pada penguatan tata kelola (*governance*) sebelum investasi teknologi lanjut, sejalan dengan prinsip keamanan informasi yang menekankan aspek manajerial sebagai fondasi pertahanan (Whitman dan Mattord, 2021). Rincian rekomendasi disajikan pada Tabel 6 berikut:

Tabel 6: Gap Analysis dan Prioritas Perbaikan

Prioritas	Fungsi NIST	Rekomendasi	Outcome Diharapkan
Urgent (0-3 Bulan)	*Govern*	Menyusun dan mengesahkan *Risk Register* formal yang ditinjau berkala oleh manajemen puncak atau pimpinan.	Pengambilan keputusan berbasis risiko (*Risk-based decision making*).
	Govern	Mengonsolidasikan SOP terpisah menjadi Kebijakan Keamanan Informasi Organisasi yang terpadu.	Tata kelola terstruktur dan kepatuhan standar (*Tier* 3).
	Respond	Membuat *Incident Response Playbook* untuk 5 skenario kritis (misal: *Ransomware*, Kebocoran Data).	Penanganan insiden yang terukur dan tidak bergantung individu.
Medium (3-12 Bulan)	*Identify*	Implementasi sistem Manajemen Aset Terpusat untuk menggantikan *spreadsheet* manual.	Visibilitas aset menyeluruh (*holistic visibility*).
	Detect	Implementasi solusi monitoring jaringan otomatis (SIEM/IDS) untuk deteksi ancaman *real-time*.	Deteksi dini untuk meminimalkan dampak serangan.

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

Recover	Melaksanakan *Disaster Recovery Drill* minimal 6 bulan sekali untuk memvalidasi RTO/RPO.	Kesiapan pemulihan yang teruji dan valid (*Validated recovery*).

Dengan implementasi disiplin terhadap rekomendasi di atas dalam kurun waktu 12 bulan, RS Radjak Salemba diharapkan dapat mencapai stabilitas operasional pada *Tier* 3, di mana perlindungan data pasien dijamin oleh kebijakan yang baku dan proses yang dapat diulang (*repeatable*), bukan lagi sekadar upaya reaktif.

3.4. Implikasi Praktis dan Manajerial

Peningkatan status tata kelola dari Tier 1 menuju Tier 3 memiliki implikasi strategis yang signifikan bagi manajemen RS Radjak Salemba. Pertama, formalisasi kebijakan melalui Risk Register akan meningkatkan kesiapan audit (audit readiness) rumah sakit dalam menghadapi akreditasi, mengingat standar keamanan data kini menjadi salah satu indikator penilaian utama layanan kesehatan. Kedua, transisi dari respons berbasis individu (person-centric) menuju prosedur standar (playbook) akan meminimalkan risiko operasional saat terjadi pergantian personel TI, sehingga keberlanjutan sistem RME tidak terganggu.

Ketiga, dan yang paling krusial, penguatan postur keamanan ini berkontribusi langsung pada peningkatan kepercayaan pasien (patient trust). Dalam ekosistem kesehatan digital, jaminan kerahasiaan rekam medis bukan sekadar kepatuhan teknis, melainkan aset reputasi. Dengan mencapai Tier 3, rumah sakit dapat menjamin kepada publik bahwa data sensitif mereka dikelola dengan standar perlindungan yang teruji, bukan sekadar upaya reaktif.

4. Kesimpulan dan Saran

Evaluasi postur keamanan siber RME RS Radjak Salemba menggunakan NIST *Cybersecurity Framework* 2.0 mengungkapkan bahwa organisasi secara umum masih berada pada Tier 1 (*Partial*). Kondisi ini mencerminkan pengelolaan risiko yang bersifat reaktif dan sangat bergantung pada inisiatif individu (*person-centric response*) tanpa pelembagaan kebijakan formal. Meskipun fungsi teknis seperti *Protect* dan *Recover* telah mencapai *Tier* 2 (*Risk-Informed*) melalui penerapan enkripsi dan *backup*, kelemahan fundamental pada fungsi *Govern* dan *Detect* menciptakan disparitas kapabilitas yang signifikan. Organisasi memiliki alat pengamanan dasar, namun tidak memiliki visi strategi risiko yang terstruktur maupun kemampuan deteksi ancaman *real-time*, sehingga rentan terhadap kegagalan sistemik dalam menjaga kerahasiaan data pasien.

Untuk mentransformasi postur keamanan menuju kondisi *Tier* 3 (*Repeatable*), manajemen disarankan memprioritaskan penguatan tata kelola sebelum ekspansi teknologi. Langkah strategis mendesak meliputi penyusunan *Risk Register* formal dan konsolidasi kebijakan keamanan informasi untuk menghilangkan ketergantungan pada personil tertentu. Selanjutnya, kapabilitas *respons* perlu distandarisasi melalui pembuatan *Incident Response Playbook* dan pelaksanaan simulasi pemulihan (DR *Drill*) secara berkala dalam siklus 12 bulan ke depan. Implementasi disiplin terhadap rekomendasi ini akan menjamin bahwa keamanan data pasien dikelola oleh sistem yang baku, terukur, dan adaptif sesuai standar keamanan modern.

Available online at https://ejournal.upnvj.ac.id/jsia
Jurnal Sistem Informasi dan Aplikasi
Volume 3 | Issue 2 | bulan Desember (2025)
e-issn : 3025 – 9347
JSIA
Jurnal Sistem Informasi & Aplikasi

Referensi

Creswell, J.W. dan Creswell, J.D. (2018) Research design: Qualitative, quantitative, and mixed methods approaches. Edisi ke-5. Los Angeles: SAGE Publications.

Gordon, L.A., Loeb, M.P. dan Zhou, L. (2020) 'Integrating Cost-Benefit Analysis into the NIST Cybersecurity Framework', Communications of the ACM, 63(5), hlm. 24–27.

Gusni, R.S.A., Kraugusteeliana, K. dan Pradnyana, I.W.W. (2021) 'Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019', Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA), 2(2), hlm. 420–429.

Kementerian Kesehatan Republik Indonesia (2022) Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Jakarta: Berita Negara Republik Indonesia.

Khamil, D.I., Sasmita, G.M.A. dan Susila, A.A.N.H. (2022) 'Evaluasi tingkat kesiapan keamanan informasi menggunakan Indeks KAMI 4.2 dan ISO/IEC 27001:2013 (Studi kasus: Diskominfo Kabupaten Gianyar)', Jurnal Teknologi Informasi dan Sistem Informasi, 9(3), hlm. 245–260.

NIST (2024) Cybersecurity Framework version 2.0. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Pemerintah Republik Indonesia (2022) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Jakarta: Lembaran Negara Republik Indonesia.

Whitman, M.E. dan Mattord, H.J. (2021) Principles of Information Security. Edisi ke-7. Boston: Cengage Learning.

Wicaksono, D.A. dan Putra, I.M.A.W. (2022) 'Evaluasi tingkat kesiapan keamanan informasi menggunakan Indeks KAMI 4.2 dan ISO/IEC 27001:2013 (Studi kasus: Diskominfo Kabupaten Gianyar), Jurnal Teknologi Informasi dan Sistem Informasi, 9(3), hlm. 245–260.

Zahra, M.N., Dzakiyyah, A., Munjiyanti, S.K., Rachim, N.A. dan Kraugusteeliana, K. (2021) 'Manajemen Risiko Sistem Informasi Rumah Sakit (Studi Kasus: Rumah Sakit EMC Tangerang)', Senamika, 2(1), hlm. 1-10.

Zaini, A.Y.F., Sugiantoro, B. dan Riwanto, Y. (2024) 'Analisis evaluasi keamanan informasi pada badan pemerintahan pemerintahan XYZ menggunakan Indeks KAMI 4.2', Jurnal Sistem Informasi dan Keamanan Informasi, 10(1), hlm. 32–48.