Journal of Information Technology and Computer Science (INTECOMS)
Volume 9 Nomor 3, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

LAYERED MAPPING MODEL FOR INFORMATION SYSTEM SECURITY EVALUATION BASED ON NIST CSF 2.0, COBIT 2019, AND NIST SP 800-53

MODEL LAYERED MAPPING EVALUASI KEAMANAN SISTEM INFORMASI BERBASIS NIST CSF 2.0, COBIT 2019, DAN NIST SP 800-53

Fendi Setiabudi[1], Alva Hendi Muhammad[2] , Sri Ngudi Wahyuni[3]
Universitas Amikom Yogyakarta
fendi2168@gmail.com[1], alva@amikom.ac.id[2], yuni@amikom.ac.id[3]

ABSTRACT

Cybersecurity evaluation is necessary to identify the security condition and gaps within an information system. The Forest Product Administration Information System (SIPUHH) is an information system used to support electronic recording and reporting in forest product administration processes. This study aims to develop a layered mapping approach for evaluating SIPUHH cybersecurity in a structured and traceable manner. The frameworks used are NIST CSF 2.0 as the cybersecurity outcome layer, COBIT 2019 APO13 – Managed Security as the management layer, and NIST SP 800-53 as the security control layer. This study employs a qualitative approach using an evaluative research design with a descriptive-analytical orientation. Data were collected through interviews with SIPUHH developers and responsible personnel, as well as through verification of technical and documentary evidence. The results of the layered mapping were operationalized into 27 indicators to establish the Current Profile, formulate the Target Profile, and identify SIPUHH cybersecurity gaps. The evaluation results show that 10 indicators are classified as High priority, 15 indicators as Medium priority, and 2 indicators as Maintenance. The findings indicate that SIPUHH has established several technical and operational security capabilities; however, these capabilities are not yet fully supported by formal and structured security governance, policies, procedures, documentation, and evaluation processes. The analysis of interrelationships among the findings resulted in six security improvement programs covering governance and risk management, third parties and interconnections, protection controls, monitoring and event analysis, incident response, and service resilience and recovery.

Keywords*: Cybersecurity Evaluation; Layered Mapping; NIST CSF 2.0; COBIT 2019; NIST SP 800-53.*

ABSTRAK

Evaluasi keamanan siber diperlukan untuk mengidentifikasi kondisi keamanan dan kesenjangan pada sebuah sistem informasi. Sistem Informasi Penatausahaan Hasil Hutan (SIPUHH) merupakan sistem informasi yang digunakan untuk mendukung pencatatan dan pelaporan elektronik dalam proses penatausahaan hasil hutan. Penelitian ini bertujuan mengembangkan layered mapping untuk melakukan evaluasi keamanan SIPUHH secara terstruktur dan dapat ditelusuri. Framework yang digunakan adalah NIST CSF 2.0 sebagai cybersecurity outcome layer, COBIT 2019 APO13 – Managed Security sebagai management layer, dan NIST SP 800-53 sebagai security control layer. Penelitian menggunakan pendekatan kualitatif dengan jenis penelitian evaluatif dan bersifat deskriptif-analitis. Data diperoleh melalui wawancara dengan pengembang dan penanggung jawab SIPUHH serta verifikasi bukti teknis dan dokumenter. Hasil layered mapping dioperasionalkan menjadi 27 indikator untuk membentuk Current Profile, merumuskan Target Profile, dan mengidentifikasi gap keamanan SIPUHH. Hasil evaluasi menunjukkan bahwa 10 indikator memiliki prioritas Tinggi, 15 indikator prioritas Sedang, dan 2 indikator berada pada kategori Pemeliharaan. Temuan menunjukkan bahwa SIPUHH telah memiliki sejumlah kapabilitas teknis dan operasional keamanan, tetapi belum seluruhnya didukung oleh tata kelola, kebijakan, prosedur, dokumentasi, dan proses evaluasi keamanan yang formal dan terstruktur. Analisis keterkaitan antartemuan menghasilkan enam program peningkatan keamanan yang mencakup tata kelola dan manajemen risiko, pihak ketiga dan interkoneksi, kontrol perlindungan, monitoring dan analisis kejadian, respons insiden, serta ketahanan dan pemulihan layanan.

Kata Kunci: keamanan siber; layered mapping; NIST CSF 2.0; COBIT 2019; NIST SP 800-53.

PENDAHULUAN

Transformasi digital meningkatkan ketergantungan organisasi terhadap sistem informasi sekaligus kebutuhan pengelolaan keamanan siber yang mencakup aspek teknis, tata kelola, manajemen risiko, pemantauan, penanganan insiden, dan pemulihan layanan (Taherdoost, 2022;

Syafrizal et al., 2020). Evaluasi keamanan siber diperlukan untuk mengidentifikasi kondisi keamanan yang telah diterapkan dan area yang masih memerlukan peningkatan.

Penelitian ini diterapkan pada Sistem Informasi Penatausahaan Hasil Hutan (SIPUHH), yaitu sistem informasi berbasis web yang mendukung pencatatan dan pelaporan elektronik dalam proses penatausahaan hasil hutan, mulai dari perencanaan produksi hingga peredaran dan pemasaran. Keterkaitan antartahapan tersebut menjadikan keberlangsungan layanan, integritas data, dan keamanan SIPUHH penting sehingga diperlukan evaluasi yang mencakup aspek tata kelola maupun mekanisme teknis.

Berbagai penelitian telah mengombinasikan framework keamanan siber untuk mendukung audit dan evaluasi keamanan (Fadila et al., 2023; Fadya & Utama, 2025; Sulistyowati et al., 2020). Namun, perbedaan tujuan, struktur, dan tingkat abstraksi antar-framework menimbulkan tantangan dalam membangun pemetaan yang konsisten (Mussmann et al., 2020). Irawan et al. (2024) mengembangkan pemetaan Subcategory NIST CSF v1.1 dengan Subcontrol CIS Controls v8 untuk membentuk kerangka penilaian kematangan keamanan siber. Penelitian ini memperbarui pendekatan tersebut dengan menggunakan NIST CSF 2.0 serta memperluas pemetaan melalui COBIT 2019 APO13 – Managed Security dan NIST SP 800-53. Mekanisme yang mempertahankan keterlacakan secara berlapis dari cybersecurity outcome, perspektif pengelolaan, referensi kontrol, hingga indikator dan bukti evaluasi masih terbatas dan menjadi research gap penelitian ini.

Berdasarkan gap tersebut, penelitian ini mengembangkan layered mapping dengan menempatkan NIST CSF 2.0 sebagai cybersecurity outcome layer, COBIT 2019 APO13 – Managed Security sebagai management layer, dan NIST SP 800-53 sebagai security control layer. Hasil pemetaan dioperasionalkan menjadi instrumen evaluasi dan diterapkan untuk mengidentifikasi kondisi eksisting serta kesenjangan keamanan SIPUHH. Kontribusi penelitian terletak pada mekanisme evaluasi yang mempertahankan keterlacakan vertikal dari framework hingga bukti evaluasi serta memungkinkan keterkaitan horizontal antartemuan dianalisis sebagai dasar perumusan peningkatan keamanan SIPUHH.

TINJAUAN PUSTAKA

Penelitian mengenai evaluasi keamanan siber menunjukkan bahwa penggunaan framework memberikan struktur yang sistematis untuk mengidentifikasi kondisi keamanan dan menentukan area yang memerlukan peningkatan. Taherdoost (2022) menunjukkan bahwa berbagai framework dan standar keamanan memiliki karakteristik, ruang lingkup, dan pendekatan yang berbeda sehingga pemilihannya perlu disesuaikan dengan kebutuhan organisasi. Perkembangan penelitian berikutnya juga menunjukkan bahwa NIST Cybersecurity Framework (CSF) banyak digunakan sebagai dasar evaluasi karena menyediakan struktur outcome keamanan yang dapat diterapkan pada berbagai konteks organisasi. Bernardo et al. (2025), misalnya, mengembangkan pendekatan penilaian maturity yang diselaraskan dengan NIST CSF untuk mengukur kondisi keamanan dan mendukung identifikasi kebutuhan peningkatan.

Penggunaan lebih dari satu framework juga berkembang untuk memperoleh perspektif evaluasi yang lebih luas. Fadila et al. (2023) mengombinasikan CIS Critical Security Controls, NIST CSF, dan COBIT 2019 dalam audit keamanan siber pada organisasi pemerintahan. CIS CSC digunakan untuk membatasi fokus area keamanan aset teknologi informasi, sedangkan NIST CSF dan COBIT 2019 digunakan dalam penilaian kemampuan

pengelolaan keamanan. Penelitian tersebut menunjukkan bahwa kombinasi framework dapat digunakan untuk memperluas cakupan evaluasi dibandingkan dengan penggunaan satu framework secara terpisah.

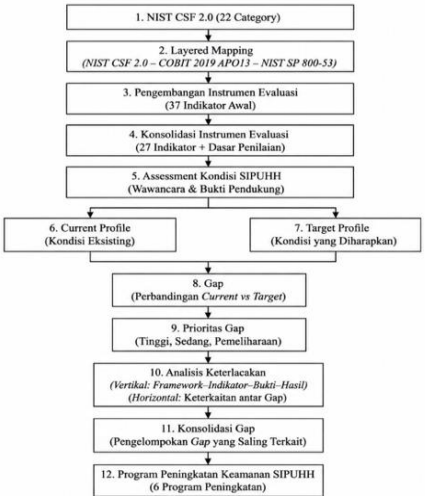
Pendekatan integrasi NIST CSF dan COBIT 2019 juga digunakan oleh Fadya dan Utama (2025) untuk mengembangkan model evaluasi keamanan informasi. Model tersebut mengintegrasikan aktivitas NIST CSF dan COBIT 2019 serta menggunakan Capability Maturity Model Integration (CMMI) untuk menentukan tingkat maturity keamanan. Hasil pengembangan menghasilkan 118 aktivitas dalam 23 kategori yang kemudian diterapkan pada sistem informasi organisasi sektor publik. Penelitian tersebut memperlihatkan bahwa NIST CSF dan COBIT 2019 dapat digunakan secara komplementer untuk menghubungkan perspektif keamanan dengan pengelolaan teknologi informasi.

Penelitian yang lebih baru semakin menekankan sifat komplementer antar-framework. Liu et al. (2025) mengembangkan model proses hierarkis untuk pengelolaan keamanan siber dan menunjukkan bahwa NIST CSF memberikan arahan pada tingkat pengelolaan risiko, tetapi penerapannya dapat memerlukan standar tambahan yang menyediakan proses dan kontrol yang lebih rinci. Rambau et al. (2026) juga membandingkan NIST CSF 2.0, ISO/IEC 27001:2022, dan COBIT 2019 pada konteks e-government dan menemukan bahwa masing-masing memberikan kekuatan yang berbeda, sehingga integrasi yang mempertimbangkan konteks organisasi dapat memberikan perspektif ketahanan siber yang lebih komprehensif.

Berdasarkan penelitian terdahulu tersebut, penggunaan dan integrasi beberapa framework telah dilakukan untuk audit, pengukuran maturity, evaluasi keamanan, maupun pembentukan model keamanan. Namun, penelitian-penelitian tersebut belum berfokus pada mekanisme evaluasi yang mempertahankan keterlacakan secara berlapis dari cybersecurity outcome, perspektif pengelolaan keamanan, referensi kontrol, hingga indikator dan bukti evaluasi. Penelitian ini membedakan diri dengan mengembangkan layered mapping yang menempatkan NIST CSF 2.0 sebagai cybersecurity outcome layer, COBIT 2019 APO13 – Managed Security sebagai management layer, dan NIST SP 800-53 sebagai security control layer. Hasil pemetaan selanjutnya dioperasionalkan menjadi instrumen evaluasi dan diterapkan secara empiris pada SIPUHH sehingga keterlacakan vertikal dari framework hingga hasil assessment serta keterkaitan horizontal antartemuan dapat dipertahankan.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian evaluatif dan bersifat deskriptif-analitis. Penelitian dilakukan untuk mengembangkan layered mapping sebagai dasar evaluasi keamanan SIPUHH serta menerapkannya dalam mengidentifikasi kondisi aktual dan kesenjangan keamanan. Tahapan penelitian meliputi pembangunan layered mapping, pengembangan instrumen evaluasi, pelaksanaan assessment, pembentukan Current Profile dan Target Profile, analisis kesenjangan, analisis keterkaitan temuan, serta perumusan program peningkatan keamanan. Alur penelitian disajikan pada Gambar 1.



Gambar 1. Alur Penelitian

Berdasarkan Gambar 1, tahap pertama dilakukan dengan membangun layered mapping menggunakan 22 Category NIST CSF 2.0 sebagai unit awal pemetaan. NIST CSF 2.0 ditempatkan sebagai cybersecurity outcome layer, COBIT 2019 APO13 – Managed Security sebagai management layer, dan NIST SP 800-53 sebagai security control layer. Pemilihan APO13 sebagai management anchor dilakukan karena objektif tersebut berfokus pada pengelolaan keamanan, sedangkan objektif COBIT 2019 lain dapat digunakan sebagai supporting objective apabila memiliki keterkaitan langsung dengan Category yang dipetakan.

Pemetaan dilakukan secara konseptual berdasarkan kesesuaian keyword/theme, tujuan, dan ruang lingkup masing-masing elemen framework. Pendekatan tersebut mempertimbangkan concept mapping sebagai mekanisme untuk mendokumentasikan hubungan antarkonsep dari sumber keamanan yang berbeda sebagaimana dijelaskan oleh Scarfone et al. (2024). Hubungan yang terbentuk tidak dimaknai sebagai ekuivalensi atau hubungan satu-ke-satu antar-framework, tetapi sebagai keterkaitan konseptual yang digunakan untuk membangun keterlacakan dari cybersecurity outcome menuju perspektif pengelolaan dan referensi kontrol keamanan.

Pada NIST SP 800-53, pemetaan dilakukan pada tingkat control family. Satu Category dapat memiliki primary family yang merepresentasikan keterkaitan utama dan supporting family apabila terdapat aspek keamanan lain yang relevan. Pendekatan yang sama digunakan pada COBIT 2019 dengan APO13 sebagai management anchor dan objective lain sebagai supporting objective apabila diperlukan. Contoh hasil layered mapping dan proses operasionalisasinya menjadi indikator evaluasi disajikan pada Tabel 1.

Tabel 1. Contoh Hasil Layered Mapping dan Operasionalisasi Indikator

Category NIST CSF 2.0	Hasil Layered Mapping	Indikator Evaluasi
GV.PO – Policy	APO13 – Managed Security → PL – Planning	GV.PO-01 Kebijakan Keamanan Informasi SIPUHH
ID.RA – Risk Assessment	APO13 – Managed Security → RA – Risk Assessment	ID.RA-01 Penilaian Risiko Keamanan SIPUHH
PR.AT – Awareness and Training	APO13 – Managed Security → AT – Awareness and Training	PR.AT-01 Pelatihan dan Kesadaran Keamanan Informasi
DE.CM – Continuous Monitoring	APO13 – Managed Security → CA – Assessment, Authorization, and Monitoring	DE.CM-01 Monitoring Infrastruktur dan Layanan SIPUHH
RS.MA – Incident Management	APO13 – Managed Security → IR – Incident Response	RS.MA-01 Pengelolaan dan Eskalasi Insiden
RC.RP – Incident Recovery Plan Execution	APO13 – Managed Security → CP – Contingency Planning	RC.RP-01 Perencanaan dan Pelaksanaan Pemulihan SIPUHH

Tahap kedua adalah pengembangan instrumen evaluasi. Hasil layered mapping diterjemahkan menjadi fokus evaluasi yang dapat diperiksa pada objek penelitian. Setiap fokus kemudian dioperasionalkan menjadi indikator evaluasi yang dilengkapi dengan bukti yang dicari, pertanyaan evaluasi, dan Dasar Penilaian. Bukti yang dicari digunakan untuk menentukan informasi atau artefak yang perlu diverifikasi, sedangkan pertanyaan evaluasi digunakan untuk mengarahkan proses wawancara dan memperoleh informasi yang relevan dengan indikator yang diperiksa.

Pada tahap awal diperoleh 37 indikator evaluasi yang merepresentasikan kebutuhan evaluasi dari 22 Category NIST CSF 2.0. Indikator tersebut selanjutnya ditinjau berdasarkan kesamaan fokus evaluasi, keterkaitan dalam satu rangkaian proses, serta potensi overlap dan double counting. Indikator yang mengukur fokus atau rangkaian proses yang sama dikonsolidasikan dengan tetap mempertahankan keterlacakan terhadap Category dan hasil layered mapping yang menjadi sumbernya. Proses tersebut menghasilkan 27 indikator final yang mencakup enam Function NIST CSF 2.0, yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. Mekanisme konsolidasi tersebut konsisten dengan rancangan instrumen penelitian yang tidak mengubah struktur 22 Category, tetapi mengoperasionalkannya menjadi unit evaluasi yang sesuai untuk pemeriksaan kondisi keamanan.

Untuk menjaga reproducibility, 27 indikator final yang digunakan dalam proses evaluasi disajikan pada Tabel 2. Instrumen tersebut mempertahankan kode Category pada kode indikator sehingga setiap hasil evaluasi dapat ditelusuri kembali ke sumber framework yang mendasarinya.

Tabel 2. Instrumen Evaluasi Keamanan SIPUHH

Function	Kode dan Indikator Evaluasi
Govern	GV.OC-01 Struktur, Peran, dan Tanggung Jawab Pengelolaan SIPUHH; GV.OC-02 Tujuan dan Ruang Lingkup Layanan SIPUHH; GV.OC-03 Regulasi Penyelenggaraan SIPUHH; GV.OC-04 Dokumentasi Proses Bisnis SIPUHH; GV.RM-01 Strategi dan Tata Kelola Manajemen Risiko Keamanan; GV.RR-01 Peran, Tanggung Jawab, dan Kewenangan Keamanan SIPUHH; GV.PO-01 Kebijakan Keamanan Informasi SIPUHH; GV.OV-01 Evaluasi dan Pengawasan Keamanan SIPUHH; GV.SC-01 Pengelolaan Risiko Keamanan Pihak Ketiga; GV.SC-02 Pengelolaan Layanan Eksternal dan Interkoneksi SIPUHH
Identify	ID.AM-01 Inventaris dan Pengelolaan Aset Teknologi SIPUHH; ID.RA-01 Penilaian Risiko Keamanan SIPUHH; ID.IM-01 Evaluasi dan Peningkatan Keamanan SIPUHH
Protect	PR.AA-01 Pengelolaan Identitas dan Hak Akses SIPUHH; PR.AT-01 Pelatihan dan Kesadaran Keamanan Informasi; PR.DS-01 Perlindungan dan Backup Data SIPUHH; PR.PS-01 Baseline dan Hardening Platform/Server; PR.IR-01 Perlindungan Jaringan dan Pengelolaan Firewall; PR.IR-02 Ketahanan Infrastruktur dan Mekanisme Redundasi
Detect	DE.CM-01 Monitoring Infrastruktur dan Layanan SIPUHH; DE.AE-01 Analisis dan Klasifikasi Kejadian Keamanan
Respond	RS.MA-01 Pengelolaan dan Eskalasi Insiden; RS.AN-01 Analisis dan Investigasi Insiden; RS.CO-01 Pelaporan dan Komunikasi Insiden; RS.MI-01 Mitigasi dan Containment Insiden
Recover	RC.RP-01 Perencanaan dan Pelaksanaan Pemulihan SIPUHH; RC.CO-01 Komunikasi dan Koordinasi Pemulihan

Dasar Penilaian ditetapkan sebagai bagian dari pengembangan instrumen sebelum pelaksanaan assessment dan digunakan untuk menjaga konsistensi pemeriksaan pada setiap indikator. Dasar Penilaian memuat aspek dan bukti yang perlu diperiksa melalui wawancara dan verifikasi bukti teknis maupun dokumenter. Hasil assessment kemudian dicatat sebagai Evidence Aktual dan digunakan sebagai dasar dalam pembentukan Current Profile. Mekanisme ini menjaga agar kondisi aktual tidak ditentukan berdasarkan persepsi responden semata, tetapi berdasarkan bukti yang dapat diverifikasi.

Tahap ketiga adalah pelaksanaan assessment kondisi keamanan SIPUHH menggunakan 27 indikator final. Pengumpulan data dilakukan melalui wawancara dengan lima informan yang terlibat dalam pengelolaan dan pengembangan SIPUHH, yaitu database administrator, system administrator, dua programmer, dan Ketua Pokja SIPUHH. Wawancara dilakukan dalam beberapa sesi selama Agustus 2026 dan dilengkapi dengan pemeriksaan bukti teknis maupun dokumenter sesuai karakteristik indikator yang dievaluasi.

Pada setiap indikator, informasi hasil wawancara dianalisis bersama bukti pendukung yang tersedia. Bukti dapat berupa dokumen, konfigurasi, laporan pengujian, catatan monitoring, dokumentasi operasional, maupun bukti teknis lain yang relevan. Kondisi yang ditemukan selanjutnya dicatat sebagai Current Profile SIPUHH. Dengan pendekatan tersebut, Current Profile menggambarkan kondisi aktual berdasarkan evidence yang diperoleh pada saat assessment.

Tahap keempat adalah analisis kesenjangan dengan membandingkan Current Profile dan Target Profile pada masing-masing indikator. Current Profile menggambarkan kondisi aktual berdasarkan hasil wawancara dan verifikasi bukti, sedangkan Target Profile menggambarkan kondisi yang diharapkan sesuai konteks dan kebutuhan keamanan SIPUHH. Target Profile dirumuskan setelah kondisi aktual diperoleh, sedangkan indikator dan Dasar Penilaian telah ditetapkan sebelum assessment sehingga penetapan target tidak mengubah batas konseptual indikator yang digunakan.

Perbedaan antara Current Profile dan Target Profile digunakan untuk mengidentifikasi gap dan menentukan kebutuhan peningkatan. Prioritas ditetapkan berdasarkan tingkat kesenjangan yang ditemukan. Prioritas Tinggi diberikan apabila mekanisme utama belum tersedia atau secara fundamental belum memadai. Prioritas Sedang diberikan apabila mekanisme telah tersedia tetapi masih memerlukan penguatan pada aspek formalitas, dokumentasi, cakupan, atau konsistensi. Kategori Pemeliharaan diberikan apabila kondisi utama telah tersedia dan didukung bukti yang memadai sehingga mekanisme tersebut perlu dipertahankan dan dimonitor. Rubrik penilaian disajikan pada Tabel 3.

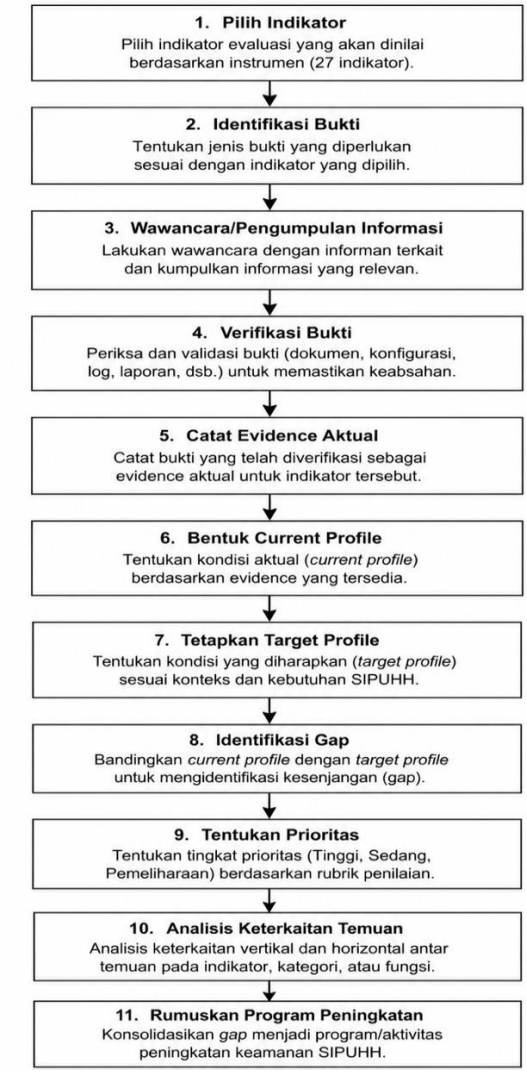
Tabel 3. Rubrik Penilaian Hasil Evaluasi

Prioritas	Kriteria Penilaian	Interpretasi
Tinggi	Mekanisme utama belum tersedia atau secara fundamental belum memadai berdasarkan hasil wawancara dan verifikasi bukti.	Terdapat kesenjangan utama terhadap Target Profile dan memerlukan peningkatan sebagai prioritas utama.
Sedang	Mekanisme telah tersedia, tetapi masih memerlukan penguatan pada aspek formalitas, dokumentasi, cakupan, atau konsistensi penerapan.	Terdapat kesenjangan terhadap Target Profile yang memerlukan penguatan.
Pemeliharaan	Kondisi utama telah tersedia dan	Tidak terdapat kesenjangan utama;

	didukung oleh bukti yang memadai.	mekanisme perlu dipertahankan dan dimonitor.

Rubrik pada Tabel 3 digunakan untuk mengklasifikasikan hasil perbandingan Current Profile dan Target Profile pada setiap indikator menjadi prioritas Tinggi, Sedang, atau Pemeliharaan.

Untuk memastikan instrumen dapat diterapkan kembali, prosedur penggunaan instrumen disusun mulai dari pemilihan indikator, identifikasi bukti, pengumpulan informasi, verifikasi evidence, pembentukan Current Profile, penetapan Target Profile, identifikasi gap, hingga penentuan prioritas peningkatan. Prosedur penggunaan instrumen disajikan pada Gambar 2.



Gambar 2. Prosedur Penggunaan Instrumen Evaluasi

Tahap terakhir adalah analisis keterkaitan temuan. Analisis dilakukan secara vertikal dan horizontal. Keterlacakan vertikal digunakan untuk menelusuri hubungan dari Category NIST CSF 2.0, COBIT 2019, NIST SP 800-53, indikator evaluasi, evidence, Current Profile, Target Profile, gap, hingga prioritas peningkatan. Analisis horizontal digunakan untuk mengidentifikasi keterkaitan antartemuan pada indikator, Category, atau Function yang berbeda. Gap yang memiliki hubungan proses atau kebutuhan peningkatan yang sama selanjutnya dikonsolidasikan menjadi program peningkatan keamanan SIPUHH.

HASIL DAN PEMBAHASAN

Hasil Layered Mapping

Layered mapping dilakukan terhadap 22 Category NIST CSF 2.0 dengan menempatkan NIST CSF 2.0 sebagai cybersecurity outcome layer, COBIT 2019 APO13 – Managed Security sebagai management layer, dan NIST SP 800-53 sebagai security control layer. Hasil pemetaan menunjukkan bahwa ketiga framework dapat dihubungkan berdasarkan kesesuaian tujuan, ruang lingkup, dan konteks keamanan yang direpresentasikan pada masing-masing layer. NIST CSF 2.0 memberikan struktur outcome keamanan yang menjadi titik awal evaluasi, COBIT 2019 memberikan perspektif pengelolaan keamanan, sedangkan NIST SP 800-53 memberikan referensi control family yang relevan terhadap outcome dan kebutuhan pengelolaan tersebut.

Hubungan yang dihasilkan tidak selalu bersifat satu-ke-satu. Satu Category NIST CSF 2.0 dapat berkaitan dengan lebih dari satu objective COBIT 2019 maupun control family NIST SP 800-53 sesuai dengan konteks evaluasinya. APO13 – Managed Security digunakan sebagai management anchor untuk mempertahankan fokus pengelolaan keamanan, sedangkan objective COBIT 2019 lainnya dapat berperan sebagai supporting objective. Demikian pula, control family NIST SP

800-53 ditempatkan sebagai primary atau supporting family berdasarkan kedekatannya dengan fokus keamanan yang dievaluasi. Struktur tersebut memungkinkan hubungan antar-framework dipertahankan tanpa menyetarakan elemen yang memiliki fungsi dan tingkat abstraksi berbeda.

Hasil ini menunjukkan bahwa layered mapping tidak hanya menghasilkan hubungan konseptual antar-framework, tetapi membentuk jalur keterlacakan dari cybersecurity outcome menuju perspektif pengelolaan dan referensi kontrol keamanan. Jalur tersebut selanjutnya menjadi dasar untuk mengoperasionalkan hasil pemetaan menjadi instrumen evaluasi yang dapat diterapkan pada SIPUHH.

Hasil Pengembangan Instrumen Evaluasi

Hasil layered mapping selanjutnya diterjemahkan menjadi fokus evaluasi, indikator evaluasi, bukti yang dicari, pertanyaan evaluasi, dan Dasar Penilaian. Proses awal menghasilkan 37 indikator yang merepresentasikan kebutuhan evaluasi dari 22 Category NIST CSF 2.0. Analisis terhadap indikator awal menunjukkan adanya beberapa indikator dengan fokus evaluasi yang beririsan atau merepresentasikan proses keamanan yang sama.

Konsolidasi dilakukan berdasarkan kesamaan fokus evaluasi, keterkaitan proses, serta potensi overlap dan double counting. Proses tersebut menghasilkan 27 indikator final tanpa menghilangkan keterlacakan terhadap Category dan hasil layered mapping yang menjadi dasar pembentukannya. Dengan demikian, konsolidasi tidak dimaksudkan untuk mengurangi cakupan evaluasi, tetapi untuk membentuk instrumen yang lebih efisien dan sesuai dengan konteks evaluasi SIPUHH.

Instrumen final mencakup enam Function NIST CSF 2.0, yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. Setiap indikator digunakan untuk mengarahkan proses pengumpulan informasi dan verifikasi bukti sehingga Current Profile tidak dibentuk berdasarkan persepsi semata, tetapi berdasarkan kondisi aktual yang dapat ditelusuri melalui bukti teknis maupun dokumenter. Hasil ini menunjukkan bahwa layered mapping dapat dioperasionalkan dari tingkat framework menjadi instrumen yang dapat digunakan dalam pelaksanaan assessment.

Hasil Assessment dan Analisis Gap

Penerapan 27 indikator menunjukkan bahwa kondisi keamanan SIPUHH memiliki tingkat kebutuhan peningkatan yang berbeda. Berdasarkan perbandingan antara Current Profile dan Target Profile, sebanyak 10 indikator berada pada prioritas Tinggi, 15 indikator pada prioritas Sedang, dan 2 indikator berada pada kategori Pemeliharaan. Distribusi hasil evaluasi disajikan pada Tabel 4.

Tabel 4. Distribusi Prioritas Hasil Evaluasi Keamanan SIPUHH

Prioritas	Jumlah Indikator	Persentase
Tinggi	10	37,0%
Sedang	15	55,6%
Pemeliharaan	2	7,4%
Total	27	100%

Berdasarkan Tabel 4, persentase setiap kategori prioritas dihitung berdasarkan jumlah indikator pada masing-masing kategori dibandingkan dengan total 27 indikator evaluasi. Hasil perhitungan menunjukkan bahwa 10 indikator prioritas Tinggi merepresentasikan 37,0% dari keseluruhan indikator, 15 indikator prioritas Sedang sebesar 55,6%, dan 2 indikator kategori Pemeliharaan sebesar 7,4%.

Sepuluh indikator prioritas tinggi menunjukkan area yang mekanisme keamanannya belum tersedia atau secara mendasar belum memadai. Kesenjangan tersebut terutama ditemukan pada dokumentasi proses bisnis, strategi dan tata kelola manajemen risiko keamanan, pembagian peran dan kewenangan keamanan, kebijakan keamanan informasi,

pengelolaan risiko pihak ketiga, penilaian risiko keamanan, pelatihan dan kesadaran keamanan, analisis dan klasifikasi kejadian keamanan, pengelolaan dan eskalasi insiden, serta perencanaan dan pelaksanaan pemulihan.

Sebanyak 15 indikator berada pada prioritas Sedang. Pada kelompok ini, mekanisme atau praktik yang relevan pada dasarnya telah tersedia, tetapi masih memerlukan penguatan pada aspek formalitas, dokumentasi, cakupan, atau konsistensi penerapan. Temuan tersebut antara lain berkaitan dengan struktur pengelolaan SIPUHH, tujuan dan ruang lingkup layanan, evaluasi keamanan, pengelolaan layanan eksternal dan interkoneksi, inventaris aset, pengelolaan identitas dan hak akses, hardening platform, perlindungan jaringan, monitoring, serta proses analisis, komunikasi, mitigasi, dan koordinasi terkait insiden maupun pemulihan.

Dua indikator berada pada kategori Pemeliharaan, yaitu regulasi penyelenggaraan SIPUHH dan perlindungan serta backup data. Kondisi utama pada kedua area tersebut telah tersedia dengan bukti yang memadai, sehingga kebutuhan berikutnya lebih diarahkan pada pemeliharaan dan pemantauan keberlanjutan penerapannya.

Tabel 5. Ringkasan Temuan Evaluasi per Function

Function	Temuan Evaluasi
Govern	Struktur dan regulasi penyelenggaraan SIPUHH telah tersedia, tetapi dokumentasi proses bisnis, tata kelola manajemen risiko, pembagian tanggung jawab keamanan, kebijakan keamanan informasi, serta pengelolaan risiko pihak ketiga masih memerlukan penguatan.
Identify	Inventaris aset teknologi telah tersedia, tetapi penilaian risiko keamanan belum dilakukan secara terstruktur dan proses evaluasi serta peningkatan keamanan masih perlu diperkuat.
Protect	Pengelolaan identitas dan hak akses, backup data, hardening server, firewall, dan mekanisme redundansi telah diterapkan, tetapi dokumentasi kontrol dan pelatihan kesadaran keamanan masih memerlukan penguatan.
Detect	Monitoring infrastruktur telah menggunakan Zabbix dan pengumpulan serta analisis log didukung Wazuh, tetapi cakupan monitoring serta mekanisme analisis dan klasifikasi kejadian keamanan masih perlu diperkuat.
Respond	Penanganan kejadian telah dilakukan secara operasional, tetapi pengelolaan, eskalasi, analisis, komunikasi, dan mitigasi insiden belum seluruhnya didukung proses respons insiden yang formal dan terstruktur.
Recover	Backup, pengujian pemulihan data, dan redundansi telah tersedia, tetapi perencanaan, pelaksanaan, komunikasi, dan koordinasi pemulihan layanan masih memerlukan penguatan.

Hasil pada Tabel 5 menunjukkan bahwa kesenjangan keamanan SIPUHH tidak tersebar secara seragam pada seluruh Function NIST CSF 2.0. Pada Function Govern, mekanisme dasar penyelenggaraan telah tersedia melalui struktur pengelolaan dan regulasi, tetapi aspek tata kelola keamanan masih memerlukan penguatan terutama pada dokumentasi proses bisnis, manajemen risiko, pembagian tanggung jawab keamanan, kebijakan keamanan informasi, serta pengelolaan risiko pihak ketiga. Pada Function Identify, inventaris aset telah tersedia, tetapi penilaian risiko keamanan belum dilakukan secara terstruktur sehingga proses identifikasi kebutuhan peningkatan keamanan belum sepenuhnya berbasis risiko.

Pada Function Protect, sejumlah kontrol teknis telah diterapkan melalui pengelolaan identitas dan hak akses, backup data, hardening server, firewall, dan mekanisme redundansi. Namun, penerapan tersebut masih memerlukan penguatan pada dokumentasi kontrol dan pelatihan kesadaran keamanan. Pada Function Detect, SIPUHH telah menggunakan Zabbix untuk monitoring infrastruktur serta Wazuh untuk mendukung pengumpulan dan analisis log, tetapi cakupan monitoring serta mekanisme analisis dan klasifikasi kejadian keamanan masih perlu diperkuat.

Pada Function Respond, penanganan kejadian telah dilakukan secara

operasional, tetapi belum seluruhnya didukung oleh proses formal yang mengatur pengelolaan, eskalasi, analisis, komunikasi, dan mitigasi insiden. Sementara itu, pada Function Recover, mekanisme backup, pengujian pemulihan data, dan redundansi telah tersedia, tetapi perencanaan, pelaksanaan, komunikasi, dan koordinasi pemulihan layanan masih memerlukan penguatan. Temuan pada enam Function tersebut menunjukkan bahwa kebutuhan utama peningkatan keamanan SIPUHH tidak hanya berkaitan dengan ketersediaan kontrol teknis, tetapi juga dengan penguatan tata kelola dan proses agar mekanisme keamanan yang telah diterapkan dapat dikelola, ditelusuri, dan dievaluasi secara konsisten.

Namun, hasil asesmen memperlihatkan perbedaan antara keberadaan kapabilitas teknis dan tingkat institusionalisasi proses keamanan. Sejumlah mekanisme yang telah berjalan belum seluruhnya didukung oleh kebijakan, prosedur, pembagian tanggung jawab, dokumentasi, dan proses evaluasi keamanan yang formal dan terstruktur. Kondisi tersebut menjelaskan mengapa sebagian besar indikator tetap berada pada prioritas Tinggi dan sedang meskipun berbagai kontrol teknis telah diterapkan. Dengan demikian, kebutuhan peningkatan keamanan SIPUHH tidak hanya terletak pada penambahan teknologi keamanan, tetapi juga pada penguatan tata kelola dan proses yang memastikan mekanisme teknis dikelola secara konsisten dan dapat dievaluasi.

Keterkaitan Temuan Berdasarkan Layered Mapping

Analisis terhadap hasil assessment menunjukkan bahwa gap pada suatu indikator tidak selalu berdiri sendiri. Keterlacakan horizontal memperlihatkan hubungan antartemuan pada indikator, Category, maupun Function yang berbeda. Tiga pola keterkaitan utama ditemukan, yaitu hubungan antara tata kelola, penilaian risiko, dan kontrol; hubungan Protect–Detect–Respond; serta hubungan Respond–Recover.

Pola pertama menunjukkan bahwa kelemahan tata kelola dan manajemen risiko memengaruhi proses identifikasi kebutuhan kontrol keamanan. Belum kuatnya strategi manajemen risiko, pembagian tanggung jawab keamanan, kebijakan keamanan informasi, dan penilaian risiko menyebabkan kebutuhan kontrol lebih banyak ditentukan berdasarkan kebutuhan operasional daripada proses pengelolaan risiko yang formal. Hal ini menunjukkan bahwa penguatan kontrol teknis perlu didukung oleh tata kelola dan penilaian risiko agar pemilihan serta evaluasi kontrol dapat dilakukan secara sistematis.

Pola kedua terlihat pada hubungan Protect–Detect–Respond. SIPUHH telah menerapkan sejumlah mekanisme perlindungan dan monitoring, tetapi hasil monitoring belum seluruhnya terhubung dengan mekanisme analisis, klasifikasi, eskalasi, dan penanganan insiden yang formal. Dengan demikian, keberadaan kontrol perlindungan dan perangkat monitoring belum secara otomatis membentuk siklus penanganan insiden yang utuh. Penguatan pada satu Function perlu mempertimbangkan ketergantungannya terhadap Function lain agar hasil monitoring dapat ditindaklanjuti secara konsisten.

Pola ketiga ditemukan pada hubungan Respond–Recover. Keterbatasan dalam pengelolaan dan eskalasi insiden berhubungan dengan kesiapan proses pemulihan layanan. Meskipun mekanisme backup, pengujian pemulihan data, dan redundansi telah tersedia, perencanaan pemulihan secara menyeluruh masih memerlukan penguatan. Temuan ini menunjukkan bahwa kemampuan pemulihan tidak hanya bergantung pada ketersediaan mekanisme teknis, tetapi juga pada proses respons, koordinasi, dan perencanaan yang mendukung pemulihan layanan setelah terjadi insiden.

Selain keterkaitan horizontal, layered mapping mempertahankan keterlacakan vertikal dari Category NIST CSF 2.0, perspektif pengelolaan COBIT 2019, control family NIST SP 800-53, indikator evaluasi, bukti, Current Profile, Target Profile, hingga gap dan prioritas peningkatan. Kombinasi kedua bentuk keterlacakan tersebut memungkinkan hasil evaluasi tidak hanya menunjukkan lokasi gap, tetapi juga menjelaskan konteks pengelolaan dan keterkaitan antartemuan yang mendasari kebutuhan peningkatan.

Program Peningkatan Keamanan SIPUHH

Keterkaitan antargap selanjutnya digunakan untuk mengonsolidasikan kebutuhan peningkatan yang memiliki fokus serupa. Konsolidasi dilakukan agar tindak lanjut tidak disusun secara terpisah untuk setiap indikator, tetapi dikelompokkan menjadi program yang dapat menangani beberapa gap yang saling berkaitan. Hasil konsolidasi menghasilkan enam program peningkatan keamanan SIPUHH sebagaimana disajikan pada Tabel 6.

Tabel 6. Program Peningkatan Keamanan SIPUHH

Program Peningkatan	Indikator Terkait	Fokus Peningkatan
Tata Kelola dan Manajemen Risiko Keamanan Informasi	GV.OC-01, GV.OC-02, GV.OC-04, GV.RM-01, GV.RR-01, GV.PO-01, GV.OV-01, ID.AM-01, ID.RA-01, ID.IM-01.	Tata kelola, tanggung jawab, kebijakan, pengelolaan aset, penilaian risiko, dan evaluasi keamanan
Penguatan Pengelolaan Risiko Pihak Ketiga dan Interkoneksi	GV.SC-01, GV.SC-02	Pihak ketiga, layanan eksternal, dan interkoneksi
Standardisasi dan Penguatan Kontrol Perlindungan	PR.AA-01, PR.AT-01, PR.PS-01, PR.IR-01	Identitas dan akses, awareness, hardening, dan perlindungan jaringan
Penguatan Monitoring dan Analisis Kejadian Keamanan	DE.CM-01, DE.AE-01	Monitoring, analisis, dan klasifikasi kejadian keamanan
Pembentukan Tata Kelola Respons Insiden	RS.MA-01, RS.AN-01, RS.CO-01, RS.MI-01	Pengelolaan, analisis, komunikasi, eskalasi, dan mitigasi insiden
Penguatan Ketahanan dan Pemulihan Layanan	PR.IR-02, RC.RP-01, RC.CO-01	Redundansi, perencanaan, koordinasi, dan pelaksanaan pemulihan

Tabel 6 menunjukkan bahwa 25 indikator yang masih memerlukan peningkatan dapat dikonsolidasikan menjadi enam program berdasarkan kesamaan fokus dan keterkaitan antargap. Keenam program tersebut terdiri atas Penguatan Tata Kelola dan Manajemen Risiko Keamanan Informasi, Penguatan Pengelolaan Risiko Pihak Ketiga dan Interkoneksi, Standardisasi dan Penguatan Kontrol Perlindungan, Penguatan Monitoring dan Analisis Kejadian Keamanan, Pembentukan Tata Kelola Respons Insiden, serta Penguatan Ketahanan dan Pemulihan Layanan. Konsolidasi ini menunjukkan bahwa satu program dapat menangani beberapa indikator secara bersamaan sehingga tindak lanjut tidak perlu dilakukan sebagai 25 tindakan yang berdiri sendiri.

Prioritas implementasi program ditentukan dengan mempertimbangkan tingkat gap dan keterkaitan antartemuan. Penguatan Tata Kelola dan Manajemen Risiko Keamanan Informasi ditempatkan sebagai prioritas awal karena mencakup indikator prioritas Tinggi pada dokumentasi proses bisnis, strategi manajemen risiko, pembagian tanggung jawab keamanan, kebijakan keamanan informasi, dan penilaian risiko serta menjadi dasar bagi pengelolaan program lainnya. Pengelolaan Risiko Pihak Ketiga dan Interkoneksi juga perlu diprioritaskan karena masih terdapat gap prioritas Tinggi pada pengelolaan risiko pihak ketiga dan keterkaitannya dengan layanan eksternal serta interkoneksi SIPUHH.

Pada aspek operasional keamanan, Penguatan Monitoring dan Analisis

Kejadian Keamanan serta Pembentukan Tata Kelola Respons Insiden perlu dilaksanakan secara berkesinambungan karena kemampuan monitoring menggunakan Zabbix dan Wazuh perlu dihubungkan dengan mekanisme analisis, klasifikasi, eskalasi, komunikasi, dan mitigasi insiden yang formal. Standardisasi dan Penguatan Kontrol Perlindungan dilakukan untuk memperkuat kontrol yang sebagian telah tersedia, termasuk pengelolaan akses, hardening, firewall, serta awareness keamanan. Selanjutnya, Penguatan Ketahanan dan Pemulihan Layanan diarahkan untuk memastikan mekanisme redundansi dan pemulihan teknis didukung oleh perencanaan, koordinasi, dan pelaksanaan pemulihan yang terstruktur.

Urutan tersebut tidak menunjukkan bahwa program dengan prioritas berikutnya dapat diabaikan, tetapi menggambarkan dependensi implementasi. Penguatan tata kelola dan manajemen risiko menjadi fondasi, kontrol perlindungan dan monitoring memperkuat kemampuan pencegahan serta deteksi, tata kelola respons memastikan kejadian dapat ditangani secara konsisten, sedangkan ketahanan dan pemulihan memastikan keberlangsungan layanan setelah insiden. Dengan pendekatan tersebut, enam program membentuk rangkaian peningkatan keamanan yang saling mendukung dari aspek governance hingga recovery.

Program pertama memiliki cakupan indikator paling luas karena gap tata kelola dan manajemen risiko berkaitan dengan berbagai proses keamanan lainnya. Program kedua diarahkan pada pengelolaan ketergantungan SIPUHH terhadap pihak ketiga dan interkoneksi. Program ketiga berfokus pada standardisasi kontrol perlindungan yang sebagian telah diterapkan secara teknis tetapi masih membutuhkan penguatan proses dan dokumentasi.

Program keempat dan kelima membentuk kesinambungan antara kemampuan monitoring dengan penanganan insiden. Monitoring dan pengumpulan log perlu didukung oleh mekanisme analisis dan klasifikasi kejadian serta prosedur pengelolaan, eskalasi, komunikasi, dan mitigasi insiden. Program keenam melengkapi rangkaian tersebut melalui penguatan ketahanan dan pemulihan layanan sehingga mekanisme redundansi dan pemulihan teknis didukung oleh perencanaan dan koordinasi pemulihan yang terstruktur.

Keenam program tersebut menunjukkan bahwa peningkatan keamanan SIPUHH tidak perlu diperlakukan sebagai 25 tindakan peningkatan yang berdiri sendiri. Layered mapping dan analisis keterkaitan memungkinkan gap yang saling berhubungan dikonsolidasikan menjadi program peningkatan yang lebih terstruktur. Dua indikator dalam kategori Pemeliharaan, yaitu GV.OC-03 dan PR.DS-01, tidak dimasukkan sebagai gap utama dalam program peningkatan karena kondisi utamanya telah terpenuhi, tetapi tetap memerlukan pemantauan untuk menjaga keberlanjutan penerapannya.

Penelitian ini memiliki keterbatasan pada tingkat granularitas pemetaan yang menggunakan Category NIST CSF 2.0 dan control family NIST SP 800-53 sehingga belum mencakup pemetaan hingga tingkat Subcategory dan kontrol individual. Proses layered mapping dilakukan melalui analisis konseptual berdasarkan kesesuaian keyword/theme, tujuan, ruang lingkup, dan alasan pemetaan tanpa melibatkan second reviewer atau pengujian inter-rater. Selain itu, hasil assessment merepresentasikan kondisi keamanan SIPUHH pada periode penelitian sehingga perubahan konfigurasi, kebijakan, maupun mekanisme keamanan setelah proses assessment dapat menghasilkan kondisi yang berbeda.

SIMPULAN

Penelitian ini menunjukkan bahwa layered mapping antara NIST CSF 2.0, COBIT 2019 APO13 – Managed Security,

dan NIST SP 800-53 dapat digunakan untuk membangun evaluasi keamanan SIPUHH yang terstruktur dan dapat ditelusuri. Pemetaan terhadap 22 Category NIST CSF 2.0 dioperasionalkan menjadi 37 indikator awal yang kemudian dikonsolidasikan menjadi 27 indikator final. Penerapan instrumen menunjukkan 10 indikator berada pada prioritas Tinggi, 15 indikator pada prioritas Sedang, dan 2 indikator pada kategori Pemeliharaan. Hasil tersebut menunjukkan bahwa SIPUHH telah memiliki sejumlah kapabilitas teknis dan operasional keamanan, tetapi belum seluruhnya didukung oleh tata kelola, kebijakan, prosedur, dokumentasi, dan proses evaluasi keamanan yang formal dan terstruktur. Analisis keterkaitan temuan menunjukkan bahwa gap pada aspek tata kelola dan manajemen risiko berkaitan dengan penerapan kontrol, sedangkan mekanisme Protect, Detect, Respond, dan Recover memerlukan keterhubungan proses agar membentuk pengelolaan keamanan yang berkesinambungan. Konsolidasi terhadap gap yang saling berkaitan menghasilkan enam program peningkatan keamanan SIPUHH. Kontribusi penelitian terletak pada penggunaan layered mapping yang tidak berhenti pada hubungan konseptual antar-framework, tetapi mempertahankan keterlacakan vertikal dari cybersecurity outcome, perspektif pengelolaan, referensi kontrol, indikator, hingga bukti dan hasil evaluasi, serta mendukung analisis horizontal terhadap keterkaitan antartemuan. Penelitian selanjutnya dapat memperluas pemetaan hingga tingkat Subcategory NIST CSF 2.0 dan kontrol individual NIST SP 800-53, melibatkan lebih dari satu penilai dalam proses pemetaan, serta melakukan evaluasi berkala setelah program peningkatan diterapkan untuk menilai perubahan kondisi dan perkembangan keamanan SIPUHH.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Kementerian Kehutanan Republik Indonesia atas izin dan dukungan yang diberikan sehingga Sistem Informasi Penatausahaan Hasil Hutan (SIPUHH) dapat digunakan sebagai objek dalam penelitian ini. Penulis juga menyampaikan terima kasih kepada pihak-pihak yang terlibat dalam pengelolaan dan pengembangan SIPUHH atas ketersediaan informasi dan bukti pendukung yang diperlukan dalam pelaksanaan evaluasi keamanan.

DAFTAR PUSTAKA

Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. Electronics, 14(7), 1364. https://doi.org/10.3390/electronics14071364

Fadila, V., Mutiah, N., & Sari, R. P. (2023). Cyber security audit using CIS CSC, NIST CSF and COBIT 2019 framework. CESS (Journal of Computer Engineering, System and Science), 8(2), 271–283. https://doi.org/10.24114/cess.v8i2.43257

Fadya, M., & Utama, D. N. (2025). Towards secure information systems: Developing and implementing an information security evaluation model using NIST CSF and COBIT 2019. TEM Journal, 14(1), 182–191. https://doi.org/10.18421/TEM141-17

Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of cybersecurity maturity assessment framework using NIST CSF v1.1 and CIS Controls v8. INOVTEK Polbeng - Seri Informatika, 9(1), 126–139. https://doi.org/10.35314/isi.v9i1.3973

ISACA. (2018a). COBIT 2019 framework: Governance and management objectives. ISACA.

ISACA. (2018b). COBIT 2019 framework: Introduction and methodology. ISACA.

Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Liu, M., Shore, M., Yeoh, W., Jiang, F., & Zeadally, S. (2025). Toward effective cybersecurity management: A hierarchical process model with performance assessment. Journal of Cybersecurity, 11(1), tyaf020. https://doi.org/10.1093/cybsec/tyaf020

Mussmann, A., Brunner, M., & Breu, R. (2020). Mapping the state of security standards mappings. Proceedings of the 15th International Conference on Wirtschaftsinformatik (WI 2020), 1309–1324. https://doi.org/10.30844/WI_2020_L4-MUSSMANN

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Rambau, T. M., Munyoka, W., Phahlamohlaka, L. J., & Kadyamatimba, A. (2026). Evaluating cyber resilience frameworks for e-government: Applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in developing country contexts. Information & Computer Security. https://doi.org/10.1108/ICS-09-2025-0376

Scarfone, K., Souppaya, M., & Fagan, M. (2024). Mapping relationships between documentary standards, regulations, frameworks, and guidelines: Developing cybersecurity and privacy concept mappings (NIST IR 8477). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8477

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). 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, 4(4), 225–230. https://doi.org/10.30630/joiv.4.4.482

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. International Journal of Communication Networks and Information Security, 12(3), 417–432. https://doi.org/10.17762/ijcnis.v12i3.4817

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. Electronics, 11(14), 2181. https://doi.org/10.3390/electronics11142181