Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 11, November 2025, Hal. 3288-3305
DOI: https://doi.org/10.52436/1.jpti.1124
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Pengembangan Instrumen Pengukuran Tingkat Kematangan Keamanan Siber untuk Instansi Pemerintah di Indonesia

Tiska Hardiana[*1], Suhardi[2]

[1,2]Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Indonesia
Email: [1]23223057@mahasiswa.itb.ac.id, [2]suhardi@itb.ac.id

Abstrak

Ancaman siber yang semakin kompleks menjadi tantangan krusial bagi instansi pemerintah di Indonesia. Namun, belum tersedianya instrumen evaluasi yang terstandar menghambat upaya pengukuran kapabilitas keamanan siber secara sistematis dan berkelanjutan. Menjawab kebutuhan tersebut, penelitian ini mengembangkan instrumen pengukuran tingkat kematangan keamanan siber yang komprehensif dan kontekstual bagi instansi pemerintah di Indonesia. Instrumen dirancang menggunakan pendekatan *Design Science Research Methodology* (DSRM), dengan mengintegrasikan kerangka kerja NIST *Cybersecurity Framework* (CSF) versi 2.0 dan regulasi nasional Perban BSSN Nomor 4 Tahun 2021. Penyusunan indikator didukung dengan pendekatan *Qualitative Content Analysis* (QCA) dan *Framework Alignment Matrix* (FAM), sedangkan skala kematangan mengacu pada prinsip *Capability Maturity Model* (CMM). Hasil utama dari penelitian ini berupa instrumen *self-assessment* yang mencakup enam domain penilaian, yaitu: Tata Kelola, Identifikasi, Proteksi, Deteksi, Penanggulangan, dan Pemulihan, yang dirinci menjadi 106 indikator berdasarkan hasil pemetaan. Validasi awal melalui simulasi pada salah satu instansi pemerintah menunjukkan nilai kematangan organisasi sebesar 3.90, yang berada pada Level 4 (Implementasi Terkelola). Evaluasi instrumen dilakukan menggunakan pendekatan *Framework for Evaluation in Design Science Research* (FEDS) untuk menilai kejelasan, kegunaan, dan kesesuaian hasil asesmen dengan kondisi aktual organisasi. Penelitian ini memberikan kontribusi praktis dan akademis melalui pengembangan alat ukur yang aplikatif bagi instansi pemerintah, sekaligus memperkaya pendekatan ilmiah dalam evaluasi kematangan keamanan siber berbasis regulasi nasional.

Kata kunci: *instrumen penilaian, kematangan keamanan siber*, *NIST CSF*, *Perban 4/2021, instansi pemerintah*, *self-assessment*

Development of a Cybersecurity Maturity Assessment Instrument for Government Institutions in Indonesia

Abstract

The growing complexity of cyber threats poses a critical challenge for government institutions in Indonesia. However, the absence of standardized evaluation instruments hinders systematic and sustainable measurement of cybersecurity capabilities. Addressing this need, this study develops a comprehensive and contextual cybersecurity maturity assessment instrument tailored for Indonesian government institutions. The instrument was designed using the Design Science Research Methodology (DSRM), integrating the NIST Cybersecurity Framework (CSF) version 2.0 with national regulations, specifically Perban BSSN Number 4 of 2021. The indicator development process was supported by Qualitative Content Analysis (QCA) and the Framework Alignment Matrix (FAM), while the maturity scale was based on the principles of the Capability Maturity Model (CMM). The main outcome of this research is a self-assessment instrument consisting of six key domains—Governance, Identification, Protection, Detection, Response, and Recovery—comprising 106 indicators derived from regulatory mapping. Initial validation through simulation at a government agency revealed an organizational maturity score of 3.90, corresponding to Level 4 (Managed Implementation). The instrument was further evaluated using the Framework for Evaluation in Design Science Research (FEDS) to assess its clarity, usability, and alignment with actual organizational conditions. This study offers both practical and academic contributions by developing an applicable assessment tool for government agencies, while also enriching scientific approaches to cybersecurity maturity evaluation grounded in national regulations.

Keywords: *assessment instrument, cybersecurity maturity, NIST CSF, Perban 4/2021, government institution, self-assessment*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

1. PENDAHULUAN

Keamanan siber merupakan isu krusial bagi berbagai organisasi, khususnya instansi pemerintah yang bertanggung jawab atas pengelolaan data strategis serta layanan publik berbasis digital. Perkembangan ancaman siber yang semakin kompleks menuntut penilaian kondisi keamanan secara rutin guna memastikan perlindungan informasi organisasi tetap optimal. Berdasarkan data Badan Siber dan Sandi Negara, tercatat sebanyak 330.527.636 trafik anomali di Indonesia pada tahun 2024, disertai dengan temuan *data exposure* yang berdampak luas terutama pada sektor administrasi pemerintahan. Kondisi ini menunjukkan bahwa sektor pemerintahan masih menjadi salah satu target utama serangan siber di Indonesia, sehingga diperlukan pendekatan sistematis untuk meningkatkan kapabilitas keamanan siber secara berkelanjutan [1]. Indonesia telah mengambil langkah strategis melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) yang ditegaskan dalam Peraturan Presiden Nomor 95 Tahun 2018. Peraturan ini secara khusus menekankan aspek keamanan sebagai bagian penting dalam implementasi SPBE, mencakup prinsip-prinsip seperti kerahasiaan, integritas, dan ketersediaan layanan pemerintahan berbasis digital [2]. Sebagai tindak lanjut teknis, BSSN telah mengeluarkan Peraturan Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis Keamanan SPBE yang selanjutnya disebut Perban 4/2021 [3]. Meski demikian, regulasi ini belum dilengkapi dengan instrumen yang baku dan terstandar untuk mengevaluasi tingkat kematangan keamanan siber secara spesifik dan terstruktur di tingkat instansi pemerintah. Padahal disisi lain, terdapat kewajiban kepatuhan terhadap regulasi dan pelaksanaan evaluasi untuk perbaikan berkelanjutan. Ketiadaan instrumen tersebut menimbulkan kesenjangan dalam melakukan validasi dan evaluasi terukur terhadap implementasi keamanan siber. Tujuan validasi dan evaluasi ini adalah untuk mengukur kondisi keamanan siber secara holistik dan komprehensif serta mengidentifikasi area-area yang memerlukan peningkatan dan memberikan rekomendasi dengan tujuan mengukur kematangan kondisi keamanan siber [4].

Dalam konteks mengukur kondisi kematangan keamanan siber, digunakan model pengukuran tingkat maturitas keamanan siber yang berfungsi sebagai alat kontrol dalam menilai serta mengidentifikasi celah kemungkinan perbaikan pada organisasi tertentu, dengan memberikan penilaian secara rinci tentang keadaan keamanan siber saat ini dan dibandingkan dengan kondisi keamanan siber secara ideal [5]. Pada konteks global, pendekatan evaluasi dengan model kematangan ini telah dikembangkan secara luas melalui berbagai model dan standar internasional, seperti *Capability Maturity Model* (CMM) dan *Capability Maturity Model Integration* (CMMI) yang menawarkan pendekatan bertahap dalam peningkatan proses organisasi [6], [7] serta *National Institute of Standards and Technology Cybersecurity Framework versi* 2.0 (NIST CSF v2.0) yang menghadirkan pendekatan lebih komprehensif dengan enam fungsi utama yaitu *Govern* (tata kelola), *Identify* (identifikasi), *Protect* (perlindungan), *Detect* (deteksi), *Respond* (penanggulangan), dan *Recover* (pemulihan) [8]. Keenam fungsi tersebut selaras dengan proses bisnis tugas dan fungsi BSSN selaku lembaga pemerintahan di bidang keamanan siber dan sandi dalam menyelenggarakan pemerintahan, yaitu tertuang pada Peraturan BSSN Nomor 6 Tahun 2021 [9].

Penelitian sebelumnya terkait model kematangan keamanan siber telah dikembangkan dalam berbagai konteks, namun belum sepenuhnya memenuhi kebutuhan spesifik sektor pemerintahan di Indonesia. Sebagai contoh, penelitian [10] yang merancang model kematangan keamanan siber untuk institusi pendidikan tinggi di Inggris, yang memiliki kerangka kebijakan, tingkat kematangan digital, serta struktur tata kelola yang berbeda dengan konteks instansi pemerintah Indonesia. Oleh karena itu, penerapannya secara langsung kurang relevan tanpa penyesuaian terhadap kerangka regulasi nasional dan kebutuhan sektoral di Indonesia. Penelitian lain juga menegaskan pentingnya pendekatan terintegrasi yang menggabungkan berbagai standar keamanan siber untuk menghasilkan evaluasi yang komprehensif dan adaptif terhadap kebutuhan organisasi [11], [12]. Namun, sebagian besar model tersebut lebih banyak dikembangkan untuk sektor swasta dan tidak secara spesifik mempertimbangkan peraturan nasional seperti Perban 4/2021, yang menjadi acuan utama dalam pengelolaan keamanan informasi instansi pemerintah di Indonesia. Untuk menjawab tantangan tersebut, penelitian ini bertujuan untuk merancang instrumen pengukuran tingkat kematangan keamanan siber yang komprehensif, sesuai dengan kebutuhan khusus instansi pemerintah di Indonesia. Instrumen ini dirancang berdasarkan pemetaan kerangka kerja NIST CSF v2.0 dengan persyaratan keamanan yang diatur dalam Perban 4/2021. Sebagai bagian dari pengembangan desain instrumen dalam penelitian ini, pemilihan dasar kriteria evaluasi, domain atau dimensi penilaian, level kematangan, metode penilaian dan metode pengaplikasian akan didasarkan pada sintesis hasil studi literatur. Metodologi yang digunakan adalah *Design Science Research Methodology* (DSRM), dengan pendekatan *Qualitattive Content Analysis* (QCA) serta *framework alignment matrix* berdasarkan yang akan memastikan kejelasan dan keterukuran setiap indikator dalam instrumen yang dikembangkan [13], [14]. Dengan demikian, tujuan utama dari penelitian ini adalah mengembangkan instrumen penilaian tingkat kematangan keamanan siber yang sesuai dengan kebutuhan instansi pemerintah di Indonesia, berdasarkan standar internasional dan ketentuan regulasi nasional.

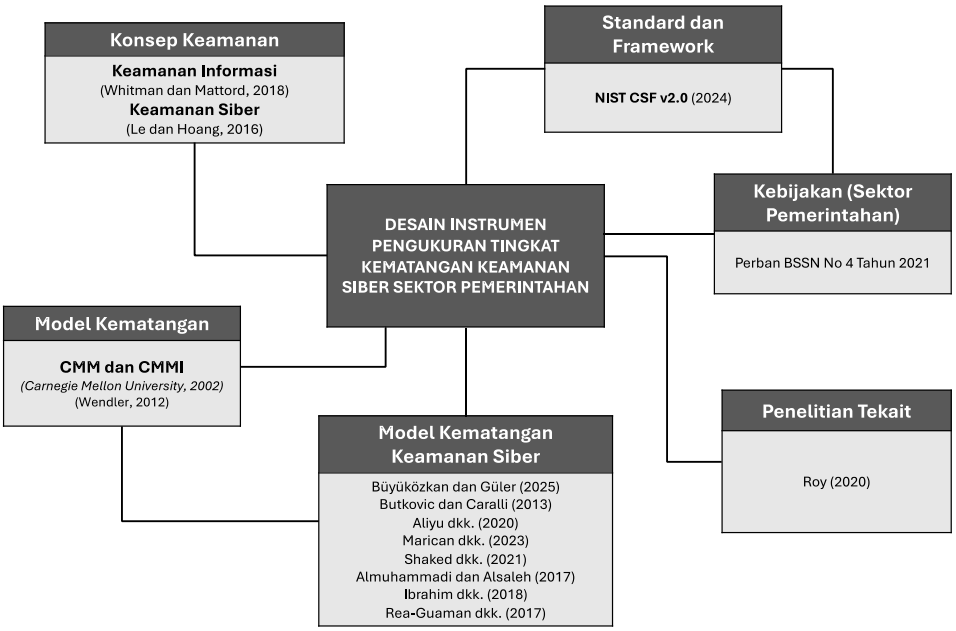
p-ISSN: 2775-4227
e-ISSN: 2775-4219

2. STUDI LITERATUR DAN PENELITIAN TERKAIT

Pengembangan instrumen pengukuran tingkat kematangan keamanan siber yang dilakukan dalam penelitian ini didasarkan pada sintesis berbagai referensi yang relevan dan telah dipetakan secara sistematis sebagaimana disajikan pada Gambar 1. Kajian literatur yang menjadi landasan penelitian ini diawali dengan penguatan konsep dasar keamanan informasi dan keamanan siber. Dimana penegaskan keamanan informasi bertujuan melindungi aset organisasi dari ancaman, dengan fokus pada aspek kerahasiaan, integritas, dan ketersediaan (CIA *triad*) [15]. Sedangkan keamanan siber memiliki cakupan yang lebih luas karena mencakup perlindungan seluruh aset digital dan lingkungan siber dari ancaman yang terus berkembang [5]. Selanjutnya, sebagai rujukan kerangka kerja dan standar internasional, penelitian ini mengadopsi NIST *Cybersecurity Framework* (CSF) versi 2.0, yang memberikan kerangka kerja komprehensif untuk mengelola risiko keamanan siber dengan enam fungsi utama, yaitu *Govern, Identify, Protect, Detect, Respond, dan Recover* [8]. Dalam konteks kebijakan nasional, referensi utama yang menjadi dasar instrumen adalah Perban 4/2021. Peraturan ini mengatur secara rinci tata kelola keamanan informasi dan standar teknis keamanan yang harus dipatuhi oleh instansi pemerintahan dalam implementasi SPBE [3].

Untuk mengembangkan model kematangan yang relevan, penelitian ini juga mengadopsi prinsip dari *Capability Maturity Model* (CMM) dan *Capability Maturity Model Integration* (CMMI) yang telah banyak digunakan sebagai acuan dalam pengembangan model kematangan proses organisasi. Model ini menyediakan pendekatan bertahap dan terstruktur yang menjadi dasar dalam merancang level kematangan yang diadopsi dalam penelitian ini, yaitu level 1 implementasi awal; level 2 implementasi berulang, level 3 implementasi terdefinisi, level 4 implementasi terkelola; dan level 5 implementasi optimal [6], [16]. Selain itu dalam mendesain intrumen tersebut, pada penelitian ini juga melakukan sisntesis konsep *framework maturity assessment model* dengan empat fase utama yang diadopsi, yaitu *scope, design, populate,* dan *test* [17].

Lebih lanjut, penelitian ini juga didukung oleh kajian sistematis terhadap berbagai model kematangan keamanan siber yang telah dikembangkan sebelumnya. Studi literatur yang dilakukan memberikan pemetaan menyeluruh terhadap tren, dimensi, level, metode penilaian, dan aplikasi model kematangan keamanan siber yang telah diterapkan di berbagai sektor, termasuk pemerintah, infrastruktur kritikal, dan sektor industri [18]. Studi lainnya yaitu [19], [20], [21], [22], [23], [24] menjadi referensi dalam merancang aspek dimensi dan indikator yang sesuai dengan konteks pemerintahan Indonesia, serta studi-studi penelitian terkait tersebut juga mengkaji model penilaian kematangan keamanan siber dalam berbagai sektor.



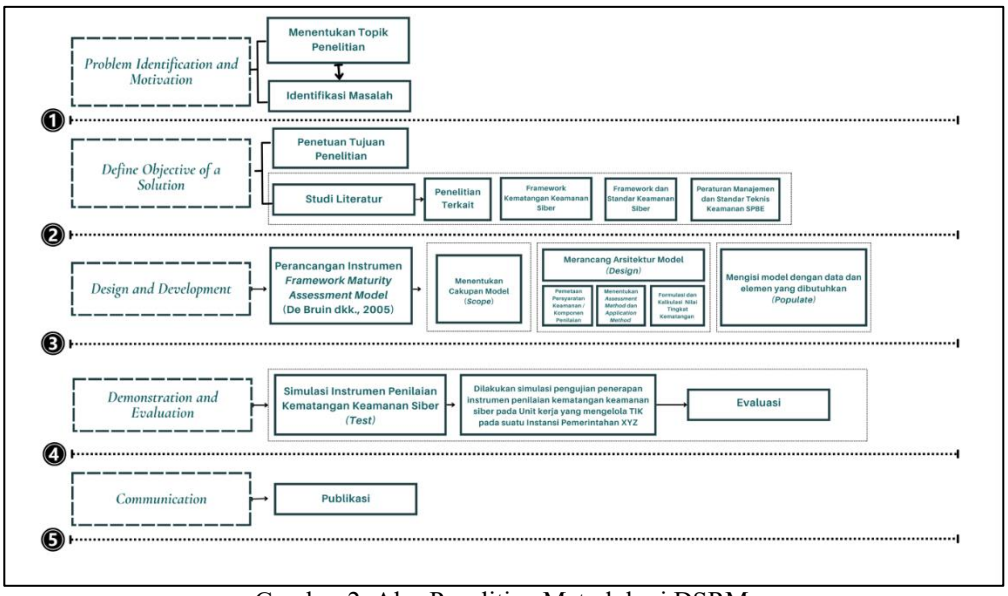
Gambar 1. Peta Literatur

3. METODE PENELITIAN

Design Science Reseacrh Methodology (DSRM) menjadi metodologi penelitian yang dipilih untuk digunakan pada penelitian ini dan dijadikan sebagai panduan penelitian dalam mendesain instrumen pengukuran

p-ISSN: 2775-4227
e-ISSN: 2775-4219

tingkat kematangan keamanan siber pada instansi pemerintahan. DSRM merupakan metodologi yang dapat digunakan sebagai suatu kerangka yang mempermudah penelitian dengan mengenali dan mengevaluasi hasil penelitian. Terdapat enam tahapan pada DSRM yaitu identifikasi masalah dan motivasi, mendefinisikan tujuan dari solusi permasalahan, perancangan dan pengembangan, demonstrasi, evaluasi, dan komunikasi [13]. Pada proses penelitian dilakukan penyelarasan dari alur DSRM agar penelitian dilakukan secara terstruktur, terukur, dan terencana. Skema penyelarasan tersebut digambarkan secara visual dalam Gambar 2, yang menunjukkan tahapan metode penelitian berdasarkan DSRM secara terstruktur dan iteratif.



Gambar 2. Alur Penelitian Metodologi DSRM

3.1. Identifikasi Masalah dan Motivasi

Problem identification and motivation adalah langkah pertama dalam proses DSRM yang bertujuan untuk mendefinisikan masalah penelitian dan memberikan justifikasi nilai dari solusi yang diharapkan. Dalam tahap ini melakukan identifikasi dan gambaran masalah yang relevan, signifikan, dan belum terpecahkan dalam konteks tertentu. Kemudian menentukan motivasi dan urgensi untuk menyelesaikan masalah tersebut, baik dari sudut pandang praktis maupun akademis. Permasalahan utama dalam penelitian ini adalah belum tersedianya instrumen evaluasi kematangan keamanan siber yang sesuai dengan kebutuhan khusus instansi pemerintah di Indonesia dan regulasi nasional, khususnya Perban 4/2021. Hal ini mendorong perlunya pengembangan instrumen yang sistematis untuk evaluasi mandiri. Dengan mengidentifikasi kebutuhan nyata akan alat ukur ini dan urgensi akan pentingnya tata kelola keamanan informasi di instansi pemerintahan, penelitian ini berupaya menjawab gap yang ada melalui pendekatan desain berbasis kebutuhan *(problem-centered initiation)* sebagaimana ditekankan dalam tahapan awal DSRM.

3.2. Definisi Tujuan dari Solusi Permasalahan

Tahapan kedua dalam metodologi DSRM difokuskan pada penentuan karakteristik dan tujuan dari solusi yang akan dikembangkan berdasarkan turunan dari hasil identifikasi masalah pada tahapan sebelumnya. Dalam penelitian ini, penetapan tujuan solusi didasarkan pada analisis kebutuhan regulatif, studi literatur akademik, serta *best practice* dari kerangka kerja keamanan siber. Tujuan dari solusi yang dikembangkan adalah menghasilkan rancangan desain instrumen pengukuran tingkat kematangan keamanan siber yang dapat digunakan oleh instansi pemerintah untuk melakukan evaluasi mandiri *(self-assessment);* merepresentasikan kondisi aktual kapabilitas keamanan siber organisasi pemerintahan; dan menyediakan skema level kematangan yang dapat dikuantifikasi. Serta menyelaraskan instrumen dengan peraturan nasional dan referensi internasional, melalui Perban 4/2021 dan integrasi domain dan kategori dari NIST CSF versi 2.0 sebagai struktur utama dari dimensi pengukuran.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3.3. Perancangan dan Pengembangan

Tahap perancangan dan pengembangan merupakan inti dari proses desain artefak dalam metodologi Design Science Research (DSRM), di mana rancangan instrumen disusun secara sistematis berdasarkan hasil identifikasi kebutuhan dan tujuan solusi yang telah ditetapkan pada tahap sebelumnya. Tujuan dari tahap ini adalah menghasilkan instrumen pengukuran yang tidak hanya sahih secara konseptual, tetapi juga dapat diimplementasikan secara praktis oleh instansi pemerintah di Indonesia. Pengembangan instrumen ini dilakukan melalui adaptasi dari kerangka *Framework Maturity Assessment Model* [17], dengan fokus pada tiga proses utama yaitu: penentuan cakupan (*scope*), perancangan struktur konseptual (*design*), dan pengisian elemen aktual ke dalam instrumen (*populate*). Masing-masing proses ini dirancang untuk menjawab pertanyaan penting terkait apa yang akan diukur, bagaimana strukturnya dibangun, dan bagaimana instrumen tersebut akan digunakan dalam praktik.

Pada tahap *scope*, peneliti menetapkan target pengguna instrumen, batasan konteks penggunaannya, serta kerangka kerja yang dijadikan acuan penilaian, yaitu NIST CSF v2.0 dan Perban BSSN Nomor 4 Tahun 2021. Selanjutnya, tahap *design* difokuskan pada penyusunan arsitektur yang mencakup domain, indikator, metode penilaian, serta skema kematangan yang menjadi arsitektur dasar instrumen evaluasi. Tahap *populate* kemudian dilakukan untuk mengisi instrumen dengan konten aktual, termasuk indikator yang telah dipetakan, skala penilaian numerik, serta panduan asesmen mandiri yang dapat digunakan oleh organisasi pemerintah dalam pelaksanaan evaluasi secara praktis. Untuk memberikan gambaran yang lebih ringkas dan sistematis, Tabel 1 di bawah ini menyajikan ringkasan dari ketiga proses tersebut, meliputi aktivitas utama, komponen yang disiapkan, serta hasil konkret yang dihasilkan dari setiap tahap.

Tabel 1. Tahapan Pengembangan Instrumen Pengukuran Kematangan Keamanan Siber

Tahap Desain	Aktivitas Utama	Komponen yang Disiapkan	Hasil/Keluaran
Scope	Menentukan ruang lingkup pengguna dan tujuan instrumen	- Sasaran: instansi pemerintah di Indonesia - Acuan: NIST CSF v2.0 dan Perban BSSN No. 4 Tahun 2021	Kerangka kerja evaluasi berbasis regulasi nasional dan standar global
Design	Merancang arsitektur model	- Domain, kategori, dan subkategori penilaian (berdasarkan hasil pemetaan persyaratan keamanan) - Skala penilaian dan level kematangan - Metode asesmen dan kalkulasi skor	Arsitektur instrumen evaluasi yang terdiri dari 6 domain utama dan skema penilaian terstruktur
Populate	Menyusun isi instrumen dengan indikator aktual dan narasi penilaian	- 106 indikator hasil pemetaan NIST CSF dan Perban 4/2021 - Format kuesioner evaluatif (self-assessment)	Instrumen siap digunakan dalam format spreadsheet, lengkap dengan dashboard penilaian

3.4. Demonstrasi dan Evaluasi

Tahapan demonstrasi ini mewaikili tahap *test* pada *Framework Maturity Assessment Model*. Demonstrasi dilakukan dengan simulasi penilaian disertai validasi menggunakan hasil desain instrumen penilaian tingkat kematangan keamanan siber yang telah dibuat, pada unit kerja yang bertanggung jawab terhadap pengelolaan keamanan informasi pada Instansi XYZ. Tujuan demonstrasi ini untuk menguji bahwa instrumen dapat diimplementasikan dengan efektif oleh organisasi pemerintahan yang menjadi sasaran, sesuai dengan konteks dan karakteristiknya. Selain itu, juga dilakukan evaluasi dengan pendekatan *formative evaluation* berdasarkan *Framework for Evaluation in Design Science Research* (FEDS) untuk mengumpulkan umpan terhadap fungsi praktis artefak melalui proses simulasi yang telah dilakukan sebelumnya [25].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3.5. Komunikasi

Tahapan terakhir dalam metode penelitian ini adalah tahap komunikasi. Tahapan ini bertujuan untuk membagikan hasil penelitian yang baru dan mendapatkan umpan balik. Selain itu diharapkan bahwa penelitian ini tidak hanya bermanfaat bagi lingkup akademis, tetapi juga memberikan dampak positif dan sesuai untuk masyarakat luas dan pihak-pihak yang terkait. Tahap komunikasi dilakukan dengan melakukan publikasi hasil penelitian pada jurnal.

4. HASIL PERANCANGAN DAN PENGEMBANGAN

Bagian ini menyajikan hasil utama dari proses penelitian yang telah dilakukan, berupa perancangan dan pengembangan instrumen pengukuran tingkat kematangan keamanan siber yang disesuaikan secara khusus untuk instansi pemerintah di Indonesia. Instrumen ini dibangun sebagai artefak dalam kerangka DSRM, melalui pendekatan yang terstruktur dan berbasis pada kebutuhan praktis serta regulatif. Proses pengembangannya melibatkan sintesis antara kerangka kerja NIST CSF v2.0 sebagai standar internasional, dan Peraturan BSSN Nomor 4 Tahun 2021 sebagai rujukan regulasi nasional.

Pembahasan dalam bab ini disusun berdasarkan tahapan desain yang dilakukan secara iteratif mulai dari penetapan cakupan model (*scope*), perancangan arsitektur model (*design*), pemetaan dan pengisian elemen indikator (*populate*), hingga proses pengujian awal melalui demonstrasi dan evaluasi (*test*). Setiap tahap dibahas secara mendalam, termasuk rasionalitas desain, hasil implementasi, serta analisis terhadap efektivitas dan kepraktisan instrumen yang dikembangkan. Penjabaran ini ditujukan untuk menunjukkan kontribusi nyata artefak terhadap peningkatan kapabilitas evaluasi keamanan siber di lingkungan instansi pemerintahan.

4.1. Ruang Lingkup dan Kodifikasi

Tahap awal pengembangan instrumen difokuskan pada penetapan ruang lingkup evaluasi dan kodifikasi elemen-elemen yang menjadi dasar desain model. Ruang lingkup pengguna dibatasi pada instansi pemerintahan di Indonesia, dengan fokus pada unit kerja yang mengelola keamanan informasi, TIK, atau SPBE. Evaluasi diarahkan pada aspek kapabilitas keamanan siber organisasi secara menyeluruh, bukan sekadar kepatuhan administratif. Selanjutmya, NIST CSF versi 2.0 digunakan sebagai referensi utama dalam menyusun struktur domain dan indikator dalam instrumen penilaian. *Framework* ini terdiri atas enam fungsi utama yaitu Tata Kelola (GV), Identifikasi (ID), Proteksi (PR), Deteksi (DE), Penanggulangan (RS), dan Pemulihan (RC) yang masing-masing dijabarkan ke dalam kategori dan subkategori teknis yang dapat dievaluasi. Hasil ekstraksi dari *framework* ini menghasilkan 22 kategori yang diturunkan lagi menjadi 106 subkategori pengendalian keamanan siber, yang kemudian dikodifikasi menjadi daftar indeks penilaian. Skema ini merujuk langsung pada penjelasan kerangka NIST CSF v2.0. Skema penomoran ini memberikan struktur yang mendukung penyusunan indikator dan memperjelas posisi tiap kontrol dalam struktur fungsi NIST [8]. Daftar kategori dan gambaran kodifikasi pada NIST CSF v2.0 dapat dilihat pada Tabel 2 dan Tabel 3.

Tabel 2. Kategori Persyaratan Keamanan NIST CSF v2.0

Fungsi	Kategori	Indeks Kodifikasi Subkategori
Tata Kelola (GV)	Konteks Organisasi (OC)	A.1-A.5
	Manajemen Risiko (RM)	A.6-A.12
	Peran, Tanggung Jawab dan Wewenang (RR)	A.13-A.16
	Kebijakan dan Prosedur (PO)	A.17-A.18
	Pengawasan (OV)	A.19-A.21
	Manajemen Risiko *Supply Chain*/Pihak Ketiga (SC)	A.22-A.31
Identifikasi (ID)	Manajemen Aset (AM)	A.32-A.38
	Penilaian Risiko (RA)	A.39-A.48
	Peningkatan (IM)	A.49-A.52
Proteksi (PR)	Manajemen Identitas, Otentikasi, dan Kontrol Akses (AA)	A.53-A.58
	Kesadaran dan Pelatihan (AT)	A.59-A.60
	Keamanan Data (DS)	A.61-A.64
	Keamanan Platform (PS)	A.65-A.70
	Ketahanan Infrastruktur Teknologi (IR)	A.71-A.74
Deteksi (DE)	Pemantauan Berkelanjutan (CM)	A.75-A.79
	Analisis Anomali dan Kejadian (AE)	A.80-A.85

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Fungsi	Kategori	Indeks Kodifikasi Subkategori
Penanggulangan (RS)	Manajemen Insiden (MA)	A.86-A90
	Analisis Insiden (AN)	A.91-A.94
	Pelaporan dan Komunikasi Respons Insiden (CO)	A.95-A.96
	Mitigasi Insiden (MI)	A.97-A.98
Pemulihan (RC)	Pelaksanaan Rencana Pemulihan Insiden (RP)	A.99-A.104
	Komunikasi Pemulihan Insiden (CR)	A.105-A.106

Tabel 3. Gambaran Kodifikasi Komponen Penilaian NIST CSF v2.0

Kode	Komponen Penilaian	Index
GV.OC-01	Misi organisasi dipahami dan menginformasikan manajemen risiko siber.	A.1
ID.AM-01	Inventaris perangkat keras yang dikelola organisasi dipertahankan dan diperbarui.	A.32
PR.AA-01	Identitas dan kredensial pengguna, layanan, dan perangkat yang sah dikelola oleh organisasi.	A.53
DE.CM-01	Jaringan dan layanan jaringan dipantau untuk mendeteksi potensi kejadian yang merugikan.	A.75
RS.MA-01	Rencana respons insiden dijalankan dengan koordinasi pihak internal dan eksternal yang relevan saat insiden dikonfirmasi.	A.86
RC.RP-01	Rencana pemulihan insiden dijalankan setelah aktivasi dari proses respons insiden.	A.99

Seluruh komponen yang diekstraksi dan dikodifikasi dari NIST CSF v2.0 digunakan sebagai landasan pemetaan terhadap regulasi nasional, serta sebagai elemen utama dalam penyusunan indikator evaluatif pada instrumen. Proses kodifikasi ini menghasilkan struktur yang konsisten, sistematis, dan kompatibel untuk integrasi dengan Perban 4/2021. Perban 4/2021 juga diekstraksi dan dikodifikasi untuk mempermudah dan proses pemetaan. Regulasi ini terdiri atas 4 bab dan 36 pasal dengan dua fokus aspek utama, yaitu yang pertama aspek pedoman manajemen keamanan informasi yang mencakup enam proses mulai dari penetapan ruang lingkup hingga perbaikan berkelanjutan. Yang kedua terkait standar teknis dan prosedur keamanan, yang mengatur keamanan pada lima area kritikal mulai dari data dan informasi hingga pusat data nasional. Hasil uraian persyaratan keamanan dari Perban 4/2021 diterjemahkan dari 11 aspek menjadi 66 komponen penilaian yang kemudian dikodifikasi dan direpresentasikan dalam indeks "B" (misalnya B.1, B.4, B.7) yang masing-masing merepresentasikan aktivitas evaluatif spesifik. Gambaran kodifikasi Perban 4/2021 dapat dilihat pada Tabel 4.

Tabel 4. Gambaran Kodifikasi Komponen Penilaian Perban 4/2021

Kode	Komponen Penilaian	Index
Aktivitas 1.1	Definisi isu internal	B.1
Aktivitas 2.1	Koordinator SPBE	B.4
Aktivitas 3.1.1	Edukasi Kesadaran	B.7
Aktivitas 3.1.4	Penanganan Insiden	B.10
Aktivitas 7.1	Aspek Kerahasiaan	B.23

4.2. Rancangan Arsitektur Model

4.2.1 Pemetaan Persyaratan Keamanan

Pemetaan antara NIST CSF v2.0 dan Perban 4/2021 dilakukan dengan pendekatan *Qualitative Content Analysis* (QCA) untuk menginterpretasi makna dan konteks regulatif secara sistematis. Setiap komponen penilaian pada NIST CSF v2.0 diperlakukan sebagai *unit of analysis* dan dikodekan untuk dibandingkan dengan komponen penilaian dari Perban BSSN 4/2021 melalui proses *coding*. Untuk meningkatkan akurasi dan konsistensi pemetaan, digunakan *Framework Alignment Matrix* (FAM) sebagai alat bantu visual [14]. Pemetaan ini bersifat non-linear, artinya satu komponen penilaian dapat memiliki lebih dari satu padanan, berdasarkan kesetaraan makna, fungsi, atau tujuan. Tingkat kesesuaian diklasifikasikan ke dalam tiga kategori, yaitu:

a) *Direct Match* (Langsung): kesesuaian penuh dalam konteks, tujuan, dan cakupan.
b) *Partial Match* (Sebagian): terdapat irisan makna namun tidak sepenuhnya sepadan.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

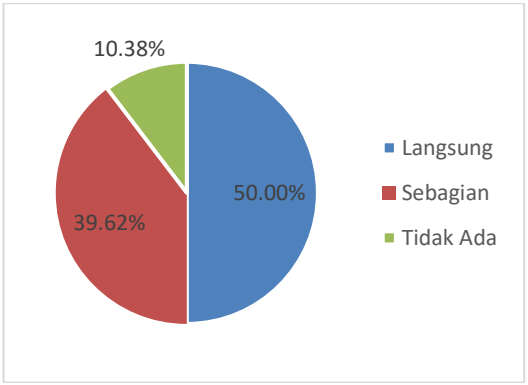
c) *No Match* (Tidak ada): tidak ditemukan padanan relevan.

Tabel 5 menggambarkan contoh hasil pemetaan antara index komponen dari NIST CSF v2.0 dan Perban 4/2021, dengan kolom tingkat kesesuaian dan justifikasi analisis. Secara keseluruhan, pemetaan mencakup 106 komponen dari NIST CSF v2.0 yang dianalisis terhadap 66 komponen dari Perban BSSN 4/2021, kemudian dituangkan dalam *alignment matrix*. Total 336 relasi identifikasi dipetakan untuk mendukung desain indikator yang bersifat kontekstual, evaluatif, dan kompatibel secara regulatif

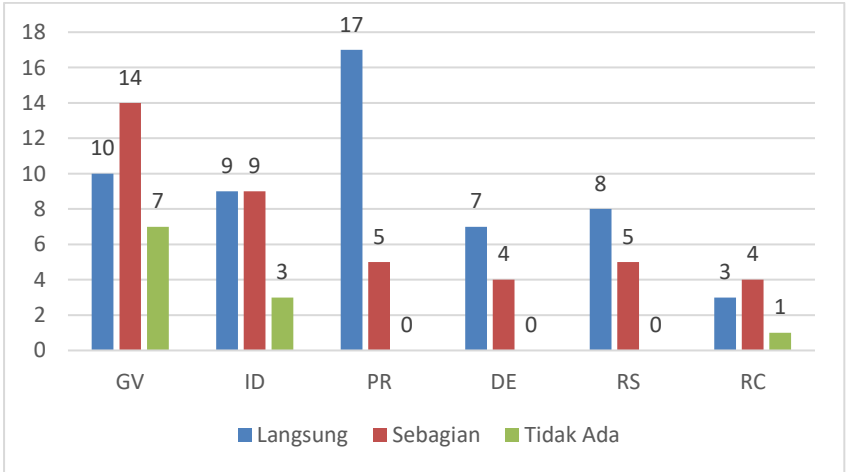
Tabel 5. Pemetaan Komponen Penilaian

No	Index (A)	Index (B)	Tingkat Kesesuaian	Justifikasi
1	A.1	B.1, B.3	Sebagian	Pemahaman misi organisasi pada A.1 sebagian tercermin melalui isu internal (B.1) dan area prioritas (B.3) sebagai proksi.
3	A.11	B.8	Langsung	Strategi manajemen risiko pada A.11 sepadan dengan mekanisme penilaian risiko SPBE pada B.8.
4	A.47	B.24	Langsung	Penilaian keaslian dan integritas perangkat pada A.47 setara dengan verifikasi data pada B.24.
5	A.48	–	Tidak Ada	Tidak ada padanan eksplisit terkait vendor assessment pada Perban BSSN.

Berdasarkan hasil pemetaan, sebanyak 53 subkategori atau 50% terpetakan dengan kategori kesesuaian Langsung atau *Direct Match*, kemudian sebanyak 42 subkategori atau 39,62% terpetakan dengan kategori kesesuaian Sebagian atau *Partial Match,* dan sisanya yaitu 11 subkategori atau 10,38% belum terpetakan karena belum diatur dalam Perban BSSN 4/2021. Visualisasi hasil analisis tingkat keseuaian pemetaannya dapat dilihat pada Gambar 3 dan Visualisasi distribusi pemetaan untuk setiap fungsi dapat dilihat pada Gambar 4.



Gambar 3. Hasil Pemetaan Persyaratan Keamanan Index A ke Index B



Gambar 4. Distribusi Hasil Pemetaan Persyaratan Keamanan pada Setiap Fungsi

p-ISSN: 2775-4227
e-ISSN: 2775-4219

4.2.2 Penyusunan Metode Penilaian dan Pengaplikasian

Metode penilaian yang digunakan adalah *self-assessment* berbasis kuesioner evaluatif, yang disusun berdasarkan hasil pemetaan antara NIST CSF v2.0 dan Perban 4/2021. Pertanyaan dalam instrumen dikembangkan melalui sintesis hasil pemetaan dan analisis kesenjangan (*gap*), guna memastikan seluruh aspek keamanan yang relevan tetap terakomodasi. Setiap pertanyaan dirancang menggunakan pendekatan audit untuk mengevaluasi keberadaan, implementasi, dan efektivitas kebijakan atau prosedur keamanan. Pengaplikasian dilakukan melalui format pertanyaan eksploratif dengan skala jawaban bertingkat yang merepresentasikan fase kematangan implementasi. Skala jawaban disusun dengan mengacu pada prinsip *maturity model* yang mengadaptasi tingkat kematangan berbasis CMM, kemudian diadopsi ke dalam empat tingkat pengukuran implementasi proses yang bersifat praktis, mudah dipahami, dan aplikatif bagi organisasi. Skala jawaban yang digunakan dalam instrumen ini terdiri dari empat pilihan, yaitu:

1. Tidak Diterapkan, skala ini secara umum menunjukkan bahwa proses keamanan siber tidak dijalankan sama sekali, tidak ada dokumentasi maupun inisiatif yang dilakukan.
2. Perencanaan, skala ini secara umum memperlihatkan bahwa proses keamanan siber sedang dalam tahap perencanaan atau perancangan awal, namun belum ada implementasi aktual.
3. Parsial, skala ini secara umum menunjukkan proses telah dijalankan sebagian namun belum konsisten, belum menyeluruh, atau belum terdokumentasi dengan baik.
4. Menyeluruh, skala ini menunjukkan proses telah diimplementasikan secara komprehensif, terdokumentasi, dan menjadi bagian dari prosedur standar organisasi. mulai dari tidak diterapkan hingga menyeluruh. Pertanyaan-pertanyaan dikelompokkan ke dalam enam domain utama. Struktur dan elemen utama dari instrumen penilaian ditampilkan dalam Tabel 6.

Tabel 6. Struktur Instrumen Peilaian Keamanan Siber Sektor Pemerintahan

No	Kategori	Pertanyaan Penilaian	Petunjuk Penilaian	Dukungan Bukti Objektif
1	Tata Kelola: Konteks Organisasi	Apakah organisasi telah mendokumentasikan dan menggunakan pemahaman tentang misi, tujuan strategis, pemangku kepentingan, serta aktivitas utamanya untuk mendukung pengelolaan risiko siber?	- Tidak Diterapkan: Tidak ada dokumentasi atau keterkaitan dengan pengelolaan risiko siber - Perencanaan: Pemahaman tersedia namun belum terintegrasi - Parsial: Terkait sebagian fungsi dan belum digunakan aktif - Menyeluruh: Terdokumentasi lengkap dan digunakan sebagai dasar dalam perencanaan risiko	Dokumen Renstra, visi–misi, peta proses bisnis, bukti integrasi ke manajemen risiko
2	Identifikasi: Identifikasi Aset/Manajemen Aset	Apakah organisasi telah mengklasifikasikan aset berdasarkan tingkat sensitivitas, dampak terhadap layanan publik, dan peran strategis dalam operasional instansi?	- Tidak Diterapkan: Tidak ada klasifikasi aset - Perencanaan: Klasifikasi sedang dirancang - Parsial: Sebagian aset sudah diklasifikasikan - Menyeluruh: Seluruh aset diklasifikasikan dan digunakan dalam manajemen risiko	Dokumen klasifikasi, peta aset kritikal, risk register berbasis aset
3	Proteksi: Kesadaran dan Pelatihan	Apakah organisasi memberikan pelatihan dan kesadaran keamanan siber kepada seluruh pegawai, termasuk non-TIK, untuk mendukung pelaksanaan tugas umum secara aman?	- Tidak Diterapkan: Tidak ada pelatihan atau sosialisasi - Perencanaan: Pelatihan dirancang namun belum dilaksanakan - Parsial: Pelatihan dilakukan terbatas untuk unit tertentu - Menyeluruh: Terdapat program pelatihan berkala untuk seluruh personel	Materi/jadwal pelatihan, daftar hadir, dokumentasi *e-learning*
4	Deteksi: Monitoring	Apakah organisasi melakukan pemantauan terhadap lalu lintas jaringan dan layanan	- Tidak Diterapkan: Tidak ada pemantauan jaringan - Perencanaan: Rencana monitoring sedang disusun	Laporan IDS/IPS, *log firewall*, konfigurasi

p-ISSN: 2775-4227
e-ISSN: 2775-4219

No	Kategori	Pertanyaan Penilaian	Petunjuk Penilaian	Dukungan Bukti Objektif
		kritikal secara rutin untuk mendeteksi potensi anomali, serangan, atau penyalahgunaan?	- Parsial: Hanya jaringan tertentu yang dimonitor - Menyeluruh: Seluruh layanan/jaringan dipantau dengan sistem deteksi terintegrasi	NMS, *alert system monitoring*
5	Penanggulangan: Manajemen Insiden	Apakah organisasi memiliki prosedur dan mekanisme yang menjamin koordinasi yang terorganisir antar unit terkait saat pelaksanaan respons insiden?	- Tidak Diterapkan: Tidak ada mekanisme koordinasi - Perencanaan: Mekanisme sedang disusun - Parsial: Koordinasi dilakukan ad hoc - Menyeluruh: Koordinasi dilakukan terstruktur sesuai prosedur yang terdokumentasi	SOP respons insiden, notulensi, *log* komunikasi antar unit
6	Perencanaan Pemulihan	Apakah organisasi mengintegrasikan fungsi bisnis kritis dan strategi manajemen risiko ke dalam rencana pemulihan?	- Tidak Diterapkan: Tidak ada integrasi - Perencanaan: Integrasi sedang dirancang - Parsial: Integrasi dilakukan sebagian atau tidak terdokumentasi - Menyeluruh: Rencana pemulihan mencakup prioritas fungsi kritis dan strategi manajemen risiko	Rencana pemulihan, matriks prioritas, analisis dampak bisnis

4.2.3 Formulasi dan Kalkulasi Nilai Tingkat Kematangan

Formulasi dalam menyusun intrumen penilaian tigkat kematangan keamanan siber pada penelitian ini mengadopsi pendekatan berbasis model CMM dengan skema *equal weighting*. Pendekatan ini dipilih dengan pertimbangan kesederhanaan, transparansi, dan kesesuaian dengan praktik yang diadopsi dalam standar dan kerangka kerja yang telah diakui secara internasional, seperti CMMI, ISO/IEC 33020:2019, serta NIST CSF. Formulasi kalkulasi kematangan yang disusun mengacu pada prinsip bahwa penilaian dilakukan secara berjenjang dan terstruktur, dimulai dari butir pertanyaan subkategori, kemudian dikonsolidasikan pada tingkat kategori, dilanjutkan pada tingkat fungsi/domain, hingga memperoleh nilai kematangan keseluruhan organisasi. Pendekatan *equal weighting* diterapkan di setiap tingkat agregasi, dimana setiap butir, kategori, maupun fungsi memiliki kontribusi yang sama terhadap skor tingkat kematangan pada level di atasnya. Pendekatan ini merujuk pada temuan penelitian [18] yang menyatakan bahwa dalam kondisi belum tersedia data objektif mengenai bobot prioritas kontrol, maka *equal weighting* adalah pendekatan dasar yang umum digunakan dalam *maturity model assessment*. Selain itu ISACA juga merekomendasikan penggunaan rata-rata sederhana dalam penghitungan kapabilitas proses jika organisasi belum menerapkan mekanisme penentuan bobot berbasis risiko atau prioritas strategis [26]. Setiap butir pertanyaan atau kontrol dinilai dalam skala jawaban 0–3, yang merepresentasikan tingkat adopsi dan implementasi dalam organisasi, detail representasi skor skala jawaban disajikan dalam Tabel 7.

Tabel 7. Representasi Skor Skala Jawaban

Skala Jawaban	Nilai Skor
Tidak Diterapkan	0
Perencanaan	1
Parsial	2
Menyeluruh	3

Selanjutnya, formulasi kalkulasi yang diadopsi dalam penelitian ini dirumuskan pada Persamaan (1) untuk nilai/level kategori, Persamaan (2) untuk nilai/level Fungsi, dan Persamaan (3) untuk nilai/level kematangan organisasi.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Pada persamaan (1), C_k merupakan nilai kematangan kategori ke-k. S_i adalah skor butir ke-i dalam kategori, sedangkan n merupakan jumlah butir dalam kategori tersebut.

$$C_k = \frac{\Sigma_{i=1}^{n} S_i}{n} \quad (1)$$

Pada persamaan (2), F_j merupakan nilai kematangan Fungsi ke-j, sedangkan m merupakan jumlah kategori dalam fungsi tersebut.

$$F_j = \frac{\Sigma_{k=1}^{m} C_k}{m} \quad (2)$$

Kemudian pada persamaan (3), M_{org} merupakan nilai kematangan keseluruhan organisasi dan p adalah jumlah fungsi yang dinilai.

$$M_{org} = \frac{\Sigma_{j=1}^{p} F_j}{p} \quad (3)$$

Hasil perhitungan skor numerik di setiap tingkat kemudian dipetakan ke dalam level kematangan yang sudah ditetapkan. Tabel pemetaan tingkat kematangan keamanan siber dideskripsikan pada Tabel 7. Penetapan rentang skor rata-rata untuk memetakan nilai kuantitatif ke dalam tingkat kematangan Level 1 sampai dengan 5 pada Tabel 8 ini didasarkan pada prinsip *threshold scoring* berbasis range interval, dimana range untuk level awal lebih lebar, dan menjadi lebih sempit pada level atas. Basis tersebut juga merujuk dari sintesis pada ISO/IEC 33001:2015 tentang Proses asesmen bidang teknologi informasi, yang menyatakan bahwa penilaian capaian atribut proses dilakukan dengan skala *Not Achieved* (<15%), *Partially Achieved* (15–50%), *Largely Achieved* (50–85%), dan *Fully Achieved* (>85%). Prinsip *threshold* pencapaian ini banyak diadopsi ke dalam model kematangan, dengan range yang disesuaikan dengan skala penilaian yang digunakan. Konsep tersebut dan menekankan pada praktik penggunaan *cut-off point* yang tidak liniear dan menyempit pada Level 4 dan 5. Hal tersebut bertujuan untuk mencerminkan kebutuhan konsistensi, metrik terukur, dan integrasi penuh yang memang lebih sulit dicapai [27], [28].

Tabel 8. Pemetaan Skor Tingkat Kematangan

Level Kematangan	Skor Rata-Rata	Deskripsi
Level 1 (Implementasi Awal)	0 - < 0.75	Tidak terukur, tidak konsisten, reaktif
Level 2 (Implementasi Berulang)	0.75 - < 1.75	Berulang, terdokumentasi terbatas
Level 3 (Implementasi Terdefinisi)	1.75 - < 2.5	Terdefinisi, terdokumentasi, terstruktur
Level 4 (Implementasi Terkelola)	2.5 - < 2.9	Terkelola, terukur, berbasis data
Level 5 (Implementasi Optimal)	2.9 – 3.0	Optimal, adaptif, otomatis

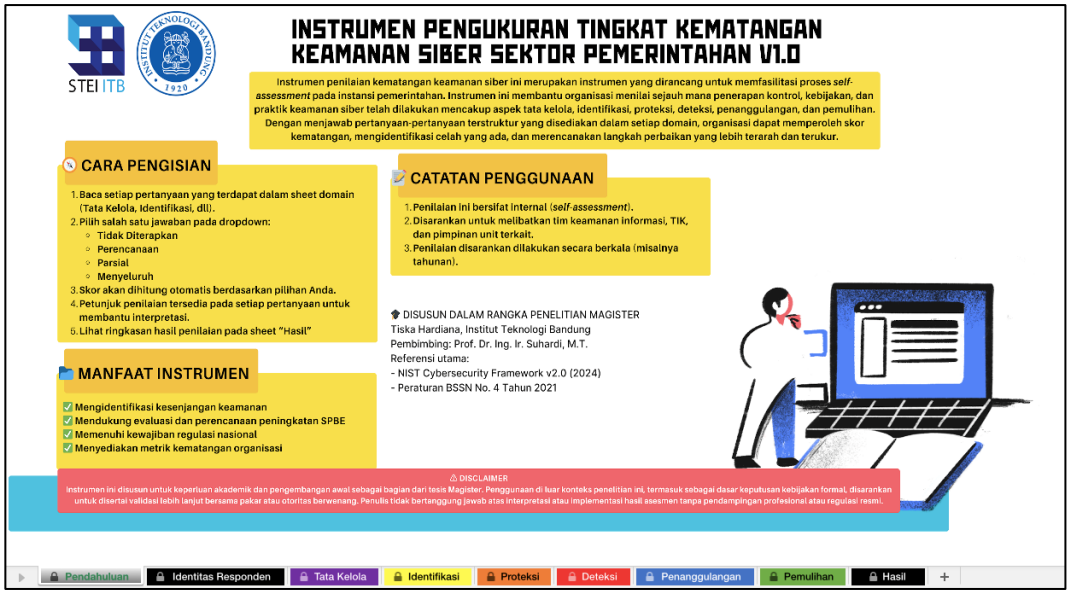
4.3. Instrumen Pengukuran Tingkat Kematangan Keamanan Siber

Instrumen pengukurang dibuat dalam format *spreadsheet* Excel dan dirancang secara terstruktur untuk mencerminkan hasil pemetaan yang sudah dilakukan. Instrumen ini dibangun dalam beberapa *sheet* yang menjadi struktur utama, yang pertama yaitu lembar Pendahuluan yang berisi tentang gambaran umum dan petunjuk umum pengisian bagi pengguna. Selanjutnya adalah lembar Identitas Responden, halaman ini bertujuan untuk mencatat informasi dasar responden asesmen, seperti nama instansi, jabatan, dan unit kerja, guna memastikan akurasi konteks organisasi dalam interpretasi hasil penilaian. Selanjutnya adalah *sheet* inti untuk keenam domain penilaian mulai dari Tata Kelola hingga Pemulihan, dimana setiap *sheet*-nya berisi indikator penilaian yang telah dirumuskan berdasarkan sub-kategori yang sudah ditentukan. Lembar terakhir adalah lembar Hasil yang menjadi *dashboard* untuk menyajikan rekapitulasi skor penilaian kematangan dari seluruh

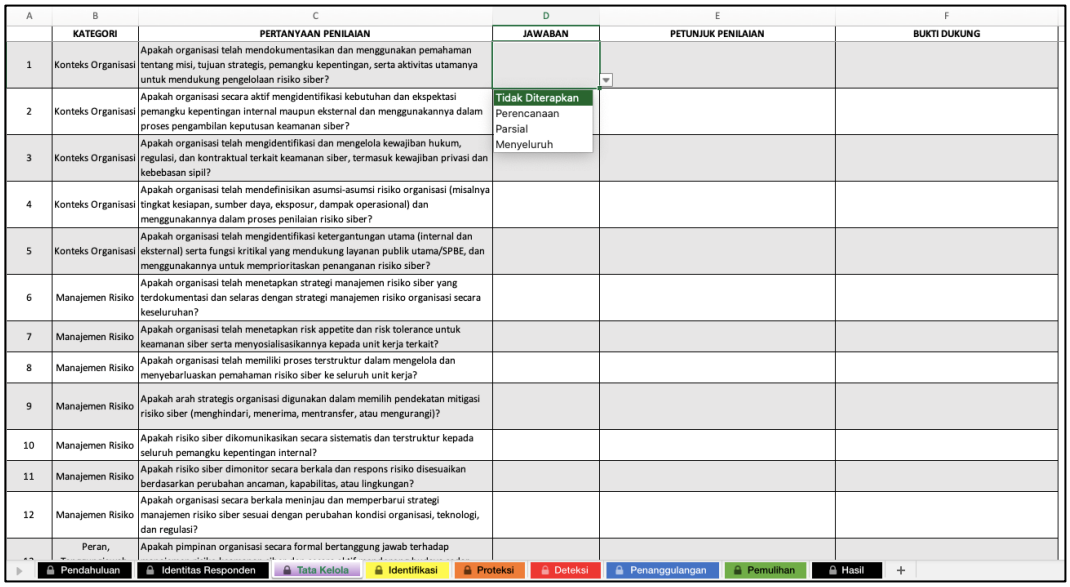
p-ISSN: 2775-4227
e-ISSN: 2775-4219

domain, lengkap dengan visualisasi tingkat kematangan dan klasifikasi kategori, sehingga memudahkan interpretasi dan pengambilan keputusan strategis.

Tampilan lembar pendahuluan dari instrumen ini daat dilihat pada Gambar 5, lembar ini menyajikan gambaran umum, petunjuk pengisian, dan manfaat instrumen, yang bertujuan untuk memberikan pemahaman awal yang komprehensif kepada pengguna sebelum memulai asesmen. Selanjutnya, Gambar 6 menampilkan struktur lembar penilaian inti. Setiap lembar domain dirancang secara sistematis, mencakup pertanyaan penilaian, pilihan jawaban bertingkat dalam format *dropdown*, petunjuk interpretasi, hingga kolom untuk melampirkan bukti dukung. Desain terstruktur ini memastikan proses evaluasi mandiri berjalan secara konsisten dan dapat diaudit. Terakhir, Gambar 7 mengilustrasikan *dashboard* pada lembar Hasil, yang secara otomatis mengolah dan memvisualisasikan seluruh data masukan. *Dashboard* ini menyajikan skor kematangan akhir serta rincian skor per domain dan kategori dalam bentuk grafik radar dan diagram batang. Visualisasi ini memungkinkan organisasi untuk secara cepat mengidentifikasi kekuatan serta area yang memerlukan perbaikan, sehingga mendukung pengambilan keputusan yang lebih efektif berbasis data.

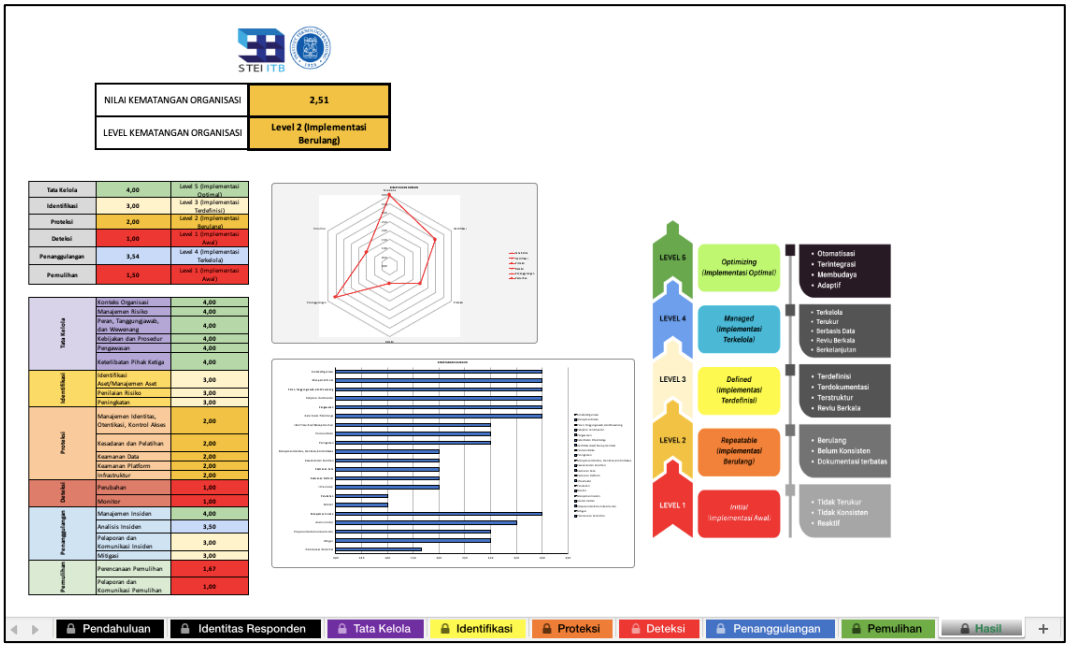


Gambar 5. Lembar Pendahuluan



Gambar 6. Lembar Penilaian Inti

p-ISSN: 2775-4227
e-ISSN: 2775-4219



Gambar 7. Lembar Hasil Penilaian Kematangan

5. DEMONSTRASI DAN EVALUASI

5.1. Simulasi Penilaian Kematangan Keamanan Siber

Simulasi dilakukan untuk mereplikasi skenario penggunaan aktual dari instrumen penilaian tingkat kematangan keamanan siber di lingkungan instansi pemerintahan. Responden merupakan pejabat fungsional Manggala Informatika dari unit kerja pengelola keamanan informasi pada Instansi XYZ, yang memiliki tugas dan tanggung jawab terhadap pengelolaan teknologi informasi serta penerapan kebijakan keamanan siber internal. Reponden akan mengisi seluruh lembar penilaian berdasarkan petunjuk penggunaan. Hasil akhir nilai kematangan organisasi tersebut adalah 3,90 dengan level kematangannya adalah Level 4 (Implementasi Terkelola). Sedangkan hasil ringkasan simulasi penilaian untuk setiap domain dan kategori, disajikan dalam Tabel 9.

Tabel 9. Ringkasan Hasil Simulasi

No	Domain	Nilai / Level Kematangan	Nilai Kematangan Kategori		Ringkasan
1	Tata Kelola	3,77/Level 4: Implementasi Terkelola	Konteks Organisasi	3,60	Instansi XYZ sudah memiliki kebijakan dan proses tata kelola keamanan siber yang terdokumentasi, terstruktur, dan berjalan secara konsisten antar unit. Namun, aspek strategis seperti penetapan formal risk appetite dan risk tolerance, integrasi asesmen risiko antar unit, serta pengelolaan risiko pihak ketiga masih belum optimal. Rekomendasi yang dapat dilakukan untuk meningkatkan level kematangan, organisasi perlu menyusun dan menyosialisasikan dokumen risk appetite secara formal, memperkuat klasifikasi risiko berbasis layanan SPBE kritikal, dan mengintegrasikan evaluasi pihak ketiga dalam kebijakan serta audit keamanan secara menyeluruh.
			Manajemen Risiko	3,71	
			Peran, Tanggung Jawab, dan Wewenang	4,00	
			Kebijakan dan Prosedur	4,00	
			Pengawasan	4,00	
			Keterlibatan Pihak Ketiga	3,30	
2	Identifikasi	3,79/Level 4: Implementasi	Identifikasi Aset dan	3,57	Instansi XYZ telah memiliki inventaris aset yang diperbarui, namun klasifikasi aset dan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

No	Domain	Nilai / Level Kematangan	Nilai Kematangan Kategori		Ringkasan
		Terkelola	Manajemen Aset		dokumentasi aliran data masih perlu diperkuat. Penilaian risiko sudah berjalan rutin, meski asesmen vendor dan verifikasi perangkat belum menjadi prosedur formal. Peningkatan keamanan telah dilaksanakan secara terstruktur dan terdokumentasi, mencerminkan komitmen *continuous improvement* dalam pengelolaan keamanan.
			Penilaian Risiko	3,80	
			Peningkatan	4,00	
3	Proteksi	3,92/Level 5: Implementasi Optimal	Manajemen Identitas, Otentikasi, dan Kontrol Akses	4,00	Instansi XYZ sudah menerapkan kontrol pengamanan yang menyeluruh dan terdokumentasi baik di aspek teknis, prosedural, dan SDM. Identitas pengguna, perangkat, dan layanan telah dikelola dengan baik, diiringi dengan pengendalian akses fisik dan digital yang sesuai prinsip *least privilege*. Program pelatihan keamanan siber dilakukan rutin dan telah meningkatkan kesadaran pegawai. Pengamanan data sudah menggunakan enkripsi dan manajemen *backup*, walaupun dokumentasi klasifikasi proteksi data perlu dilengkapi. Perlindungan *platform* dan infrastruktur telah memanfaatkan *firewall*, IDS/IPS, dan *patch* rutin, namun prosedur pengujian keamanan aplikasi internal berbasis SSDLC belum sepenuhnya formal. Peninjauan risiko fisik dan ketersediaan layanan dilakukan teratur, mendukung kesinambungan operasional organisasi.
			Kesadaran dan Pelatihan	4,00	
			Keamanan Data	3,75	
			Keamanan *Platform*	3,83	
			Infrastruktur	4,00	
4	Deteksi	3,90/Level 5: Implementasi Optimal	*Monitoring*	3,80	Intansi XYZ telah memiliki kapabilitas yang sangat baik dalam melakukan deteksi ancaman siber secara proaktif dan responsif. Pemantauan terhadap aktivitas jaringan, sistem, dan layanan kritikal dilakukan secara rutin dan mencakup aspek internal maupun eksternal. Proses analisis kejadian juga telah dilengkapi dengan mekanisme korelasi data, penilaian dampak, dan pelaporan yang tepat sasaran. Seluruh kegiatan deteksi didukung oleh tim operasional yang berfungsi sebagai pusat monitoring, serta sistem yang memungkinkan deteksi dini terhadap anomali dan insiden siber. Prosedur deklarasi insiden telah disusun dengan kriteria yang jelas dan sesuai dengan pedoman regulator nasional. Walaupun demikian, organisasi masih dapat meningkatkan mekanisme integrasi *monitoring* antar sistem dan penguatan otomasi dalam analisis anomali
			Analisis Anomali dan Kejadian	4,00	
5	Penanggulangan	4,00/Level 5: Implementasi Optimal	Manajemen Insiden	4,00	Intansi XYZ telah memiliki kapabilitas tanggap insiden yang matang dan terdokumentasi, mencakup deteksi, klasifikasi, koordinasi antar unit, mitigasi, dan pelaporan ke pihak eksternal. Investigasi dan analisis insiden telah mendalam, mencakup identifikasi penyebab utama, pengumpulan data forensik,
			Analisis Insiden	4,00	
			Pelaporan dan Komunikasi	4,00	

p-ISSN: 2775-4227
e-ISSN: 2775-4219

No	Domain	Nilai / Level Kematangan	Nilai Kematangan Kategori		Ringkasan
			Insiden		dan verifikasi dampak untuk mendukung pemulihan dan pembelajaran organisasi. Tindakan mitigasi insiden dilakukan secara terstruktur berbasis bukti, mencegah dampak lanjutan dan potensi pengulangan. Untuk meningkatkan efektivitas, disarankan memperkuat integrasi sistem pelaporan antar unit agar proses eskalasi berjalan lebih cepat dan otomatis. Selain itu, perlu memformalkan dokumentasi hasil evaluasi pasca-insiden sebagai rujukan untuk perbaikan kebijakan, peningkatan kapabilitas teknis, dan penguatan kesiapsiagaan terhadap insiden berskala besar yang melibatkan banyak pihak.
			Mitigasi	4,00	
6	Pemulihan	4,00/Level 5: Implementasi Optimal	Perencanaan Pemulihan	4,00	Intansi XYZ menunjukkan kesiapan tinggi dalam proses pemulihan pasca-insiden, dengan prosedur formal dan terstruktur yang memastikan integritas data cadangan serta keamanan layanan sebelum operasional dipulihkan. Komunikasi selama pemulihan dilakukan transparan dan tepat sasaran kepada seluruh pemangku kepentingan internal maupun eksternal. Praktik ini mencerminkan ketangguhan dan keandalan organisasi dalam memulihkan layanan. Untuk penguatan lebih lanjut, disarankan integrasi yang lebih erat antara rencana pemulihan dan strategi manajemen kontinuitas bisnis, serta formalisasi deklarasi penutupan pemulihan dan dokumentasi lessons learned sebagai landasan untuk pembaruan kebijakan dan peningkatan kapasitas pemulihan di masa depan.
			Pelaporan dan Komunikasi Pemulihan	4,00	

5.2. Evaluasi

Bab Evaluasi pada penelitian ini menggunakan pendekatan *formative* mengacu pada kerangka FEDS (*Formative Evaluation in Design Science Research*) [25]. Evaluasi dilakukan dalam *setting naturalistic* dan *artificial* untuk memperoleh umpan balik yang relevan, baik secara praktis maupun akademis. Tujuan evaluasi ini adalah menilai kualitas, kegunaan, serta validitas instrumen penilaian tingkat kematangan keamanan siber. Lima aspek utama yang dievaluasi meliputi: validitas konten, kelayakan struktur instrumen, pengalaman pengguna (*usability*), representasi level kematangan, dan kesesuaian output penilaian. Evaluasi dilakukan melalui beberapa tahapan, yaitu:

1. Validitas Konten: Melibatkan telaah indikator oleh peneliti dan simulasi pengguna dari Instansi XYZ. Hasilnya, sebagian besar indikator dinilai relevan dan jelas, meskipun terdapat 5 indikator yang perlu diperbaiki karena redaksi kurang umum atau tumpang tindih secara substansi.
2. Kelayakan Struktur Instrumen: Dinilai dari logika penyusunan indikator dan kemudahan navigasi. Mayoritas responden memberikan skor tinggi (rata-rata 4 dari 5), dengan saran teknis minor seperti fleksibilitas sel excel untuk pengisian bukti dukung.
3. Pengalaman Pengguna (*Usability*): Dilakukan melalui observasi dan formulir umpan balik. Responden menilai instrumen mudah dipahami dan digunakan, meskipun diusulkan adanya tambahan contoh isian.
4. Representasi Level Kematangan: Responden menyatakan narasi level sudah jelas dan logis, tetapi merekomendasikan kata kunci ringkas di tiap level untuk mempermudah pemahaman.
5. Kesesuaian Output Penilaian: Hasil skor dan level kematangan dianggap mencerminkan kondisi organisasi. Hal ini diperkuat dengan triangulasi data hasil evaluasi SPBE Instansi XYZ tahun 2024, yang menunjukkan konsistensi pada level kematangan 4–5.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Evaluasi ini memberikan umpan balik penting untuk penyempurnaan instrumen sebelum diimplementasikan lebih luas. Hasilnya menunjukkan bahwa instrumen penilaian telah valid, relevan, dan fungsional sebagai alat asesmen tingkat kematangan keamanan siber pada sektor publik.

5.3. Diskusi

Hasil penelitian menunjukkan bahwa instrumen yang dikembangkan dapat berfungsi dengan baik dan sesuai untuk kebutuhan sektor publik di Indonesia. Pada bagian ini, akan dibahas lebih lanjut mengenai temuan tersebut, perbandingannya dengan model-model yang sudah ada, serta keunggulan, keterbatasan, dan arah pengembangan instrumen ini ke depan. Pendekatan yang digunakan dalam instrumen ini memiliki keunikan jika dibandingkan dengan model-model terdahulu. Beberapa model kematangan sebelumnya cenderung masih bersifat konseptual dan belum terhubung dengan regulasi lokal. Ada pula kerangka kerja generik seperti CMM dan CMMI yang lebih fokus pada rekayasa perangkat lunak, bukan untuk instansi pemerintah dengan kebijakan keamanan spesifik. Penelitian lain seperti [11] juga telah mengembangkan model tata kelola keamanan, namun belum secara spesifik mengintegrasikan aspek kepatuhan terhadap peraturan negara tertentu. Instrumen ini secara eksplisit mengisi kesenjangan tersebut dengan menjembatani standar teknis dengan mandat hukum yang berlaku di Indonesia. Keunggulan utama dari instrumen ini adalah kemampuannya menyelaraskan standar internasional (NIST CSF v2.0) dengan regulasi nasional (Perban 4/2021). Penyelarasan ini membuat setiap indikator penilaian tidak hanya kuat secara teknis, tetapi juga sejalan dengan kewajiban hukum dalam penerapan SPBE. Dari sisi penggunaan, instrumen ini dirancang agar praktis melalui format *spreadsheet* yang dilengkapi *dashboard* visual. Hal ini memudahkan instansi pemerintah dari berbagai tingkat kemampuan untuk melakukan evaluasi mandiri secara lebih objektif dan terstruktur.

Meskipun demikian, penelitian ini juga memiliki beberapa keterbatasan yang perlu diperhatikan untuk pengembangan selanjutnya. Proses validasi baru dilakukan pada satu instansi pemerintah, sehingga pengujian pada skala yang lebih luas diperlukan agar hasilnya dapat lebih umum diterapkan. Selain itu, belum dilakukan uji validitas kuantitatif seperti *Confirmatory Factor Analysis* (CFA) dan uji reliabilitas instrumen, yang penting untuk lebih memperkuat dasar pembuktian model ini secara statistik. Untuk pengembangan ke depan, instrumen ini berpotensi dapat diintegrasikan dengan sistem evaluasi SPBE nasional, khususnya pada domain keamanan SPBE. Kesimpulannya, penelitian ini tidak hanya menghasilkan sebuah alat bantu evaluasi yang praktis dan aplikatif, tetapi juga memberikan kontribusi kajian keilmuan pada bidang keamanan siber. Penelitian ini menawarkan model pengembangan instrumen kematangan keamanan siber yang berlandaskan pada kepatuhan regulasi.

6. KESIMPULAN

Penelitian ini telah berhasil mengembangkan instrumen pengukuran tingkat kematangan keamanan siber yang relevan dan kontekstual untuk instansi pemerintah di Indonesia. Instrumen ini dirancang dengan pendekatan sistematis yang memadukan kerangka kerja NIST CSF versi 2.0 dan regulasi nasional, yaitu Peraturan BSSN Nomor 4 Tahun 2021, sehingga menghasilkan indikator yang komprehensif dan praktis bagi instansi pemerintah. Melalui tahapan evaluasi formatif, ditemukan bahwa instrumen ini memadai untuk digunakan sebagai alat penilaian mandiri, dengan indikator yang mudah dipahami, struktur yang efisien, dan hasil yang representatif. Berdasarkan hasil simulasi dan evaluasi, instrumen ini terbukti dapat memperkuat praktik tata kelola keamanan siber dan dapat digunakan sebagai dasar pengambilan kebijakan instansi pemerintah dalam SPBE. Sebagai rekomendasi, temuan ini menjadi dasar penting untuk penelitian selanjutnya yang dapat difokuskan untuk memperluas validasi instrumen, memperkaya data dengan partisipasi lebih banyak instansi, serta mengintegrasikan pembobotan risiko strategis guna meningkatkan akurasi dan relevansi hasil asesmen.

UCAPAN TERIMAKASIH

Penulis menyampaikan rasa terima kasih kepada Kementerian Komunikasi dan Digital Republik Indonesia atas dukungan pendanaan dari program beasiswa magister dalam penerbitan makalah ini.

DAFTAR PUSTAKA

[1] BSSN, “LANSKAP KEAMANAN SIBER INDONESIA 2024,” 2024. Accessed: Mar. 13, 2025. [Online]. Available: https://www.bssn.go.id/monitoring-keamanan-siber/

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[2] Republik Indonesia, *Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik*. Indonesia, 2018.
[3] Badan Siber dan Sandi Negara, *Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik*. Indonesia, 2021.
[4] A. Rabii, S. Assoul, K. Ouazzani Touhami, and O. Roudies, "Information and cyber security maturity models: a systematic literature review," Oct. 01, 2020, *Emerald Group Holdings Ltd.* doi: 10.1108/ICS-03-2019-0039.
[5] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, 2016. doi: 10.1109/PCCC.2016.7820663.
[6] M. C. Paulk, B. Curtis, M. B. Chrissis, and C. V Weber, "Capability Maturity Model SM for Software, Version 1.1," 1993. [Online]. Available: http://www.rai.com
[7] Carnegie Mellon University, *Capability Maturity Model Integration (CMMI SM), Version 1.1*. 2002.
[8] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. doi: 10.6028/NIST.CSWP.29.
[9] Badan Siber dan Sandi Negara, *PERATURAN BADAN SIBER DAN SANDI NEGARA NOMOR 6 TAHUN 2021 TENTANG ORGANISASI DAN TATA KERJA BADAN SIBER DAN SANDI NEGARA*. Indonesia, 2021.
[10] A. Shaked, L. Tabansky, and Y. Reich, "Incorporating Systems Thinking into a Cyber Resilience Maturity Model," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 110–115, Apr. 2021, doi: 10.1109/EMR.2020.3046533.
[11] Y. Maleh, A. Sahid, and M. Belaissaoui, "A MATURITY FRAMEWORK FOR CYBERSECURITY GOVERNANCE IN ORGANIZATIONS," *EDPACS*, vol. 63, no. 6, pp. 1–22, 2021, doi: 10.1080/07366981.2020.1815354.
[12] M. Zammani, R. Razali, and D. Singh, "Organisational Information Security Management Maturity Model," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 9, pp. 668–678, 2021, doi: 10.14569/IJACSA.2021.0120974.
[13] J. Vom Brocke, A. Hevner, and A. Maedche, *Design Science Research. Cases*. Springer, 2020. doi: https://doi.org/10.1007/978-3-030-46781-4.
[14] Klaus. Krippendorff, *Content analysis : an introduction to its methodology*. Sage, 2004.
[15] M. E. Whitman and H. J. Mattord, *Management of Information Security*, Sixth Edition. Cengage, 2018.
[16] R. Wendler, "The maturity of maturity model research: A systematic mapping study," *Inf Softw Technol*, vol. 54, no. 12, pp. 1317–1339, Dec. 2012, doi: 10.1016/j.infsof.2012.07.007.
[17] T. De Bruin *et al.*, "Understanding the Main Phases of Developing a Maturity Assessment Model," in *Australasian (ACIS) ACIS 2005 Proceedings*, 2005. [Online]. Available: http://aisel.aisnet.org/acis2005/109
[18] G. Büyüközkan and M. Güler, "Cybersecurity maturity model: Systematic literature review and a proposed model," *Technol Forecast Soc Change*, vol. 213, Apr. 2025, doi: 10.1016/j.techfore.2025.123996.
[19] A. Aliyu *et al.*, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Applied Sciences (Switzerland)*, vol. 10, no. 10, May 2020, doi: 10.3390/app10103660.
[20] M. N. Y. Marican, S. A. Razak, A. Selamat, and S. H. Othman, "Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review," *IEEE Access*, vol. 11, pp. 5442–5452, 2023, doi: 10.1109/ACCESS.2022.3229766.
[21] M. J. Butkovic and R. A. Caralli, "Advancing Cybersecurity Capability Measurement Using the CERT ®-RMM Maturity Indicator Level Scale CERT ® Division," 2013. [Online]. Available: http://www.sei.cmu.edu
[22] S. Almuhammadi and M. Alsaleh, "Information Security Maturity Model for Nist Cyber Security Framework," Academy and Industry Research Collaboration Center (AIRCC), Feb. 2017, pp. 51–62. doi: 10.5121/csit.2017.70305.
[23] A. M. Rea-Guaman, T. San Feliu, J. A. Calvo-Manzano, and I. D. Sanchez-Garcia, "Comparative study of cybersecurity capability maturity models," in *Communications in Computer and Information Science*, Springer Verlag, 2017, pp. 100–113. doi: 10.1007/978-3-319-67383-7_8.
[24] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: a case study," *Journal of Supercomputing*, vol. 74, no. 10, pp. 5171–5186, Oct. 2018, doi: 10.1007/s11227-018-2479-2.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[25] J. Venable, J. Pries-Heje, and R. Baskerville, "FEDS: A Framework for Evaluation in Design Science Research," *European Journal of Information Systems*, vol. 25, no. 1, pp. 77–89, Jan. 2016, doi: 10.1057/ejis.2014.36.

[26] ISACA, *Implementing the NIST Cybersecurity Framework Using COBIT 2019*. 2019. [Online]. Available: www.instagram.com/isacanews/

[27] A. Tarhan, O. Turetken, and H. A. Reijers, "Business process maturity models: A systematic literature review," *Inf Softw Technol*, vol. 75, pp. 122–134, Jul. 2016, doi: 10.1016/j.infsof.2016.01.010.

[28] L. Bernardo, S. Malta, and J. Magalhães, "An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF," *Electronics (Switzerland)*, vol. 14, no. 7, Apr. 2025, doi: 10.3390/electronics14071364.