BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1. Tinjauan Pustaka

Terdapat banyak studi literatur yang membahas terkait dengan kerangka kerja pengukuran tingkat kematangan keamanan sistem informasi. Sebelum memulai penelitian, perlu dilakukan kajian terhadap penelitian sebelumnya terkait pengukuran tingkat kematangan keamanan sistem informasi.

Penelitian mengenai keamanan informasi dan evaluasi tingkat kematangan sistem telah banyak dilakukan di berbagai sektor, terutama seiring meningkatnya ancaman siber yang mendorong kebutuhan akan kerangka kerja keamanan informasi yang kuat, adaptif, dan terukur. Salah satu studi mengintegrasikan tiga standar internasional, NIST CSF 2.0, ISO/IEC 27001:2022 dan CIS *Controls* v8, dan berhasil merumuskan 22 komponen pengendalian keamanan informasi yang efektif untuk memperkuat Sistem Pemerintahan Berbasis Elektronik (SPBE) di sektor publik. Keterbatasan pada penelitian ini yaitu tidak ada pengukuran kematangan aktual, hanya fokus pada rancangan kontrol. (Tanjung dkk., 2024).

Penelitian pada organisasi pemerintah di Indonesia, rancangan kerangka penilaian kematangan keamanan siber dengan menggabungkan NIST CSF, ISO/IEC 27002, dan CIS v8, menghasilkan identifikasi terhadap 21 domain kematangan kritis yang mencerminkan kinerja manajemen TIK instansi pemerintah, keterbatasan pada penelitian ini yaitu belum diterapkan di organisasi nyata dan tidak ada pembahasan risiko spesifik atau *gap analysis* (Bashofi & Salman, 2022). Penelitian serupa membandingkan NIST CSF, ISO/IEC 27002, COBIT, dan PCI DSS, dan menekankan pentingnya konsistensi dalam menetapkan indikator kematangan di lingkungan pemerintahan. Dalam penelitiannya mempunyai keterbatasan cakupan luas namun tidak diuji pada studi kasus nyata, hasil hanya berupa desain framework tanpa implementasi empiris. (Sulistyowati dkk., 2020). Namun demikian, adopsi kerangka internasional belum sepenuhnya merata. Penelitian lain menunjukan lemahnya implementasi NIST CSF di lingkungan organisasi publik di Peru dan merekomendasikan penerapan kerangka yang lebih sistematis untuk meningkatkan tata kelola dan kebijakan keamanan

informasi yang akuntabel. Keterbatasan yang ada pada penelitian ini yaitu skor kematangan didapat dari persepsi, pengumpulan data belum mendalam, tidak ada data kualitatif pendukung (Delgado dkk., 2021). Penelitian di Indonesia menilai kematangan keamanan informasi pada BAPENDA Provinsi Jawa Tengah dengan pendekatan NIST-CSF dan ISO/IEC 27001:2013, yang menunjukkan bahwa beberapa area seperti kebijakan keamanan dan manajemen insiden masih berada di bawah tingkat kematangan optimal dan memerlukan mitigasi risiko yang terstruktur. Keterbatasan pada penelitian ini yaitu evaluasi terbatas pada satu instansi, tidak ada validasi ahli, tidak disertai *roadmap* atau strategi implementasi (Aminudin & Supriyanto, 2024).

Pendekatan kombinasi kerangka NIST CSF dan COBIT 2019, menghasilkan 23 kategori kegiatan keamanan informasi dengan 118 aktivitas evaluasi. Evaluasi ini memperkuat pentingnya pengukuran tingkat kematangan yang berorientasi pada perbaikan berkelanjutan di sektor publik. Keterbatasan pada peneliti ini yaitu Fokus pada evaluasi tingkat awal, rekomendasi masih bersifat umum tanpa prioritas mitigasi risiko (Fadya & Utama, 2025). Adapun C2M2, memberikan pendekatan berbasis kapabilitas untuk organisasi kritikal yang memiliki keunikan dalam struktur domain dan metrik indikator, serta dapat dikombinasikan secara sinergis dengan NIST-CSF untuk menghasilkan penilaian kematangan yang lebih komprehensif. Keterbatasan dalam analisis masih terbatas pada aspek teoritis, tidak ada penerapan langsung atau studi lapangan. (Zakiy & Angresti, 2024). Penelitian yang menerapkan kombinasi NIST-CSF dan CMMI dalam menilai kematangan keamanan sistem informasi akademik, menunjukkan perlunya perbaikan signifikan pada fungsi identifikasi risiko. Penelitian tersebut hanya fokus pada satu fungsi NIST (*Identify*), belum mencakup semua domain penting keamanan informasi (Amanda dkk., 2023). Di sisi lain, pendekatan kebijakan pengamanan infrastruktur dengan mengintegrasikan domain "*Govern*" dari NIST CSF 2.0 dan ISO/IEC 27001:2022, memperjelas peran tata kelola sebagai fondasi sistem keamanan yang efektif pada sektor pemerintahan. Penelitian tersebut tidak menyertakan evaluasi kematangan aktual, hanya menghasilkan model kebijakan. (Afiansyah & Febriyani, 2023). Pengembangan metodologi *Enhanced*

Prioritized Gap Analysis (EPGA) berbasis NIST CSF dan C2M2 untuk melakukan mitigasi kerentanan secara prioritas. *Framework* ini sangat berguna dalam konteks infrastruktur kritis seperti sistem pajak, yang membutuhkan prioritas tindakan pengamanan berbasis analisis kuantitatif dan multi-kriteria. Model dalam penelitian ini kompleks dan butuh sumber daya tinggi, tidak cocok untuk organisasi skala kecil/menengah. (Nikhil dkk., 2020).

Tabel 2.1. Penelitian terdahulu

No	Penelitian	*Framework*	Fokus & Hasil	*Gap*
1.	*Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using* NIST CSF, COBIT, ISO/IEC 27002 *and* PCI DSS. (Sulistyowati dkk., 2020)	NIST CSF, COBIT, ISO/IEC 27002, PCI DSS (model : *Integrated Maturity Framework)*	Evaluasi dan Perancangan. Temuan 21 kategori keamanan siber sebagai acuan perbaikan manajemen IT	Hanya merancang kontrol, tidak mengukur *maturity* dan tanpa implementasi nyata.
2.	*Cybersecurity Maturity Assessment Design Using* NISTCSF, CIS CONTROLS v8 *and* ISO/IEC 27002. (Bashofi & Salman, 2022)	NIST CSF, ISO/IEC 27002, CIS v8 (model: SSECMM (5 Level))	Evaluasi dan Rekomendasi. Temuan 21 kategori keamanan sebagai dasar evaluasi dan peningkatan performa IT	Model konseptual, belum diterapkan dan tanpa *gap analysis*.
3.	*Design Information Security in Electronic-Based Government Systems Using* NIST CSF 2.0, ISO/IEC 27001: 2022 *and* CIS Control. (Tanjung dkk., 2024)	NIST CSF 2.0, ISO/IEC 27001:2022, CIS v8 (model: Synthesis 22 komponen)	Evaluasi dan Rekomendasi. Temuan penguatan kontrol dan dokumen keamanan sistem SPBE	Komparatif *framework*, tidak ada pemetaan rinci atau penilaian *maturity*.

Tabel 2.1. Penelitian terdahulu (Lanjutan)

No	Penelitian	*Framework*	Fokus & Hasil	*Gap*
4.	*Comparative Analysis of Cybersecurity Maturity Frameworks*: NIST-CSF and C2M2. (Zakiy & Angresti, 2024)	NIST CSF, C2M2	Evaluasi. Temuan penggunaan gabungan *framework* memberikan penilaian lebih komprehensif	Implementasi NIST CSF saja, tanpa ISO 27002 dan C2M2.
5.	*Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis*. (Nikhil dkk., 2020)	NIST CSF, C2M2 (model: EPGA (Enhanced Prioritized *Gap Analysis*))	Evaluasi dan Rekomendasi. Temuan model EPGA mampu prioritaskan mitigasi celah keamanan secara otomatis	Evaluasi terbatas, tanpa C2M2 dan pemetaan menyeluruh.
6.	Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022. (Afiansyah & Febriyani, 2023)	NIST CSF 2.0, ISO/IEC 27001:2022 Integrasi konsep govern	Rekomendasi Strategis. Temuan model kebijakan tata kelola keamanan siber yang sistematis	Identifikasi aktivitas keamanan, tidak mengukur *maturity* aktual.
7.	*Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using* NIST CSF *and* COBIT 2019. (Fadya & Utama, 2025)	NIST CSF, COBIT 2019, model CMMI	Evaluasi dan Rekomendasi. Semua fungsi pada tingkat 1, dibutuhkan peningkatan ketahanan sistem	Analisis teoretis NIST-C2M2, tanpa studi kasus.

Tabel 2.1. Penelitian terdahulu (Lanjutan)

No	Penelitian	*Framework*	Fokus & Hasil	*Gap*
8.	Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013. (Aminudin & Supriyanto, 2024)	NIST CSF, ISO/IEC 27001:2013, model KAMI Index + *Mapping* NIST	Evaluasi. Risiko tinggi pada aset TI, dibutuhkan mitigasi dengan kontrol NIST dan ISO	Fokus pada fungsi *Identify*, cakupan *framework* terbatas.
9.	*Methodology Based On The* NIST *Cybersecurity Framework As A Proposal For Cybersecurity Management In Government Organizations*. (Delgado dkk., 2021)	NIST CSF, model Skala Likert (0-4) tiap fungsi NIST	Evaluasi. Temuan perlunya adopsi formal *framework* NIST oleh pemerintah untuk penguatan sistem keamanan informasi nasional	Hanya domain *Govern*, tanpa evaluasi *maturity*.
10.	Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST *Cybersecurity Framework* dan CMMI. (Amanda dkk., 2023)	NIST CSF, CMMI, model CMMI (5 Level: *Initial* - *Optimizing*)	Evaluasi dan Rekomendasi. Disusun 92 rekomendasi peningkatan berdasarkan NIST SP 800-53.	Metode teoretis, belum cocok untuk pemda dan tanpa ISO 27002.

Berdasarkan Tabel 2.1, pada penelitian yang dilakukan sebelumnya belum ditemukan kajian yang menghasilkan kerangka kerja penilaian tingkat kematangan keamanan informasi untuk sektor publik Indonesia berbasis integrasi NIST CSF, ISO/IEC 27002, dan C2M2. Sehingga penelitian ini menerapkan ketiga kerangka tersebut untuk mengevaluasi tingkat kematangan keamanan informasi pada sistem manajemen informasi objek pajak bumi dan bangunan, serta memberikan rekomendasi strategis berbasis hasil evaluasi tersebut. Pendekatan ini memberikan kontribusi praktis dalam peningkatan kualitas layanan *e-Government* berbasis

pengukuran kematangan keamanan informasi yang terstruktur dan berbasis standar internasional.

2.2. Dasar Teori

2.2.1. Profil Badan Pendapatan, Pengelolaan Keuangan dan Aset Daerah

Badan Pendapatan, Pengelolaan Keuangan dan Aset Daerah (BPPKAD) Kabupaten Banjarnegara yang merupakan Organisasi Perangkat Daerah di bawah Pemerintah Kabupaten Banjarnegara sehingga dalam pelaksanaan tugasnya mendukung visi dan misi yang tertuang dalam Rencana Pembangunan Daerah (RPD) Kabupaten Banjarnegara Tahun 2023-2026.

Dalam kegiatan mendukung visi dan misi Kabupaten Banjarnegara Banjarnegara, BPPKAD Kabupaten Banjarnegara akan "Mewujudkan tata kelola pemerintahan yang baik (*good governance*) dalam kehidupan yang demokratis dan bertanggungjawab", sesuai tujuan yaitu mewujudkan reformasi tata kelola keuangan dengan sasaran meningkatnya kualitas pengelolaan keuangan dan aset daerah dan meningkatnya kemandirian daerah dalam mendukung pembangunan daerah dengan strategi penerapan sistem pengelolaan keuangan terpadu, peningkatan pengelolaan keuangan dan aset daerah.

Bidang Pajak Bumi Dan Bangunan dan Bea Perolehan Hak Atas Tanah Dan Bangunan mempunyai tugas melakukan perencanaan perumusan, pengkoordinasian, pelaksanaan, pembinaan dan fasilitasi, pemantauan, evaluasi serta pelaporan kebijakan bidang pendataan, penilaian dan penetapan objek dan subjek pajak bumi dan bangunan dan bea perolehan hak atas tanah dan bangunan (PBB dan BPHTB), penyajian data dan informasi penerimaan dan mutasi data pajak bumi dan bangunan dan bea perolehan hak atas tanah dan bangunan (PBB dan BPHTB), pemeliharaan, penyempurnaan sistem jaringan, backup data dan sistem pembentukan basis data pendapatan daerah, dan penagihan dan penerimaan serta penentuan objek pemeriksaan pajak bumi dan bangunan dan bea perolehan hak atas tanah dan bangunan (PBB dan BPHTB).

Bidang Pajak Bumi dan Bangunan dan Bea Perolehan Hak Atas Tanah dan Bangunan menyelenggarakan fungsi salah satunya yaitu merumuskan kebijakan terkait PBB dan BPHTB, menyajikan data dan informasi penerimaan serta mutasi

data PBB dan BPHTB, memelihara dan menyempurnakan sistem jaringan serta basis data pendapatan daerah,

Seksi Pengolahan Data dan Informasi mempunyai tugas melakukan penyiapan bahan perumusan, pengkoordinasian, pelaksanaan, pembinaan dan fasilitasi, pemantauan, evaluasi serta pelaporan kebijakan bidang penyajian data dan informasi penerimaan dan mutasi data pajak bumi dan bangunan dan bea perolehan hak atas tanah dan bangunan (PBB dan BPHTB), pemeliharaan, penyempurnaan sistem jaringan, backup data dan sistem pembentukan basis data pendapatan daerah.

Bentuk data dan informasi yang dikelola pada SISMIOP mencakup data pribadi wajib pajak, data finansial bernilai strategis, serta data transaksi lintas proses yang digunakan dalam pengelolaan pendapatan daerah. Karakteristik data tersebut menuntut pendekatan evaluasi keamanan informasi yang tidak hanya berfokus pada kontrol teknis, tetapi juga pada tata kelola risiko dan tingkat kapabilitas organisasi.

2.2.2. Sistem Manajemen Informasi Objek Pajak Bumi dan Bangunan (SISMIOP)

SISMIOP merupakan suatu sistem informasi yang terpadu yang dimaksudkan untuk mendukung penyediaan informasi yang berhubungan dengan seluruh fungsi di dalam administrasi pada semua tingkat organisasi pengelola PBB. SISMIOP diperuntukan bagi kegiatan operasional dan manajemen, pengambilan keputusan, evaluasi kerja, dan analisis kebijaksanaan melalui aplikasi komputer yang khusus dirancang untuk kebutuhan tersebut. SISMIOP dibangun dengan menggunakan pendekatan sistem, yaitu permasalahan yang dihadapi ditinjau secara komprehensif dan terpadu sehingga tujuan yang akan dicapai merupakan solusi global yang memperhatikan interaksi diantara komponen-komponen organisasi dan juga komponen eksternal.

SISMIOP dimanfaatkan untuk mengolah informasi data objek dan subjek pajak dengan bantuan komputer, sejak pengumpulan data (pendaftaran, pendataan, dan penilaian), pemberian identitas (Nomor Objek Pajak), pemrosesan, pemeliharaan, sampai dengan pencetakan hasil keluaran berupa SPPT, STTS dan

DHKP serta Pelayanan Satu Tempat (PST) (Kementerian Keuangan Republik Indonesia, 2017).

Sistem Manajemen Informasi Objek Pajak (SISMIOP) adalah suatu sistem yang terintegrasi untuk mengolah informasi data objek dan subjek pajak dengan bantuan komputer, pajak pengumpulan data (dengan pendaftaran, pendataan dan penilaian), pemberian identitas Nomor Objek Pajak (NOP), pemrosesan, pemeliharaan (*updating*), sampai dengan hasil keluaran berupa SPPT, STTS, dan DHKP dalam program SISMIOP, serta peningkatan pelayanan Wajib Pajak pada satu tempat. (DJP, 1994)

2.2.3. Sistem Manajemen Keamanan Informasi (SMKI)

Sistem manajemen keamanan informasi adalah pendekatan terstruktur dan sistematis untuk mengelola keamanan informasi dan risiko terkait TI lainnya. Sistem ini mencakup berbagai kontrol untuk menjaga data tetap aman dari berbagai ancaman dan kerentanan keamanan. Sistem ini dapat membantu memastikan keamanan informasi umum, serta perlindungan data pribadi (National Safety and Quality Digital Mental Health Standards, 2022).

Sistem Manajemen Keamanan Informasi (SMKI) bekerja berdasarkan prinsip siklus *Plan-Do-Check-Act* (PDCA), yang memastikan bahwa keamanan informasi tidak hanya diimplementasikan sekali, tetapi dijalankan sebagai proses berulang yang selalu diperbaiki. Dalam fase *Plan*, organisasi merancang kebijakan dan sasaran keamanan informasi sesuai dengan kebutuhan bisnis dan risiko yang dihadapi. Fase *Do* melibatkan implementasi dan pengoperasian kontrol keamanan, sedangkan *Check* mengacu pada aktivitas pemantauan, pengukuran, dan evaluasi efektivitas kontrol tersebut. Terakhir, fase *Act* digunakan untuk menindaklanjuti temuan audit dan hasil evaluasi guna meningkatkan sistem keamanan secara terus-menerus (Firmansyah, 2024).

Pada inti pelaksanaan ISMS, terdapat literatur klasik keamanan informasi menurut Whitman dan Mattord (2013) yang mengemukakan bahwa seluruh strategi dan kebijakan keamanan informasi harus berpijak pada tiga prinsip utama yang dikenal sebagai CIA *Triad*, yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

Gambar 2.1. The Confidentiality, Integrity, Availability (CIA) Triad (Nikander dkk., 2020)

Ketiga aspek pada Gambar 2.1 tidak hanya menjadi landasan dalam perancangan sistem keamanan informasi, tetapi juga digunakan sebagai tolok ukur dalam mengevaluasi efektivitas pengamanan suatu organisasi terhadap berbagai ancaman siber. Aspek pertama, *confidentiality* (kerahasiaan), menekankan pentingnya mencegah akses yang tidak sah terhadap data dan informasi. Aspek kedua, *integrity* (integritas) merujuk pada jaminan bahwa informasi yang dikelola tetap akurat, utuh, dan tidak mengalami perubahan tanpa otorisasi selama proses penyimpanan, pengolahan, maupun transmisi. Aspek terakhir, *availability* (ketersediaan) memastikan bahwa sistem informasi dan data yang tersimpan di dalamnya selalu dapat diakses tepat waktu oleh pengguna yang berwenang (Whitman dan Mattord, 2013).

Terdapat beberapa standar SMKI yang berbeda tergantung pada tingkat, lingkup, dan jenis informasi yang digunakan. Satu jenis standar manajemen keamanan informasi adalah ISO 27000 *family*, yang mencakup banyak industri. Dalam standar keamanan informasi ISO/IEC 27000 memiliki beberapa series yang telah dikembangkan, dapat dilihat pada Tabel 2.2.

Tabel 2.2. Daftar ISO 27000 *Family* (ISO/IEC, 2022)

Standar	Judul (Teknologi Informasi - Teknik Keamanan - Subjudul)
Terminologi	
ISO/IEC 27000:2018	Sistem manajemen keamanan informasi - Ikhtisar dan kosakata
Persyaratan	
ISO/IEC 27001:2013	Sistem manajemen keamanan informasi - Persyaratan
ISO/IEC 27006:2015	Persyaratan untuk badan yang menyediakan audit dan sertifikasi sistem manajemen keamanan informasi
ISO/IEC 27009:2016	Aplikasi sektor spesifik ISO/IEC 27001 - Persyaratan

Tabel 2.2. Daftar ISO 27000 *Family* (ISO/IEC, 2022) (lanjutan)

Standar	Judul (Teknologi Informasi - Teknik Keamanan - Subjudul)
ISO/IEC 27011:2016	Aplikasi sektor spesifik ISO/IEC 27001 untuk telekomunikasi
Pedoman (*Guidelines*)	
ISO/IEC 27002:2013	Kode praktik untuk kontrol keamanan informasi
ISO/IEC 27003:2017	Sistem manajemen keamanan informasi - Panduan implementasi
ISO/IEC 27004:2016	Sistem manajemen keamanan informasi - Pemantauan, pengukuran, analisis dan evaluasi
ISO/IEC 27005:2018	Manajemen risiko keamanan informasi
ISO/IEC 27007:2020	Panduan untuk audit sistem manajemen keamanan informasi
ISO/IEC TS 27008:2019	Panduan untuk penilaian kontrol keamanan informasi
ISO/IEC 27013:2015	Panduan integrasi implementasi ISO/IEC 27001 dan ISO/IEC 20000-1
ISO/IEC TR 27016:2014	Ekonomi organisasi dalam keamanan informasi
Pedoman Spesifik Sektor	
ISO/IEC 27010:2015	Kode praktik keamanan informasi untuk komunikasi antar dan intra-organisasi
ISO/IEC 27011:2016	Kode praktik untuk kontrol keamanan informasi berdasarkan ISO/IEC 27002 untuk organisasi telekomunikasi
ISO/IEC 27017:2015	Kode praktik untuk kontrol keamanan informasi dalam layanan cloud
ISO/IEC 27018:2019	Kode praktik untuk perlindungan informasi identitas pribadi (PII) di lingkungan *cloud* publik sebagai pemroses PII
ISO/IEC 27019:2017	Kontrol keamanan informasi untuk industri utilitas energi

Berdasarkan Tabel 2.2, standar ISO 27000 *family* yang memiliki keterkaitan sesuai dengan tema penelitian ini terdapat pada Tabel 2.3.

Tabel 2.3. Seri standar keamanan informasi ISO/IEC 27000

Standar yang Diterbitkan	Tahun Terbit	Judul Standar
ISO/IEC 27000	2009	Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Dasar dan kosakata
ISO/IEC 27001	2005	Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Persyaratan
ISO/IEC 27002	2005	Teknologi informasi - Teknik keamanan - Kode praktik untuk manajemen keamanan informasi
ISO/IEC 27003	2010	Teknologi informasi - Teknik keamanan - Panduan implementasi sistem manajemen keamanan informasi
ISO/IEC 27004	2009	Teknologi informasi - Teknik keamanan - Manajemen keamanan informasi - Pengukuran
ISO/IEC 27005	2008	Teknologi informasi - Teknik keamanan - Manajemen risiko keamanan informasi
ISO/IEC 27006	2007	Teknologi informasi - Teknik keamanan - Persyaratan untuk badan yang menyediakan audit dan sertifikasi sistem manajemen keamanan informasi

2.2.4. Tingkat Kematangan TI (IT *Maturity Level*)

Tingkat kematangan keamanan informasi adalah ukuran sejauh mana proses, kebijakan, dan kontrol keamanan informasi telah diterapkan, dikelola, dan dioptimalkan dalam suatu organisasi (Tinungki dkk., 2021). Model tingkat kematangan sistem manajemen keamanan informasi (SMKI) pada suatu organisasi

akan menentukan tingkat manfaat dan bagaimana kesesuaian SMKI yang telah diterapkan dikaitkan dengan yang diharapkan dan disesuaikan dengan standar yang ada (Iffano dan Riyanarto, 2009). Untuk penilaian, berdasarkan kematangan proses, nilai 0-5 (*incomplete, initial, managed, defined, quantitative, optimizing*) akan diberikan pada tingkat kemampuan dan kematangan (ISO/IEC, 2022).

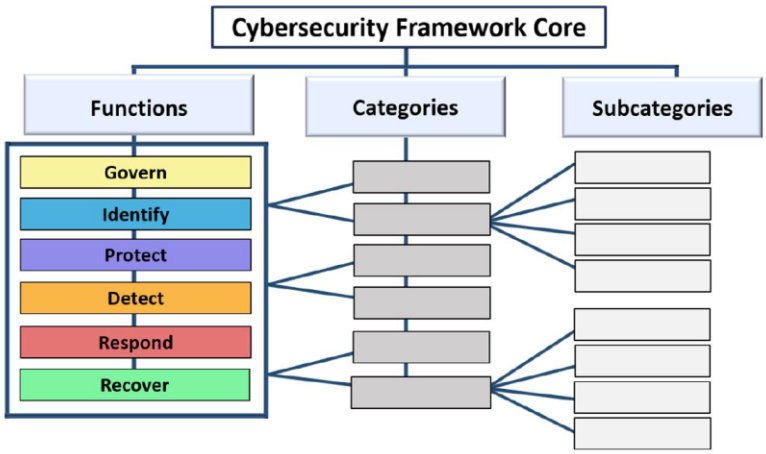
Dalam keamanan siber, NIST *Cybersecurity Framework* (CSF) menggunakan pendekatan maturitas berbasis *Tiers*, yaitu *Tier* 1 (*Partial*) hingga *Tier* 4 (*Adaptive*). *Tier* ini tidak menunjukkan tingkat teknis, tetapi mencerminkan seberapa baik suatu organisasi mengintegrasikan manajemen risiko keamanan ke dalam strategi bisnisnya (National Institute of Standards and Technology, 2024). Model lainnya adalah *Cybersecurity Capability Maturity Model* (C2M2) yang dikembangkan oleh U.S. Department of Energy, terdiri dari 10 domain kapabilitas dan menggunakan 4 tingkat kematangan (MIL 0-3) untuk mengevaluasi seberapa konsisten dan terdokumentasinya praktik keamanan dalam organisasi. MIL ini mencerminkan kemajuan dari tidak adanya praktik formal hingga proses yang terdokumentasi, terintegrasi, dan berkelanjutan (U.S. Department Of Energy, 2022). Nilai-nilai ini dinilai secara subjektif, berdasarkan wawancara dengan para pemangku kepentingan, tinjauan dokumen prosedur yang dijalankan, program pengawasan dan pelaksanaan tujuan dan sasaran perusahaan (ISO/IEC, 2022).

Analisis model kematangan (*maturity model*) dapat digunakan untuk mengidentifikasi status suatu industri saat ini, target dan kondisi yang diinginkan dalam hal peningkatan kualitas layanan perusahaan, dan pertumbuhan yang diinginkan antara saat ini (*as-is*) dan masa yang akan datang (*to-be*). Diharapkan dengan hal ini dapat mengidentifikasi apa saja yang dibutuhkan ketika ingin meningkatkan pengelolaan SI/TI yang mana dalam hal ini pada aspek keamanan informasi hingga dapat mencapai target yang diinginkan. (IT Governance Institute, 2007).

2.2.5. *NIST Cybersecurity Framework* (NIST CSF)

NIST Cybersecurity Framework (CSF) versi 2.0 adalah kerangka kerja strategis yang dikembangkan oleh National Institute of Standards and Technology (NIST) untuk membantu organisasi dari berbagai sektor dan ukuran dalam

mengelola risiko siber secara efektif. CSF 2.0 mengorganisasi hasil keamanan siber dalam bentuk hierarki tiga tingkat: *Functions*, *Categories*, dan *Subcategories* pada Gambar 2.2, yang dirancang agar dapat dipahami oleh audiens luas, mulai dari eksekutif hingga praktisi teknis (National Institute of Standards and Technology, 2024). Kerangka kerja NIST CSF 2.0 digunakan oleh organisasi untuk mengevaluasi sistem dan infrastruktur teknologi informasi yang digunakan untuk menjaga keamanan teknologi dan sistem informasi organisasi dari ancaman siber (Kwon dkk., 2020).



Gambar 2.2. CSF *Core Structure* (National Institute of Standards and Technology, 2024)

Gambar 2.2 terdapat enam fungsi inti dalam CSF 2.0, yaitu *Govern*, *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*, yang secara kolektif mencerminkan siklus manajemen risiko siber secara menyeluruh.

a. Fungsi *Govern* (GV) memastikan strategi, kebijakan, dan peran tanggung jawab keamanan siber organisasi ditetapkan dan diawasi.
b. Fungsi *Identify* (ID) membantu mengenali aset, ancaman, dan kerentanan yang relevan untuk memahami risiko yang dihadapi.
c. Fungsi *Protect* (PR) mencakup langkah-langkah perlindungan seperti pengendalian akses, pelatihan, dan keamanan data untuk mencegah insiden.
d. Fungsi *Detect* (DE) fokus pada pendeteksian dini aktivitas mencurigakan atau serangan siber.
e. Fungsi *Respond* (RS) mengarahkan respons cepat terhadap insiden guna membatasi dampak.

f. Fungsi *Recover* (RC) mendukung pemulihan sistem dan layanan agar operasional kembali normal pasca insiden.

Pada Gambar 2.3. CSF 2.0 juga memperkenalkan konsep *Organizational Profiles* untuk menggambarkan postur keamanan saat ini dan yang ditargetkan, berdasarkan pencapaian terhadap *outcomes* pada CSF *Core*. NIST menjelaskan bahwa penyusunan *Organizational Profile* dilakukan melalui tiga tahap awal, yaitu:

a. *Scoping* untuk menetapkan ruang lingkup, asumsi, dan batasan sistem yang akan dinilai
b. *Gathering Information*, yaitu mengumpulkan seluruh informasi yang diperlukan seperti kebijakan keamanan, prioritas manajemen risiko, dokumentasi proses bisnis, profil risiko, serta standar atau persyaratan yang berlaku
c. *Creating the Profile*, yaitu menentukan *outcomes* CSF yang relevan bagi organisasi dan mendokumentasikan capaian aktual (*Current Profile*) serta capaian yang ditargetkan (*Target Profile*) sesuai konteks misi, kebutuhan pemangku kepentingan, persyaratan regulasi, dan lanskap ancaman.

Gambar 2.3. Langkah-langkah Profil Organisasi CSF (National Institute of Standards and Technology, 2024)

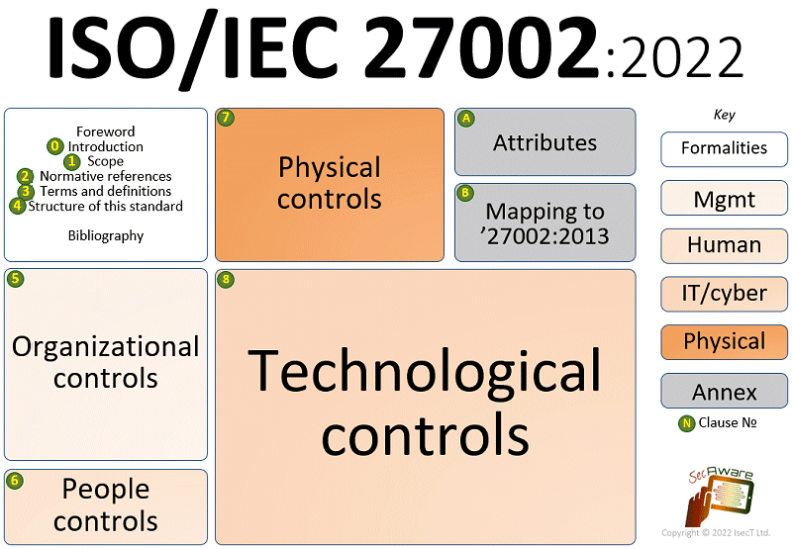
Organizational Profile menjadi dasar penting untuk memahami kondisi keamanan siber organisasi dan menentukan arah peningkatan yang diperlukan. Dengan struktur yang fleksibel, netral terhadap sektor dan teknologi, serta didukung oleh berbagai sumber daya *open source*, CSF 2.0 memungkinkan organisasi untuk menyesuaikan kerangka kerja ini dengan kebutuhan dan konteks spesifiknya. CSF

juga mendukung integrasi dengan manajemen risiko perusahaan secara menyeluruh dan memberikan dasar komunikasi risiko siber yang efektif antar tingkat organisasi maupun dengan pihak eksternal (National Institute of Standards and Technology, 2024).

2.2.6. ISO/IEC 27002

Standar keamanan informasi ISO/IEC 27002 adalah "*Code of Practice for Information Security Management System*" merupakan dokumen standar berisi panduan praktis (*code of practice*) teknik keamanan informasi. ISO/IEC 27002 memberikan panduan kontrol untuk mencapai tujuan kontrol *(control objectives)* keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu (ISO/IEC, 2022). ISO/IEC 27002 berfungsi sebagai panduan dalam pemilihan dan implementasi kontrol keamanan informasi yang relevan berdasarkan hasil kajian risiko organisasi. Standar ini tidak bersifat mengikat atau wajib, namun memberikan referensi yang komprehensif terkait kontrol yang dapat diterapkan dalam mendukung penerapan Sistem Manajemen Keamanan Informasi (SMKI) sesuai ISO/IEC 27001 (Bashofi & Salman, 2022).

Versi terbaru ISO/IEC 27002 tahun 2022 terdiri dari 93 kontrol yang dikelompokkan ke dalam empat kategori utama, yaitu kontrol organisasi, kontrol SDM (Sumber Daya Manusia), kontrol fisik, dan kontrol teknologi (ISO/IEC, 2022). Masing-masing kontrol didesain untuk membantu organisasi dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Standar ini juga memperkenalkan pendekatan atribut untuk mengklasifikasikan kontrol, sehingga memudahkan organisasi dalam menyusun strategi keamanan berbasis risiko dan konteks operasional (Bashofi & Salman, 2022).



Gambar 2.4. Struktur ISO/IEC 27002 (ISECT Limited, 2025)

Pada Gambar 2.4, ISO 27002:2022 memiliki 93 kontrol dan 4 klausul yang terdaftar antara lain:

1. *Organizational controls* terdiri dari 37 kontrol.
2. *People controls* terdiri dari 8 kontrol.
3. *Physical controls* terdiri dari 14 kontrol.
4. *Technological controls* terdiri dari 34 kontrol.

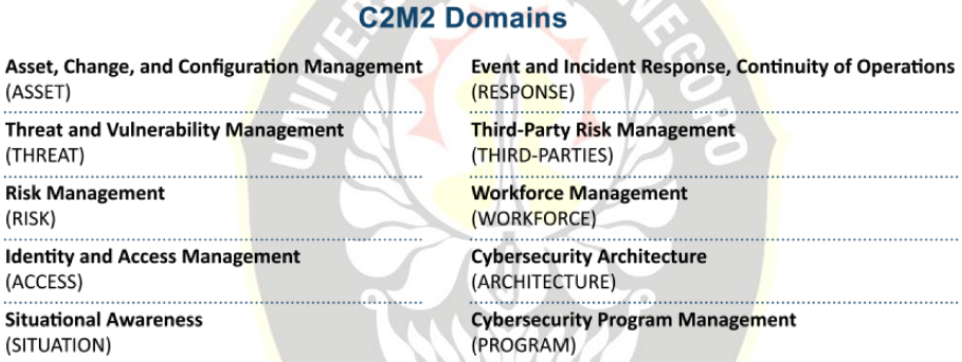
2.2.7. *Cybersecurity Capability Maturity Model* (C2M2)

Cybersecurity Capability Maturity Model (C2M2) muncul dari model kematangan kapabilitas yang dirancang dari bidang manajemen kualitas pada tahun 1930-an. Model ini menjadi populer pada tahun 1990-an ketika pertama kali dikembangkan oleh lembaga rekayasa perangkat lunak (Paulk, 2009).

Cybersecurity Capability Maturity Model (C2M2) adalah kerangka kerja yang dikembangkan oleh Departemen Energi Amerika Serikat. Kerangka kerja ini awalnya diterbitkan pada tahun 2012 dan terakhir diperbarui pada tahun 2022. Kerangka kerja ini bersifat sukarela yang dirancang untuk membantu organisasi mengevaluasi kemampuan keamanan siber mereka dan mengoptimalkan investasi keamanan. C2M2 mendefinisikan praktik di 10 domain keamanan siber dan mengukur perkembangan dalam setiap domain menggunakan indikator tingkat kematangan (U.S. Department Of Energy, 2022).

Cybersecurity Capability Maturity Model (C2M2) merupakan alat gratis untuk membantu organisasi mengevaluasi kemampuan keamanan siber mereka dan mengoptimalkan investasi keamanan. Model ini menggunakan serangkaian praktik keamanan siber yang telah teruji oleh industri yang berfokus pada aset dan lingkungan *information technology* (TI) dan *operation technology* (OT). Organisasi dapat menggunakan C2M2 untuk mengukur kemampuan keamanan siber mereka secara konsisten dari waktu ke waktu, mengidentifikasi tingkat kematangan target berdasarkan risiko, dan memprioritaskan tindakan dan investasi yang memungkinkan mereka memenuhi target (Energy, 2022).

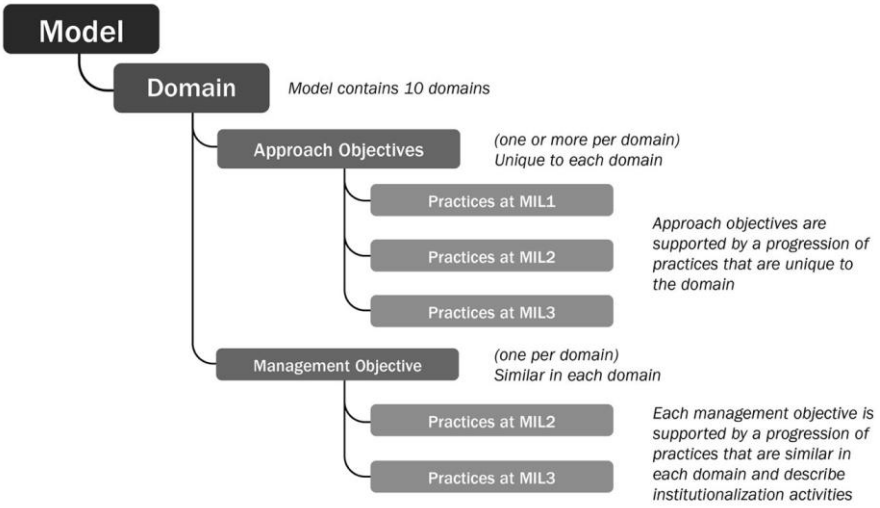
Komponen model C2M2 berisi lebih dari 350 praktik keamanan siber, yang dikelompokkan berdasarkan tujuan ke dalam 10 domain logis (Departemen Energi AS, 2022) pada Gambar 2.5.



Gambar 2.5. Domain C2M2 (Departemen Energi AS, 2022)

Praktik dalam setiap domain diorganisasikan ke dalam tujuan yang dapat dicapai dengan menerapkan praktik dalam domain tersebut. Praktik merupakan komponen paling mendasar dari C2M2. Setiap praktik merupakan pernyataan singkat yang menjelaskan aktivitas keamanan siber yang dapat dilakukan oleh suatu organisasi. Praktik dalam setiap domain disusun untuk maju seiring dengan skala kematangan (Energy, 2022).

Untuk mengukur kematangan, C2M2 menggunakan skala tingkat indikator kematangan, yang masing-masing mewakili atribut kematangan yang dijelaskan dalam struktur model C2M2 pada Gambar 2.6.



Gambar 2.6. Elemen Model dan Domain C2M2 (Energy, 2022)

Model C2M2 terdiri dari 10 domain yang masing-masing domain menggambarkan area penting dalam pengelolaan keamanan informasi. Di dalam setiap domain terdapat dua objektif/tujuan yaitu tujuan pendekatan (*approach objectives*) dan tujuan manajemen (*management objective*). *Approach objectives* merupakan tujuan pendekatan yang spesifik untuk setiap domain. Tujuan tersebut dikelompokan ke dalam tiga tingkat kematangan yang disebut MIL (*Maturity Indicator Level*)/ tingkat indikator kematangan dari MIL 1 - MIL 3 yang setiap tingkat menunjukan kemajuan praktik keamanan yang semakin matang dan di tiap praktiknya bersifat unik sesuai dengan kebutuhan domain tersebut. *Management objective* merupakan tujuan yang hanya ada satu per domain dan bersifat mirip di semua domain. Tujuan tersebut difokuskan pada pengelolaan dan penerapan berkelanjutan pada organisasi. Terdapat dua tingkat kematangan yang mendukung praktik pada tujuan manajemen yaitu MIL 2 dan MIL 3. Dengan struktur model di atas, model C2M2 tidak hanya menilai apa yang dilakukan oleh organisasi melalui *approach objective*, tapi menilai sejauh mana kegiatan pada organisasi terkelola dan menjadi budaya organisasi melalui *management objective*.

Analisis kesenjangan tingkat kematangan dalam penelitian ini merujuk pada konsep *Maturity Indicator Levels* (MILs) dalam model *Cybersecurity Capability Maturity Model* (C2M2). Kesenjangan kematangan dapat didefinisikan

sebagai selisih antara MIL saat ini (*current* MIL) dengan MIL yang ditargetkan (*target* MIL) berdasarkan strategi dan kebutuhan keamanan organisasi.

Strategi ini memungkinkan organisasi untuk lebih fokus dalam merancang program peningkatan keamanan yang terarah dan berbasis risiko. Tidak semua domain perlu mencapai MIL 3 prioritas peningkatan sebaiknya disesuaikan dengan tujuan bisnis, kapasitas sumber daya, serta biaya dan manfaat dari pencapaian setiap tingkat MIL. Analisis *gap* dalam teori kematangan sistem informasi, yang menjelaskan bahwa organisasi perlu mengevaluasi kapabilitas keamanan informasinya melalui tahapan bertingkat untuk mencapai performa optimal (IT Governance Institute, 2007). Pemetaan antara kondisi saat ini dan kondisi ideal menjadi kunci untuk merumuskan prioritas peningkatan keamanan informasi secara tepat dan terarah (Rabii dkk., 2020).