Perancangan Kriteria CSA Sektor Industri Energi berdasarkan CIS Control dan Peraturan Menteri BUMN

Melandy Andriawan[1)], Ira Rosianal Hikmah[2,*)], Tiyas Yulita[3)]

1) *Rekayasa Keamanan Siber, Keamanan Siber, Politeknik Siber dan Sandi Negara, melandy.andriawan@bssn.go.id*
2) *Rekayasa Keamanan Siber, Keamanan Siber, Politeknik Siber dan Sandi Negara, ira.rosianal@poltekssn.ac.id*
3) *Rekayasa Keamanan Siber, Keamanan Siber, Politeknik Siber dan Sandi Negara, tiyas.yulita@poltekssn.ac.id*

Riwayat Artikel

Dikirim 27 Mei 2025
Diterima 22 Agu 2025
Diterbitkan 31 Agu 2025

Kata kunci:

Sektor Industri Energi
Cyber Security Audit
NIST CSF
CIS *Controls*
PER 02-03/MBU/02/2018

Abstrak

Perkembangan teknologi digital di Indonesia tumbuh sangat pesat dan telah mendorong lonjakan pemanfaatan ruang siber. Dengan kemudahan akses serta fleksibilitasnya, ruang siber kini menjadi tulang punggung utama aktivitas di era modern. Tidak hanya digunakan masyarakat luas, ruang siber juga menopang berbagai sektor strategis nasional yang tergolong sebagai Infrastruktur Informasi Vital Nasional (IIVN), termasuk sektor industri energi. Namun, di balik peluang besar tersebut, ruang siber menyimpan berbagai kerentanan yang berpotensi menjadi celah serangan siber. Untuk menjawab tantangan ini, organisasi perlu menerapkan Cyber Security Audit (CSA) sebagai upaya evaluasi menyeluruh atas tingkat keamanan sistem yang mereka kelola. CSA dapat mengacu pada standar internasional, seperti NIST Cybersecurity Framework (CSF), CIS *Controls*, maupun COBIT. Dalam penelitian ini, NIST CSF dan CIS *Controls* dipilih karena memiliki struktur hierarkis yang jelas, terukur, serta mudah diimplementasikan. Lebih jauh, kedua standar tersebut diselaraskan dengan Peraturan Menteri BUMN Nomor PER-02/MBU/02/2018 dan PER-03/MBU/02/2018 sebagai landasan hukum pelaksanaan audit. Hasil dari proses harmonisasi ini melahirkan seperangkat 160 pertanyaan audit, yang dikelompokkan ke dalam empat domain utama: Identify (23 pertanyaan), Protect (90 pertanyaan), Detect (35 pertanyaan), dan Respond (12 pertanyaan).

Keywors:

Energy Industry Sector
Cyber Security Audit
NIST CSF
CIS Controls
PER 02-03/MBU/02/2018

Abstract

The rapid growth of digital technology in Indonesia has significantly accelerated the use of cyberspace. With its accessibility and flexibility, cyberspace has become the backbone of modern activities. Beyond serving the public, it also supports various national strategic sectors categorized as National Vital Information Infrastructure (NVII), including the energy industry sector. However, behind these vast opportunities, cyberspace contains vulnerabilities that can become entry points for cyberattacks. To address this challenge, organizations need to implement a Cyber Security Audit (CSA) as a comprehensive evaluation of their system security posture. CSA can refer to international standards such as the NIST Cybersecurity Framework (CSF), CIS Controls, and COBIT. This study specifically adopts NIST CSF and CIS Controls due to their clear hierarchical structures, measurability, and ease of implementation. Furthermore, both standards are harmonized with Minister of State-Owned Enterprises Regulation No. PER-02/MBU/02/2018 and PER-03/MBU/02/2018 as the legal basis for conducting the audit. The harmonization process resulted in a set of 160 audit

questions, classified into four main domains: Identify (23 questions), Protect (90 questions), Detect (35 questions), and Respond (12 questions).

1. PENDAHULUAN

Peningkatan jumlah pengguna teknologi informasi di tingkat global menunjukkan tren pertumbuhan yang konsisten setiap tahun, termasuk di Indonesia [1]. Fenomena ini diperkuat oleh optimalisasi pemanfaatan internet selama masa pandemi Covid-19, yang mendorong transformasi signifikan dalam keberlangsungan operasional bisnis. Pandemi menjadi katalisator percepatan digitalisasi di berbagai sektor strategis, seperti pemerintahan, ekonomi digital, dan Infrastruktur Informasi Vital Nasional (IIVN), di mana proses bisnis mengalami migrasi masif ke ruang siber [2]. Ruang siber sebagai entitas digital yang terbentuk melalui interkoneksi data, jaringan, perangkat komputasi, dan sistem informasi, merepresentasikan virtualisasi aktivitas masyarakat kontemporer. Meskipun menjadi tulang punggung transformasi digital, ruang siber mengandung kerentanan struktural yang berpotensi memicu ancaman multidimensi, termasuk serangan siber (*cyberattack*) [3]. Serangan siber merupakan gangguan sistematis yang berdampak transnasional, termasuk pada sektor-sektor kritis di Indonesia yang terklasifikasi dalam IIVN [4].

Sektor energi, sebagai salah satu komponen IIVN, memiliki tingkat eksposur tinggi terhadap risiko serangan siber. Kerentanan ini bersumber pada peran infrastruktur energi sebagai *backbone* perekonomian, di mana ketergantungan terhadap sistem distribusi berbasis teknologi menuntut presisi keseimbangan antara produksi dan konsumsi energi. Adanya gangguan siber pada proses bisnis sektor ini dapat mengakibatkan disrupsi distribusi energi, mengingat kapasitas penyimpanan energi skala besar bersifat terbatas. Lebih lanjut, kegagalan operasional infrastruktur energi berpotensi menimbulkan efek domino (*spillover effect*) pada seluruh sektor dependen, baik domestik maupun global [5].

Untuk memitigasi dampak negatif serangan siber, diperlukan implementasi langkah-langkah sistematis, salah satunya melalui evaluasi kesesuaian sistem dan proses bisnis organisasi terhadap standar keamanan siber minimum. Mekanisme evaluasi ini secara formal dikenal sebagai audit keamanan siber atau Cyber Security Audit (CSA), yang berfungsi mengidentifikasi celah keamanan berbasis kriteria terstandardisasi [6]. CSA memerlukan kerangka atau kriteria pengauditan, sehingga dirasa perlu terdapat penelitian yang memiliki hasil berupa penyusunan kriteria CSA di berbagai sektor. Penelitian terdahulu telah merumuskan kriteria CSA pada sektor perbankan [7] dan pemerintahan [8]. Keberadaan sektor industri beserta dengan kerawanannya atas serangan siber merupakan peluang atas penelitian ini atas penyusunan kriteria CSA untuk sektor industri energi.

Kriteria CSA harus dikembangkan berdasarkan kerangka keamanan siber yang diakui secara internasional, seperti National Institute of Standards and Technology Cybersecurity Framework *Core* (NIST CSF-*Core*) dan Center for Internet Security *Controls* (CIS *Controls*). NIST CSF-*Core* dipilih sebagai basis penelitian karena memiliki tiga keunggulan utama: (1) struktur hierarkis yang terintegrasi, (2) kompatibilitas dengan standar internasional melalui *Informative Reference* (termasuk CIS CSC, ISO/IEC 27001, dan NIST SP.800-53), serta (3) kemudahan adaptasi ke berbagai konteks organisasi [9]. Sementara itu, CIS *Controls* menyediakan rekomendasi teknis operasional yang bersifat *actionable* untuk implementasi *best practice* keamanan siber [10].

Dalam pelaksanaannya, kriteria CSA juga memerlukan profil risiko atau dasar hukum yang berupa mandat atas pelaksanaan audit, sehingga audit dapat dilaksanakan dengan parameter yang jelas. Perusahaan energi di Indonesia, terutama yang berada di bawah Kementerian Badan Usaha Milik Negara (BUMN) antara lain PT. Perusahaan Gas Negara (PGN), PT. Pertamina, dan PT. Perusahaan Listrik Negara (PLN) [11]. Perusahaan tersebut masuk dalam cakupan IIVN di Indonesia. Pada Kementerian BUMN, terdapat regulasi terkait prinsip tata kelola teknologi informasi, yang disusun dalam Peraturan Menteri BUMN Nomor PER-02/MBU/02/2018 dan PER-03/MBU/02/2018 (Permen BUMN No. 02 dan 03 Tahun 2018). Regulasi tersebut menekankan prinsip Good Information Technology Governance (GIG) melalui pengelolaan TI yang terkoordinasi

dan terukur [12], sekaligus menjadi landasan hukum pelaksanaan audit siber. Urgensi ini semakin mengemuka menyusul insiden kebocoran data pelanggan PT PLN [13] yang mengindikasikan kerentanan sistemik di sektor energi.

Berdasarkan hal tersebut, maka penelitian ini bertujuan merumuskan kriteria CSA khusus sektor energi melalui integrasi tiga komponen, yaitu pemetaan fungsi NIST CSF-*Core* sebagai kerangka konseptual, korelasi dengan CIS *Controls* v8 untuk aspek teknis operasional, dan harmonisasi dengan Permen BUMN Nomor 02 Tahun 2018 sebagai basis legal. Kriteria ini diharapkan menjadi instrumen audit komprehensif yang menjawab tantangan *cyber resilience* di sektor energi Indonesia.

2. LANDASAN TEORI

2.1. *Cyber Security Audit*

Audit didefinisikan sebagai proses sistematis untuk menilai kesesuaian sistem atau proses bisnis suatu organisasi terhadap batas kelayakan minimum atau standar yang ditetapkan [6]. Standar ISO 19011-2018 merumuskan tahapan audit dalam sembilan fase yaitu: [14]

a. Penetapan tujuan program audit
b. Identifikasi dan evaluasi risiko serta peluang program audit
c. Perancangan program audit
d. Implementasi program audit
e. Pemantauan program audit
f. Penyelesaian audit
g. Persiapan dan pendistribusian laporan audit
h. Implementasi tindak lanjut audit
i. Peninjauan dan peningkatan program audit

Penelitian ini mengkhususkan sasaran audit pada sektor industri energi dengan mengadopsi Permen BUMN Nomor 02 Tahun 2018 sebagai basis evaluasi risiko dan peluang. Fokus pengembangan terbatas pada perumusan kriteria audit—komponen esensial dalam program audit yang berfungsi sebagai parameter penilaian pemenuhan persyaratan audit [6]. CSA merupakan instrumen evaluasi komprehensif untuk mengukur kapabilitas keamanan siber suatu organisasi melalui *benchmarking* terhadap standar yang relevan. Program ini dirancang untuk menguji kemampuan organisasi dalam deteksi, pencegahan, dan respons terhadap kerentanan, ancaman, atau serangan siber yang berpotensi mengganggu kontinuitas bisnis; menghasilkan rekomendasi implementatif (teknis dan manajerial) untuk peningkatan *cyber resilience*, serta menyediakan basis empiris bagi penyusunan kebijakan keamanan siber berbasis risiko [15].

2.2. NIST CSF (*Cyber Security Framework*)

Kerangka Kerja Keamanan Siber NIST (NIST CSF) terdiri atas tiga komponen utama, yaitu NIST CSF *Core*, *Implementation Tiers*, dan *Profiles*. Komponen inti (*Core*) dari NIST CSF merupakan bagian fundamental yang mendefinisikan serangkaian aktivitas, hasil, dan referensi yang berkaitan dengan aspek-aspek utama keamanan siber. NIST CSF sendiri merupakan kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST) sebagai pedoman praktik terbaik (*best practices*) dalam pengelolaan keamanan siber. Tujuan utama dari kerangka ini adalah untuk membantu organisasi dalam membangun, meningkatkan, dan mempertahankan strategi keamanan siber yang efektif dan adaptif terhadap berbagai ancaman. Kerangka ini juga memberikan panduan terstruktur terkait dengan lima fungsi utama dalam siklus manajemen keamanan siber, yaitu: Identifikasi (*Identify*), Perlindungan (*Protect*), Deteksi (*Detect*), Respons (*Respond*), dan Pemulihan (*Recover*), yang mencakup seluruh spektrum respons terhadap insiden keamanan siber [9].

2.3. CIS *Controls*

CIS menyediakan seperangkat standar dan pedoman keamanan siber yang terstruktur, yang dirancang untuk membantu organisasi dalam meningkatkan postur keamanan sibernya sesuai dengan praktik terbaik (*best practices*) yang telah terbukti [10]. CIS *Controls* dirancang agar dapat diimplementasikan secara praktis oleh berbagai jenis organisasi, baik skala besar maupun kecil, dengan tujuan utama untuk mengurangi risiko dan mencegah sebagian besar jenis serangan siber [10]. CIS *Controls* versi 8 (CIS *Controls* v8) terdiri atas 18 kontrol utama yang dirinci lebih lanjut menjadi 153 sub-kontrol. Dalam konteks penelitian ini, pemetaan antara CIS *Controls* dan NIST CSF – *Core* dilakukan pada tingkat sub-kontrol, karena tingkat perincian ini memungkinkan pemetaan yang lebih akurat terhadap fungsi-fungsi spesifik dalam kerangka kerja NIST CSF. Setiap fungsi dalam NIST CSF dapat dikaitkan dengan sejumlah kontrol, yang kemudian dijabarkan lebih detail dalam bentuk sub-kontrol. CIS *Controls* v8 mengelompokkan kontrol ke dalam tiga kategori utama, yaitu: Basic *Controls* – terdiri atas enam kontrol awal yang dianggap esensial untuk membangun fondasi keamanan; Foundational *Controls* – mencakup delapan kontrol yang mendukung penerapan keamanan yang lebih mendalam; dan Organizational *Controls* – terdiri dari empat kontrol yang berfokus pada kebijakan, manajemen risiko, dan pengembangan sumber daya manusia dalam keamanan siber.

3. METODE PENELITIAN

3.1. Objek Penelitian

Pada penelitian ini, dilakukan perancangan dan penyusunan kriteria CSA yang dapat dimanfaatkan di sektor industri energi dibawah Kementerian BUMN. Perancangan dan penyusunan kriteria CSA dilakukan menggunakan NIST CSF - *Core* yang dikombinasikan dengan kontrol pada CIS *Controls* v8 dan berdasarkan pada Permen BUMN Nomor 02 dan 03 Tahun 2018.

3.2. Jenis Penelitian

Pada penelitian ini, terdapat pengolahan penelitian dengan metode penelitian kualitatif deskriptif. Metode ini diimplementasikan dengan mengamati aktivitas berdasarkan data valid yang sesuai dengan kondisi yang sebenarnya. Data yang digunakan pada penelitian ini direpresentasikan dalam bentuk kalimat, tabel maupun gambar. Teknik pengambilan data pada penelitian ini adalah dengan metode kajian pustaka. Metode ini dipraktikan melalui pengumpulan serta pengkajian referensi penelitian seperti artikel dan dokumen yang berkorelasi dengan penelitian.

3.3. Desain Penelitian

Tahapan penelitian ini adalah sebagai berikut:

a. Studi Literatur

Proses ini dilakukan melalui serangkaian tahapan yang meliputi pencarian, pengumpulan, dan analisis terhadap berbagai referensi yang relevan dengan topik penelitian. Kegiatan studi literatur ini bertujuan untuk memperoleh pemahaman yang komprehensif mengenai konsep keamanan siber, ruang lingkup dan tantangan yang dihadapi, serta strategi mitigasi terhadap potensi ancaman yang mungkin terjadi. Selain itu, dilakukan pula penelaahan terhadap konsep audit keamanan siber, termasuk proses pembentukannya, parameter yang harus dipenuhi, serta standar yang dapat dijadikan acuan dalam pelaksanaannya. Studi literatur yang dilakukan dalam penelitian ini secara khusus difokuskan pada beberapa sumber utama, yaitu: konsep dan praktik dalam *cybersecurity*, CSA, kerangka kerja NIST CSF, CIS *Controls* v8, serta regulasi nasional yang relevan, khususnya Permen BUMN Nomor 02 Tahun 2018. Fokus ini dipilih untuk memastikan bahwa pembentukan model audit keamanan siber yang diusulkan selaras dengan praktik internasional dan regulasi yang berlaku di Indonesia.

b. Pengumpulan Data

Tahap pengumpulan data bertujuan untuk memperoleh informasi yang relevan dan mendalam sebagai dasar dalam penyusunan penelitian. Informasi yang dikumpulkan mencakup berbagai aspek penting, antara lain: urgensi implementasi CSA dalam sektor industri energi, metode pemilihan kontrol yang tepat, pemetaan hubungan antara dokumen pra-penelitian, klasifikasi kontrol berdasarkan karakteristik dan fungsinya, serta identifikasi parameter yang digunakan dalam perumusan kriteria dan penyusunan pertanyaan yang sesuai untuk mendukung penelitian di bidang CSA.

c. Analisis Data

Tahap analisis data dilakukan untuk mengolah informasi yang telah diperoleh sebelumnya, dengan tujuan menyusun kriteria dan pertanyaan yang relevan untuk CSA. Analisis ini difokuskan pada penyusunan pemetaan yang sistematis dan komprehensif antara kerangka kerja NIST CSF, CIS *Controls* v8, serta Permen BUMN Nomor 02 Tahun 2018, yang menjadi acuan dalam pengelolaan teknologi informasi di lingkungan Kementerian BUMN. Hasil dari tahap ini diharapkan dapat digunakan sebagai dasar dalam pembentukan kriteria CSA dan perumusan pertanyaan audit yang sesuai dengan konteks organisasi dan regulasi yang berlaku.

d. Validasi

Validasi bertujuan untuk mengukur validitas dari isi penelitian, baik dari tahapan penelitian, pemetaan yang dilakukan, maupun hasil dari penelitian ini yaitu kriteria keamanan siber dan pertanyaan. Pengujian ini dilakukan oleh pakar atau *expert judgement* [16] yang bersesuaian dengan topik penelitian dari pemohon validasi, yang pada kesempatan ini terkait audit keamanan siber dan merupakan perwakilan auditor dari ISACA Indonesia *Chapter*, yang memiliki jabatan selaku *Government and Regulatory Advocacy Director*.

4. HASIL DAN PEMBAHASAN

4.1. Identifikasi Dokumen

Tahap identifikasi dokumen dilakukan untuk memastikan bahwa seluruh dokumen yang digunakan dalam proses penelitian dapat dikenali dan dianalisis secara sistematis melalui metode penelaahan dokumen (*document review*). Dalam penelitian ini, Peraturan Menteri BUMN Nomor 02 dan 03 Tahun 2018 dijadikan sebagai acuan utama dalam menilai standar pengelolaan teknologi informasi pada BUMN, termasuk yang bergerak di sektor industri energi.

4.2. Analisis Dokumen

Tahap analisis dokumen dilakukan melalui proses membaca, memahami, dan memetakan isi dari masing-masing kontrol yang terdapat dalam dokumen yang dianalisis. Tujuan dari tahap ini adalah untuk menyusun kriteria keamanan siber yang sistematis dan relevan. Hasil analisis kemudian disajikan dalam bentuk tabel, yang dilengkapi dengan pengkodean khusus. Teknik pengkodean diterapkan guna membedakan setiap kontrol berdasarkan sumber dokumennya serta untuk mempermudah proses perancangan kriteria audit. Setiap kontrol diberikan kode unik, yang berfungsi sebagai identifikasi sekaligus sebagai acuan dalam penyusunan dan pemetaan kriteria audit keamanan siber secara efisien dan terstruktur.

a. NIST CSF

NIST CSF merupakan standar atau pedoman praktik terbaik dalam keamanan siber yang dikembangkan oleh NIST. Kerangka kerja ini dirancang untuk membantu organisasi dalam mengembangkan, meningkatkan, serta memelihara strategi keamanan siber secara efektif. Selain itu, NIST CSF juga memberikan rekomendasi mengenai proses pendeteksian, respons, dan pemulihan terhadap insiden keamanan.

NIST CSF terdiri dari tiga komponen utama, yaitu inti kerangka kerja (NIST CSF - *Core*), *Implementation Tiers*, dan *Profiles*. *Core* merujuk pada serangkaian aktivitas dan hasil yang terkait dengan penerapan keamanan siber. Sedangkan *Profile* bersifat adaptif dan bervariasi

antar organisasi, disesuaikan dengan tantangan, kebutuhan, serta peluang yang spesifik, guna mencapai tujuan keamanan yang berbeda sesuai konteks masing-masing organisasi [17]. Sementara itu, *Implementation Tiers* mengindikasikan tingkat pengelolaan setiap elemen standar oleh organisasi. Penentuan tingkatan ini tidak semata didasarkan pada kematangan sistem, melainkan pada tingkat kebutuhan dan penerimaan yang sesuai untuk setiap elemen dalam konteks organisasi tersebut.

Pada NIST CSF - *Core*, terdapat lima fungsi utama, yaitu: *Identify* (ID), *Protect* (PR), *Detect* (DE), *Respond* (RS), dan *Recover* (RC) [9]. Setiap fungsi terdiri atas tiga elemen, yaitu *Categories*, *Subcategories*, dan *Informative References*. Secara hierarkis, di bawah level fungsi terdapat 23 kategori yang spesifik untuk masing-masing fungsi. Selanjutnya, setiap kategori terbagi menjadi subkategori, yang berjumlah 108 secara keseluruhan. Subkategori-subkategori ini dapat diintegrasikan dengan standar lain, dengan keterikatan yang dijelaskan melalui *informative references*.

b. CIS *Control*s v8

CIS *Controls* v8 tersusun dari lima *Security Function*, 18 *Controls*, 153 *Sub-Controls* [10]. Pada Tabel 1 ditunjukan perincian nama kontrol dan jumlah *Sub-control*s pada CIS *Controls* v8.

Tabel 1. Rincian *Controls* dan jumlah *Sub-Controls* pada CIS *Controls* v8 [10]

No	***Controls***	**Jumlah *Subcontrol***
1	*Control 1: Inventory and control of enterprise assets*	5
2	*Control 2: Inventory and control of software assets*	7
3	*Control 3: Data Protection*	14
4	*Control 4: Secure Configuration of enterprise assets and software*	12
5	*Control 5: Account Management*	6
6	*Control 6: Access Control Management*	8
7	*Control 7: Continous vulnerability management*	7
8	*Control 8: Audit Log Management*	12
9	*Control 9: Email and Web Browser Protections*	7
10	*Control 10: Malware Defenses*	7
11	*Control 11: Data Recovery*	5
12	*Control 12: Network Infrastructure management*	8
13	*Control 13: Network Monitoring and Defense*	11
14	*Control 14: Security Awareness and Skills Training*	9
15	*Control 15: Service Provider Management*	7
16	*Control 16: Application software security*	14
17	*Control 17: Incident response management*	9
18	*Control 18: Penetration testing*	5

c. Peraturan Menteri BUMN

Permen BUMN Nomor 02 dan 03 Tahun 2018 merupakan regulasi yang diterbitkan oleh BUMN terkait dengan Prinsip Tata Kelola Teknologi Informasi (TI) serta Panduan Penyusunan Pengelolaan TI di lingkungan BUMN. Peraturan ini terdiri dari satu bab yang memuat tujuh pasal dan dilengkapi dengan dua lampiran [12]. Dalam penelitian ini, pengkodean pada poin-poin dalam Permen BUMN Nomor 02 dan 03 Tahun 2018 dilakukan melalui singkatan sub-bagian yang terdapat pada lampiran peraturan tersebut. Selain itu, digunakan pula singkatan istilah yang terdapat dalam peraturan, seperti PM-KP, yang merujuk pada Prinsip-prinsip Tata Kelola TI yang wajib dipatuhi oleh seluruh unit kerja di bawah naungan Kementerian BUMN. Kepatuhan seluruh unit kerja terhadap prinsip-prinsip tersebut akan menjamin tersedianya

informasi yang berkualitas, konsisten, dan terukur, sehingga mendukung pengambilan keputusan yang efektif dan tepat di tingkat manajemen.

4.3. Pemetaan

Pada tahap pemetaan, elemen-elemen yang diperoleh dari dokumen hasil analisis sebelumnya dilakukan pemetaan berdasarkan tingkat keterkaitan antar elemen tersebut. Contohnya, pada pemetaan pertama, dua standar yang digunakan, yaitu CIS *Controls* v8 dan NIST CSF – *Core*, dipetakan berdasarkan keterkaitan yang terdapat pada bagian *Informative Reference* dalam NIST CSF – *Core*. Sedangkan pada pemetaan kedua, keterkaitan antardokumen didasarkan pada kesamaan kata kunci yang ditemukan.

a. Pemetaan CIS *Controls* v8 terhadap NIST CSF – *Core*

Pemetaan pertama dilakukan dengan mengidentifikasi sub-kontrol CIS *Controls* yang sesuai dengan *Informative References* dalam NIST CSF – *Core*. Dari total 153 sub-kontrol CIS, sebanyak 124 sub-kontrol berhasil dipetakan terhadap 66 dari 108 sub-kategori yang terdapat dalam NIST CSF – *Core*. Contoh hasil pemetaan CIS *Controls* v8 dapat dilihat pada Tabel 2.

Tabel 2. Contoh Hasil Pemetaan CIS *Controls* v8 Terhadap NIST CSF- *Core*

No	Subkategori *Framework Core*	*Sub-Controls* CIS v8	Deskripsi
1	ID.AM-1	*Control*-1.1	Menetapkan dan Memelihara Inventaris Aset Terperinci
2	ID.AM-2	*Control*-2.1	Membangun dan Memelihara Inventaris Perangkat Lunak
		Control-2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung
		Control-16.4	Menetapkan dan Mengelola Inventaris Komponen Perangkat Lunak Pihak Ketiga
3	ID.AM-3	*Control*-3.8	Aliran Data Dokumen
4	ID.AM-4	*Control*-12.4	Membangun dan Memelihara Diagram Arsitektur
5	ID.AM-5	*Control*-3.2	Membangun dan Memelihara Inventarisasi Data
		Control-3.7	Menetapkan dan Memelihara Skema Klasifikasi Data
6	ID.AM-6	*Control*-14.1	Membangun dan Memelihara Program Kesadaran Keamanan
7	ID.GV-1	*Control*-14.1	Membangun dan Memelihara Program Kesadaran Keamanan
8	ID.GV-2	*Control*-15.2	Menetapkan dan Memelihara Kebijakan Manajemen Penyedia Layanan
		Control-17.4	Tetapkan dan Pertahankan Proses Respons Insiden
9	ID.RA-1	*Control*-7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan
		Control-7.2	Menetapkan dan mempertahankan Proses Remediasi
		Control-7.4	Lakukan Manajemen Patch Aplikasi Otomatis
10	ID.RA-5	*Control*-3.7	Menetapkan dan Memelihara Skema Klasifikasi Data
		Control-7.6	Lakukan Pemindaian Kerentanan Otomatis dari Aset Perusahaan yang Terekspos Secara Eksternal

b. Permen BUMN Nomor 02 dan 03 Tahun 2018 terhadap NIST CSF – *Core*

Pemetaan kedua dimulai dengan melakukan pemetaan Permen BUMN Nomor 02 Tahun 2018 terhadap NIST CSF – *Core*. Hasil pemetaan ini menunjukkan bahwa dari 71 kontrol yang tercantum dalam peraturan tersebut, hanya 24 kontrol yang berhasil dipetakan ke dalam 63 dari 66 sub-kategori NIST CSF – *Core* yang telah diidentifikasi pada pemetaan pertama. Contoh daftar kontrol Permen BUMN Nomor 02 Tahun 2018 yang terpetakan terhadap NIST CSF – *Core* disajikan pada Tabel 3, yang mencakup kolom nomor, bagian, sub-bagian, deskripsi, dan

pengkodean. Selanjutnya, Tabel 4 menampilkan contoh hasil pemetaan lengkap antara Permen BUMN Nomor 02 dan 03 Tahun 2018 dengan NIST CSF – *Core*.

Tabel 3. Contoh daftar kontrol dari PER 02-03/MBU/02/2018 yang telah dikodifikasi

No.	Bagian	Sub Bagian	Deskripsi	Pengkodean
1	Prinsip Manajemen	Keberhasilan penerapan TI merupakan hasil kontribusi seluruh unit kerja di Kementerian BUMN	Seluruh unit kerja Kementerian BUMN terkait harus berkontribusi dalam proses pengambilan keputusan strategis TI, serta berperan aktif dalam pemanfaatan TI dalam mendukung tercapainya strategi bisnis dan sesuai dengan skala prioritas bisnis.	PM-KT
2	Prinsip Manajemen	Menjaga keberlangsungan kegiatan operasional Kementerian BUMN	Seluruh unit kerja di Kementerian BUMN bertanggung jawab untuk menjaga keberlangsungan kegiatan Kementerian BUMN agar tetap berjalan, walaupun terjadi gangguan atau bencana yang mempengaruhi TI. Penerapan TI untuk mendukung seluruh kegiatan Kementerian BUMN	PM-MK
3	Prinsip Data dan Informasi	Menteri BUMN merupakan pengguna utama Data dan Informasi	Pengguna utama Data dan Informasi di Kementerian BUMN adalah Menteri BUMN. Sedangkan pengguna lainnya ditentukan berdasarkan tingkat otoritas dalam melaksanakan tugas dan fungsinya	PD-PU

Tabel 4. Contoh hasil pemetaan PER 02-03/MBU/02/2018 terhadap NIST CSF- *Core*

No	Kategori	Subkategori *Framework Core*	Deskripsi	PERATURAN NOMOR PER 02-03/MBU/02/2018
1	Asset Management	ID.AM-1	Perangkat dan sistem fisik dalam organisasi diinventarisasi	PT-IB
2		ID.AM-2	Platform perangkat lunak dan aplikasi dalam organisasi diinventarisasi	KS-PS3
3		ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	KS-PS2
4		ID.AM-4	Sistem informasi eksternal dikatalogkan	KO-PL4
5		ID.AM-5	Sumber daya (misalnya, perangkat keras, perangkat, data, waktu, personel, dan perangkat lunak) diprioritaskan berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya	KO-PS
6		ID.AM-6	Peran dan tanggung jawab keamanan siber untuk seluruh tenaga kerja dan pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, mitra) ditetapkan	KO-PK

Setelah pelaksanaan dua pemetaan atas semua dokumen, didapatkan hasil berupa kriteria CSA organisasi sektor industri energi. Kriteria CSA yang telah dihasilkan selanjutnya digunakan menjadi bahan pembuatan pertanyaan audit. Pada Tabel 5 disajikan contoh kriteria CSA dengan kolom NIST CSF, Deskripsi, Kontrol pada Permen BUMN Nomor 02 dan 03 Tahun 2018, CIS *Controls* v8, dan Deskripsi.

Tabel 5. Contoh kriteria *Cyber Security Audit*

No	Fungsi	Kategori	Subkategori *Framework Core*	Deskripsi NIST CSF-*Core*	PER 02-03/MBU/02/2018	*Sub-Controls* CIS v8	kriteria *Cyber Security Audit*
1	**ID**	Asset Management	ID.AM-1	Perangkat dan sistem fisik dalam organisasi diinventarisasi	PT-IB	*Control*-1.1	Menetapkan dan Memelihara Inventaris Aset Terperinci
2			ID.AM-2	Platform perangkat lunak dan aplikasi dalam organisasi diinventarisasi	KS-PS3	*Control*-2.1	Membangun dan Memelihara Inventaris Perangkat Lunak
3						*Control*-2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung
4						*Control*-16.4	Mengelola Inventaris Komponen Perangkat Lunak Pihak Ketiga

4.4. Penyusunan Daftar Pertanyaan

Pada tahap penyusunan, hasil dari pemetaan pertama dan kedua dikonversi menjadi kriteria CSA yang kemudian disesuaikan menjadi pertanyaan audit. Pertanyaan-pertanyaan ini dirancang untuk mengevaluasi kesesuaian kondisi atau tingkat keamanan siber suatu organisasi. Penyusunan pertanyaan dilakukan berdasarkan sub-kontrol dari CIS *Controls* v8 yang telah ditetapkan sebelumnya. Setelah dirumuskan, pertanyaan-pertanyaan tersebut dikelompokkan sesuai dengan fungsi-fungsi yang terdapat dalam NIST CSF – *Core*. Pengelompokan ini bertujuan untuk memudahkan auditor dalam mengurutkan pertanyaan berdasarkan fungsi, sekaligus membuat dokumen audit menjadi lebih terstruktur dan sistematis. Contoh hasil penyusunan pertanyaan dapat dilihat pada Tabel 6, yang memuat kolom nomor, kategori, dan pertanyaan. Beberapa bagian dari pemetaan yang tidak lolos seleksi, dikarenakan adanya kesamaan jenis dan bentuk kontrol.

Tabel 6. Contoh hasil penyusunan pertanyaan

No	Kategori	Pertanyaan
1	*Identify - Asset Management*	Apakah perusahaan Anda sudah menetapkan dan memelihara inventaris aset secara terperinci?
2		Apakah perusahaan Anda sudah membangun dan memelihara inventaris perangkat lunak?
3		Apakah lunak yang ada pada perusahaan Anda mendukung kinerja satu sama lain?
4		Apakah perusahaan Anda sudah menetapkan dan memelihara komponen perangkat lunak pihak ketiga?
5		Apakah di perusahaan Anda terdapat skema terkait aliran data, informasi maupun dokumen?
6		Apakah di perusahaan Anda terdapat diagram arsitektur jaringan yang terperinci?
7		Apakah perusahaan Anda sudah membangun dan memelihara inventaris data?
8		Apakah di perusahaan Anda sudah melakukan klasifikasi penggunaan data?
9		Apakah pihak manajemen perusahaan Anda sudah menginformasikan terkait siapa saja yang bertugas untuk melakukan pengamanan informasi di perusahaan Anda?

Pada pertanyaan yang sudah dibuat selanjutnya memiliki kategorisasi jawaban, dimana terdapat empat opsi jenis jawaban yang penyusunannya disesuaikan dengan Systems Security Engineering-Capability Maturity Model (SSE-CMM). Penjelasan lebih lanjut dari kategorisasi jawaban dari pertanyaan audit adalah sebagai berikut:

a. Kategori 1

Kategori yang pertama merupakan jawaban dengan pertanyaan yang kemungkinan jawabannya terkait dengan periode kegiatan yang idealnya dilaksanakan berkelanjutan. Sehingga jawaban yang diharapkan adalah "dilakukan berkala", "kadang-kadang" atau "tidak dilakukan". Tabel penilaian kategori 1 berdasarkan SSE-CMM dapat dilihat pada Tabel 7.

Tabel 7. Penilaian Jawaban Kategori 1

No.	Jawaban/Opsi	Nilai
1	Ya, dilakukan secara berkelanjutan setidaknya setahun sekali	5
2	-	-
3	Ya, namun tidak dilakukan secara berkelanjutan/Kadang-kadang	3
4	-	-
5	Tidak	1

b. Kategori 2

Kategori kedua merupakan jawaban atas pertanyaan yang dijawab sebagai "YA" atau "TIDAK". Pertanyaan yang memungkinkan untuk jawaban seperti ini adalah pertanyaan terkait penetapan atau pendefinisian Tabel penilaian kategori 2 SSE-CMM ada pada Tabel 8.

Tabel 8. Penilaian Jawaban Kategori 2

No.	Jawaban/Opsi	Nilai
1	Ya	5
2	-	-
3	-	-
4	-	-
5	Tidak	1

c. Kategori 3

Kategori ketiga dari jawaban adalah untuk pertanyaan yang memepertanyakan terkait keberadaan pembaruan hal yang berada dalam organisasi, apakah dilaksanakan dalam waktu tertentu atau tidak. Pembaruan yang dimaksud bisa berupa sistem, sumber daya, atau perangkat. Tabel penilaian kategori 3 berdasarkan SSE-CMM ada pada Tabel 9.

Tabel 9. Penilaian Jawaban Kategori 3

No.	Jawaban/Opsi	Nilai
1	Ada, dan diperbaharui setiap ada perubahan	5
2	Ada, diperbaharui setiap 3 bulan	4
3	Ada, diperbaharui setiap tahun	3
4	Ada, jarang diperbaharui	2
5	Tidak ada/tidak lengkap	1

d. Kategori 4

Kategori keempat dari jenis jawaban adalah kategori jawaban atas pertanyaan yang menanyakan pemerataan pelaksanaan tindakan dalam organisasi, biasanya ditandai dengan kata keseluruhan atau sebagian. Tabel penilaian kategori 4 berdasarkan SSE-CMM ada pada Tabel 10.

Tabel 10 Penilaian Kategori Jawaban 4

No.	Jawaban/Opsi	Nilai
1	Ya, sudah keseluruhan	5
2	-	-
3	Ya, sudah sebagian	3
4	-	-
5	Tidak	1

4.5. Validasi

Validasi adalah tahapan akhir pada penelitian ini. Validasi kriteria CSA yang di hasilkan ditinjau dari segi proses pembuatan dan urutan kesesuaian tingkat kontrol secara hierarki dilakukan oleh pakar keamanan siber khususnya di sektor audit keamanan siber, yang dalam hal ini adalah Bapak David Wungkana selaku perwakilan Auditor ISACA Indonesia *Chapter*. Validasi ini bertujuan untuk memastikan bahwa kriteria dan pertanyaan CSA yang telah dibuat sesuai jika dilihat dari tahap pembuatan hingga tahap penyelesaian dan dapat diterapkan.

5. KESIMPULAN

Perancangan kriteria dilakukan dengan cara memetakan kontrol terpilih dari setiap dokumen yang menghasilkan kriteria yang tersusun atas 63 kontrol NIST CSF, 116 kontrol CIS *Controls* v8, dan 24 kontrol Permen BUMN Nomor 02 dan 03 Tahun 2018. Rancangan kriteria yang selanjutnya disusun menjadi pertanyaan yang kemudian divalidasikan kepada praktisi audit keamanan siber yaitu perwakilan auditor dari ISACA Indonesia *Chapter*. Proses tersebut menghasilkan 160 pertanyaan yang terdiri dari *Identify* (23 pertanyaan), *Protect* (90 pertanyaan), *Detect* (35 Pertanyaan), dan *Respond* (12 Pertanyaan).

Perancangan kriteria CSA ini berhasil karena menggabungkan rigor metodologis (standar internasional), kepatuhan regulasi lokal, serta validasi praktisi. Untuk menghasilkan instrumen audit yang terukur, dapat ditindaklanjuti, dan memiliki legitimasi. Keberhasilan tersebut bukan semata jumlah kontrol atau pertanyaan, melainkan tercapainya *operational readiness*: kontrol yang sebelumnya abstrak sekarang menjadi *checklist* audit yang jelas dan diterima oleh pemangku kepentingan. Oleh karena itu, kriteria ini siap menjadi fondasi CSA yang efektif untuk menjaga ketahanan siber sektor energi.

REFERENSI

[1] Asosiasi Penyelenggara Jasa Internet Indonesia(APJII), "Profil Internet Indonesia 2022," Jakarta, Jun. 2022. Accessed: Aug. 19, 2022. [Online]. Available: https://apjii.or.id/content/read/39/559/Laporan-Survei-Profil-Internet-Indonesia-2022

[2] BSSN, "Laporan Tahunan 2021 Honeynet Project BSSN-IHP," Jakarta, Apr. 2022. Accessed: Aug. 19, 2022. [Online]. Available: https://bssn.go.id/laporan-tahunan-honeynet-project-tahun-2021-upaya-bssn-menyedikan-literasi-terkini-memacu-masyarakat-bersinergi-menciptakan-ranah-siber-indonesia-yang-aman-dan-tahan-terhadap-serangan-siber/

[3] Kementerian Pertahanan Republik Indonesia, *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber*. Jakarta, 2014. Accessed: Aug. 19, 2022. [Online]. Available: https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf

[4] Presiden Republik Indonesia, *Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 Tentang Perlindungan Infrastruktur Informasi Vital*. Jakarta, 2022. Accessed: Aug. 19, 2022. [Online]. Available: https://jdih.setkab.go.id/PUUdoc/176752/Salinan_Perpres_Nomor_82_Tahun_2022.pdf

[5] F. A. Shaikh, M. S. Alam, M. S. J. Asghar, and F. Ahmad, "Blackout Mitigation of Voltage Stability Constrained Transmission Corridors through Controlled Series Resistors," *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, vol. 11, no. 1, Nov. 2017, doi: 10.2174/2352096510666171108160930.

[6] ISACA, *CISA Review Manual 27th Edition*, vol. 27. 2019. Accessed: Aug. 19, 2022. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KokCEAS

[7] Fajar Sofar, "Perancangan Kriteria Cyber Security Audit untuk Sektor Perbankan menggunakan NIST CSF dan CIS *Controls* v8 Sesuai dengan Peraturan OJK Nomor 38/POJK.03/2016 (Studi Kasus: Bank BNI)," Politeknik Siber dan Sandi Negara,

Bogor, 2021.

[8] M. Daffi Alhafizh, "Perancangan Kriteria Cyber Security Audit Berdasarkan NIST CSF dan COBIT 5 (Studi Kasus : Badan Pengusahaan Batam)," Politeknik Siber dan Sandi Negara, Bogor, 2021.

[9] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[10] Center for Internet Security (CIS), "CIS *Controls* CIS *Controls* Version 8," Oct. 06, 2021 [Online]. Available: www.cisecurity.org/*Controls*/

[11] "Kementerian Badan Usaha Milik Negara." https://bumn.go.id/portfolio/cluster (accessed Dec. 23, 2021).

[12] Kementerian Badan Usaha Milik Negara Republik Indonesia, *Peraturan Menteri Badan Usaha Milik Negara Republik Indonesia Nomor Per 02-03/MBU/02/2018 Tentang Prinsip Tata Kelola Teknologi Informasi Kementerian Badan Usaha Milik Negara*. 2018.

[13] A. M. Karunia, "PLN Gandeng Kominfo dan BSSN dalam Investigasi Dugaan Kebocoran Data Pelanggan," Aug. 20, 2022. https://money.kompas.com/read/2022/08/20/204817326/pln-gandeng-kominfo-dan-bssn-dalam-investigasi-dugaan-kebocoran-data-pelanggan (accessed Aug. 21, 2022).

[14] International Standard Organization, "ISO 19011:2018 'Guidelines for auditing management systems,'" Jul. 2018 Accessed: Aug. 19, 2022. [Online]. Available: https://www.iso.org/standard/70017.html

[15] ISACA, *IT Audit Framework (ITAF ™) Professional Practices Framework for IT Audit 4 th Edition*. 2020. [Online]. Available: www.isaca.org

[16] A. R. Colson and R. M. Cooke, "Expert elicitation: Using the classical model to validate experts' judgments," *Rev Environ Econ Policy*, vol. 12, no. 1, pp. 113–132, Feb. 2018, doi: 10.1093/reep/rex022.

[17] 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.