TESIS

EVALUASI DAN AUDIT TATA KELOLA KEAMANAN SIBER MENGGUNAKAN NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 DAN CIS CONTROLS V8

Disusun oleh:

Nama : **Hafizhan Irawan**
NIM : **22.55.2306**
Konsentrasi : **Digital Transformation Intelligence**

PROGRAM STUDI S2 INFORMATIKA
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2024

TESIS

EVALUASI DAN AUDIT TATA KELOLA KEAMANAN SIBER MENGGUNAKAN NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 DAN CIS CONTROLS V8

EVALUATION AND AUDIT CYBER SECURITY GOVERNANCE USE NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 AND CIS CONTROLS V8

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Magister

Disusun oleh:

Nama : **Hafizhan Irawan**
NIM : **22.55.2306**
Konsentrasi : **Digital Transformation Intelligence**

PROGRAM STUDI S2 INFORMATIKA
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2024

HALAMAN PENGESAHAN

EVALUASI DAN AUDIT TATA KELOLA KEAMANAN SIBER MENGGUNAKAN NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 DAN CIS CONTROLS V8

EVALUATION AND AUDIT CYBER SECURITY GOVERNANCE USE NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 AND CIS CONTROLS V8

Dipersiapkan dan Disusun oleh

Hafizhan Irawan

22.55.2306

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Kamis, 1 Agustus 2024

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 1 Agustus 2024
Rektor

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

HALAMAN PERSETUJUAN

EVALUASI DAN AUDIT TATA KELOLA KEAMANAN SIBER MENGGUNAKAN NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 DAN CIS CONTROLS V8

EVALUATION AND AUDIT CYBER SECURITY GOVERNANCE USE NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 AND CIS CONTROLS V8

Dipersiapkan dan Disusun oleh

Hafizhan Irawan

22.55.2306

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Kamis, 1 Agustus 2024

Pembimbing Utama

Alva Hendi Muhammad, S.T., M.Eng., Ph.D.
NIK. 190302493

Pembimbing Pendamping

Drs. Asro Nasiri, M.Kom.
NIK. 190302152

Anggota Tim Penguji

Dhani Ariatmanto, S.Kom., M.Kom., Ph.D.
NIK. 190302197

Dr. Ferry Wahyu Wibowo, S.Si., M.Cs.
NIK. 190302235

Alva Hendi Muhammad, S.T., M.Eng., Ph.D.
NIK. 190302493

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 1 Agustus 2024
Direktur Program Pascasarjana

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Hafizhan Irawan
NIM : 22.55.2306
Konsentrasi : Digital Transformation Intelligence

Menyatakan bahwa Tesis dengan judul berikut:
EVALUASI DAN AUDIT TATA KELOLA KEAMANAN SIBER MENGGUNAKAN NIST CYBER SECURITY FRAMEWORK, ISO/IEC 27002 DAN CIS CONTROLS V8

Dosen Pembimbing Utama : Alva Hendi Muhammad, S.T., M.Eng., Ph.D.
Dosen Pembimbing Pendamping : Drs. Asro Nasiri, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 1 Agustus 2024
Yang Menyatakan,

Hafizhan Irawan

HALAMAN PERSEMBAHAN

Puji dan syukur penulis ucapkan ke hadirat Allah SWT atas limpahan rahmat, karunia, dan hidayah-Nya yang tiada terkira sehingga penulis dapat menyelesaikan Tesis ini dengan lancar. Ucapan terimakasih penulis sampaikan kepada keluarga tercinta, yang telah senantiasa memberikan kasih sayang, doa, dan dukungan tiada henti dalam setiap langkah hidup penulis.

Tidak lupa juga penulis sampaikan ucapan terima kasih kepada seluruh dosen dan civitas akademisi Program Studi Magister Teknik Informatika (MTI) Universitas AMIKOM Yogyakarta atas ilmu dan semanagat yang diberikan dalam proses pembelajaran, di dalam kelas maupun di luar kelas. Terlebih khusus penulis ucapkan terima kasih kepada Bapak Alva Hendi Muhammad, S.T., M.Eng., Ph.D. dan Bapak Drs. Asro Nasiri, M.Kom. atas bimbingan, arahan, dan ketelatenannya dalam membimbing penulis selama proses penyusunan Tesis ini.

Penulis juga mengucapkan terima kasih kepada semua pihak di Dinas Komunikasi dan Informatika, yang telah berpartisipasi dalam penelitian ini. Dan terakhir, penulis ucapkan kepada semua pihak yang telah berkontribusi dalam penyelesaian Tesis ini, baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa Tesis ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari semua pihak demi perbaikan dan penyempurnaan Tesis ini di masa depan.

HALAMAN MOTTO

"Dialah yang menjadikan bumi untuk kamu dalam keadaan mudah dimanfaatkan. Maka, jelajahilah segala penjurunya dan makanlah sebagian dari rezeki-Nya. Hanya kepada-Nya kamu (kembali setelah) dibangkitkan." (Q.S Al-Mulk Ayat 15).

KATA PENGANTAR

Puji syukur kehadirat Allah SWT, atas limpahan rahmat, karunia, dan hidayah-Nya sehingga penulis dapat menyelesaikan Tesis ini dengan lancar. Shalawat serta salam semoga senantiasa tercurahkan kepada Nabi Muhammad SAW, beserta keluarga, sahabat, dan pengikutnya yang setia hingga akhir zaman.

Penyusunan Tesis ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Alva Hendi Muhammad, S.T., M.Eng., Ph.D. selaku pembimbing utama atas bimbingan, arahan, dan ketelatenannya dalam membimbing penulis selama proses penyusunan Tesis ini. Beliau senantiasa memberikan masukan dan saran yang berharga bagi penulis dalam menyelesaikan Tesis ini.
2. Bapak Drs. Asro Nasiri, M.Kom. selaku pembimbing pendamping atas bimbingan dan motivasi yang diberikan dalam proses penulisan Tesis ini.
3. Bapak Dhani Ariatmanto, S.Kom., M.Kom., Ph.D. atas masukan dan sarannya terhadap Tesis ini, sehingga penulis dapat menyempurnakan Tesis ini dalam bentuk yang terbaik.
4. Bapak Dr. Ferry Wahyu Wibowo, S.Si., M.Cs. atas masukannya dan sarannya terhadap Tesis ini, sehingga Tesis ini menjadi lebih rinci dan komprehensif.
5. Seluruh Dosen dan civitas akademisi Program Studi Magister Teknik Informatika (MTI) Universitas AMIKOM Yogyakarta atas ilmu dan sem anagatyang diberikan dalam proses pembelajaran,

6. Bapak Dr. TB. Asep Nurdin, M.Kom selaku Kepala Dinas Komunikasi dan Informatika Kota Tangerang Selatan beserta seluruh jajaran pegawainya yang telah memberikan dukungan dan kerja sama yang baik dalam proses penelitian ini.
7. Seluruh anggota keluarga atas pengertian dan dukungannya terhadap penulis dalam seluruh proses penelitian.
8. Seluruh mahasiswa/i Angkatan 8 Program Studi PJJ Magister Teknik Informatika Universitas AMIKOM Yogyakarta atas diskusi, motivasi, inspirasi yang terbentuk di dalam maupun di luar sesi perkuliahan.
9. Semua pihak yang telah berkontribusi dalam penyelesaian Tesis ini, baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa Tesis ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari semua pihak demi perbaikan dan penyempurnaan Tesis ini di masa depan. Semoga Tesis ini dapat bermanfaat bagi penulis, keluarga, almamater, dan masyarakat luas.

Yogyakarta, 1 Agustus 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Ancaman keamanan siber terus berkembang, sehingga penting bagi organisasi untuk mempertahankan postur keamanan siber yang kuat dan matang. Berdasarkan Laporan Tahunan Proyek Honeynet Badan Siber dan Sandi Negara (BSSN) Tahun 2023, terdapat 603.276.807 serangan siber terhadap Indonesia. Salah satu strategi yang dapat diterapkan adalah dengan melakukan penilaian kematangan keamanan siber untuk mengetahui tingkat penerapan keamanan siber organisasi saat ini. Laporan tesis ini mengusulkan desain kerangka penilaian kematangan keamanan siber yang memanfaatkan tiga standar yang telah ditetapkan: Cybersecurity Framework (CSF) v1.1 dari National Institute of Standards and Technology (NIST), ISO/IEC 27002:2022 dan Center for Internet Security (CIS) *Controls* v8.

Kerangka kerja yang diusulkan menggunakan pemetaan antara subkategori NIST CSF v.1.1, kontrol ISO/IEC 27002:2022, dan subkontrol CIS *Controls* v8, sehingga memungkinkan evaluasi komprehensif terhadap penerapan keamanan siber suatu organisasi. Metodologi evaluasi berfokus pada evaluasi implementasi dan efektivitas pengendalian yang selaras dengan setiap fungsi CSF NIST. Pendekatan ini memungkinkan organisasi untuk mengidentifikasi kekuatan dan kelemahan dalam postur keamanan siber mereka dan memprioritaskan area yang perlu ditingkatkan.

Penelitian ini mengembangkan pemetaan antara framework NIST CSF, ISO/IEC 27002:2002 dan CIS Controls v8 yang dijadikan sebuah kerangka kerja yang terintegrasi. Proses evaluasi dengan menggunakan kerangka kerja yang terintegrasi menghasilkan 40 (empat puluh) rekomendasi terhadap penerapan keamanan siber di Pusat Data Kota Tangerang Selatan.

Kata kunci: Evaluasi, Keamanan Siber, NIST CSF, ISO/IEC 27002:2022, CIS Controls v8

ABSTRACT

Cybersecurity threats continue to evolve, making it important for organizations to maintain a strong and mature cybersecurity posture. Based on the 2023 National Cyber and Crypto Agency (BSSN) Honeynet Project Annual Report, there were 603.276.807 cyberattacks against Indonesia. One strategy that can be implemented is to conduct a cyber security maturity assessment to determine the organization's current level of cyber security implementation. This paper proposes the design of a cybersecurity maturity assessment framework that leverages three established standards: the Cybersecurity Framework (CSF) v1.1 of the National Institute of Standards and Technology (NIST), ISO/IEC 27002:2022 and the Center for Internet Security (CIS) v8 Controls.

The proposed framework uses a mapping between NIST CSF v.1.1 subcategories, ISO/IEC 27002:2022 controls, and CIS Controls v8 subcontrols, thereby enabling a comprehensive evaluation of an organization's cybersecurity implementation. The evaluation methodology focuses on evaluating the implementation and effectiveness of controls aligned with each NIST CSF function. This approach allows organizations to identify strengths and weaknesses in their cybersecurity posture and prioritize areas for improvement.

This research develops a mapping between the NIST CSF framework, ISO/IEC 27002:2002 and CIS Controls v8. The evaluation process using the integration framework resulted in 40 (forty) recommendations for implementation of cyber security in Data Center of South Tangerang City Government.

Keyword: Evaluation, Cybersecurity, NIST CSF, ISO/IEC 27002:2022, CIS Controls v8

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Pertumbuhan pesat dalam penggunaan teknologi informasi dan ketergantungan organisasi terhadap pusat data sebagai infrastruktur inti menunjukkan pentingnya tata kelola keamanan siber yang efektif. Dalam menghadapi ancaman siber yang semakin kompleks dan beragam, pusat data menjadi target yang signifikan bagi serangan siber yang dapat merugikan integritas, kerahasiaan, dan ketersediaan data. Pusat data, sebagai fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk penempatan, penyimpanan dan pengolahan data, dan pemulihan data (Peraturan Presiden No. 95 Tahun 2018), memerlukan tata kelola keamanan siber yang solid untuk melindungi data sensitif dan memastikan kelangsungan operasional.

Keamanan siber adalah bagian dari keamanan informasi yang melindungi aset informasi dari ancaman terhadap informasi yang diproses, disimpan dan ditransmisikan melalui interkoneksi sistem informasi. Upaya dalam perlindungan informasi dalam konteks keamanan siber adalah mencegah, mengatasi dan mengurangi dampak dari kerusakan sistem (Jeremy, 2020). Menurut Laporan Tahunan Honeynet Project Badan Siber Sandi Negara (BSSN) tahun 2023, terjadi serangan siber terhadap Indonesia sebanyak 603.276.807 serangan (BSSN, 2023). Oleh sebab itu, risiko-risiko keamanan siber tersebut perlu dikelola dengan baik sehingga dapat mengurangi kerugian organisasi. Untuk meningkatkan keamanan

siber di organisasi, organisasi perlu melakukan audit dan evaluasi agar organisasi dapat mengukur kepabilitas dan kondisi eksisting dan meningkatkannya ke level yang lebih baik, sehingga di masa yang akan datang dampak ancaman siber dapat dikendalikan lebih optimal oleh organisasi.

Dewasa ini, tersedia banyak kerangka kerja yang dapat mengukur maturitas keamanan siber, seperti NIST, ISO, CIS dan kerangka kerja lainnya yang digunakan negara maupun organisasi sebagai kendali dalam meningkatkan implementasi keamanan siber. Penelitian ini menggunakan kerangka kerja NIST *Cyber Security Framework* (CSF), yaitu kerangka kerja yang dapat digunakan untuk membantu mengidentifikasi dan memprioritaskan tindakan untuk mengurangi risiko keamanan siber. NIST CSF juga dapat digunakan untuk mengelola risiko keamanan siber di seluruh organisasi atau dapat difokuskan pada layanan yang dianggap prioritas dalam organisasi. NIST CSF terdari diri tiga komponen, yaitu *Framework Core*, *Framework Implementation Tiers*, dan *Framework Profile*. NIST CSF memiliki lima *function* yang dijadikan prinsip, yaitu *Identify*, *Protect*, *Detect*, *Respond* dan *Recover* (NIST, 2018).

Dalam penggunaannya, NIST CSF bergantung pada kerangka kerja lain yang dituangkan dalam dokumen *Informative References*. Kerangka lain yang digunakan pada penelitian ini adalah ISO/IEC 27002 dan *Center for Internet Security* (CIS) *Controls* v8. NIST CSF telah memetakan CIS *Controls* pada *Framework Core* dan memiliki dokumentasi yang selaras (CIS, 2021), sehingga CIS *Controls* dapat menjadi salah satu kerangka kerja yang dapat digunakan untuk menangani risiko.

Selain CIS *Controls* v8, penelitian ini juga menggunakan ISO/IEC 27002:2022. Standar tersebut membahas mengenai keamanan informasi, keamanan siber, dan perlindungan data pribadi pada suatu organisasi. ISO/IEC 27002:2022 memiliki empat kategori pengendalian, yaitu *People*, *Phsyical*, *Technological*, dan *Organizational*. Dan terdapat 5 jenis atribut dalam ISO/IEC 27002:2022, yaitu *Control type* (*Preventive, Detective, Corrective*), *Information security properties* (*CIA*), *Cybersecurity concepts* (*Identify, Protect, Detect, Respond and Recover*), *Operational capabilities* (*infosec controls*) dan *Security domains* (*Governance & ecosystem, protection, Defence, Resilience*) (ISO/IEC, 2022).

Dinas Komunikasi dan Informatika Kota Tangerang Selatan (Diskominfo Kota Tangerang Selatan) adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang komunikasi dan informatika, bidang statistik, dan bidang persandian berdasarkan Peraturan Wali Kota Tangerang Selatan Nomor 56 Tahun 2022. Diskominfo Kota Tangerang Selatan juga memiliki fungsi pengelolaan informasi dan komunikasi publik pemerintah daerah serta penyelenggaraan persandian untuk pengamanan informasi pemerintah daerah (Peraturan Wali Kota Tangerang Selatan No. 56 Tahun 2022). Salah satu layanan yang menjadi prioritas Diskominfo Kota Tangerang Selatan adalah layanan Pusat Data. Seluruh Sistem Elektronik yang dimiliki oleh seluruh Perangkat Daerah menggunakan layanan Pusat Data untuk menunjang operasionalnya, sehingga menjadi urgensi untuk melaksanaan audit dan evaluasi terhadap penerapan keamanan siber di Pusat Data Diskominfo Kota Tangerang Selatan.

Berdasarkan pembahasan di atas, penelitian ini akan melakukan audit dan evaluasi tata kelola keamanan siber pada Pusat Data Diskominfo Kota Tangerang Selatan dengan menggunakan kerangka kerja NIST CSF sebagai tahapan *cyber-risk management*, ISO/IEC 27002:2022 sebagai kerangka kerja pendukung dan CIS *Controls* v8 sebagai kerangka kerja rekomendasi kontrol. Hasil dari penelitian ini berupa integrasi kerangka kerja serta hasil audit dan evaluasi menggunakan integrasi kerangka kerja berupa kondisi organisasi terhadap penerapan keamanan siber, nilai risiko, dan rekomendasi kontrol keamanan siber pada Pusat Data Diskominfo Kota Tangerang Selatan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang diuraikan, rumusan permasalahan dalam penelitian ini yaitu:

1. Bagaimana mengintegrasikan kerangka kerja NIST CSF, ISO/IEC 27002:2022 dan CIS *Controls* v8?
2. Bagaimana hasil audit dan evaluasi tata kelola keamanan siber pada Pusat Data Diskominfo Kota Tangerang Selatan berdasarkan integrasi kerangka kerja antara NIST CSF, ISO/IEC 27002:2022 dan CIS *Controls* v8 untuk mendapatkan hasil yang lebih komprehensif?
3. Apa rekomendasi kontrol yang dapat diterapkan untuk mengelola risiko keamanan siber pada Pusat Data Diskominfo Kota Tangerang Selatan berdasarkan CIS *Controls* v8?

1.3. Batasan Masalah

Penelitian ini akan dibatasi oleh hal-hal berikut, yaitu:

a. Audit dan evaluasi penerapan keamanan siber dilakukan pada layanan Pusat Data Diskominfo Kota Tangerang Selatan
b. Kerangka kerja yang digunakan adalah NIST CSF yang diintegrasikan dengan ISO/IEC 27002 dan CIS *Controls* v8
c. Audit dan evaluasi akan menghasilkan rekomendasi berdasarkan kerangka kerja CIS *Controls* v8

1.4. Tujuan Penelitian

Tujuan yang diharapkan dari rancangan penelitian "Evaluasi dan Audit Tata Kelola Keamanan Siber Menggunakan NIST *Cyber Security Framework*, ISO/IEC 27002 dan CIS *Controls* v8" antara lain adalah:

a. Memberikan pemahaman dan manfaat tentang penerapan evaluasi, asesmen dan audit terhadap tata kelola keamanan siber menggunakan NIST CSF, ISO/27002 dan CIS *Controls* v8 pada Instansi Pemerintah, khususnya Dinas Komunikasi dan Informatika Kota Tangerang Selatan;
b. Mengidentifikasi tingkat kepatuhan dan maturitas tata kelola keamanan siber pada Intansi;
c. Mengevalusi dan mengidentifikasi kekurangan dan kekuatan pada Instansi sebagai dasar untuk pengembangan dan peningkatan program keamanan siber;
d. Memberikan rekomendasi kontrol untuk meningkatkan tingkat kepatuhan dan maturitas tata kelola keamanan siber pada Instansi;
e. Mengurangi risiko dan dampak yang diakibatkan oleh ancaman siber; dan

f. Meningkatkan *Service Level Agreement* (SLA) dan kualitas layanan Pusat Data milik Pemerintah Kota Tangerang Selatan.

1.5. Manfaat Penelitian

Penelitian ini diharapkan bermanfaat bagi seluruh pihak dan pemangku kepentingan. Beberapa manfaat yang diharapkan diantaranya:

a. Hasil penelitian ini dapat dijadikan bahan rujukan maupun dikembangkan sebagai penelitian lebih lanjut.
b. Dapat digunakan sebagai referensi untuk penelitian yang sejenis di masa yang akan datang.
c. Meningkatnya tingkat kepedulian dan kapabilitas penerapan keamanan siber di Pusat Data Diskominfo Kota Tangerang Selatan.

BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Pada penelitian yang berjudul *Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS V8 and ISO/IEC 27002* (Bashofi dan Salman, 2022), peneliti mengintegrasikan NISTCSF, CIS *Controls* v8 dan ISO 27002:2013 untuk membuat *cybersecurity maturity framework* untuk mengoptimalkan implementasi manajemen keamanan informasi pada organisasi. Dan sebagai hasil integrasi, diusulkan 21 kategori yang diharapkan menjadi alat yang dapat meningkatkan performa dari manajemen keamanan informasi pada organisasi.

Pada penelitian *Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8* (Amiruddin et, al., 2021), dilakukan penelitian pada Unit TI XYZ yang ditemukan bahwa belum pernah dilakukan evaluasi keamanan siber sehingga belum memiliki rencana manajemen risiko siber. Dalam penelitian tersebut, peneliti menyusun rencana risiko siber khusus untuk Unit TI XYZ dengan menggunakan NIST CSF sebagai kerangka utama dan CIS Controls v8 serta NIST SP 800-53 Rev 5 untuk mendefinisikan kontrol dan rekomendasi tindakan. Sebagai hasilnya, peneliti menemukan 42 skenario risiko di Unit TI di mana 12 diterima dan 30 diredam. Ada 14 rekomendasi tindakan untuk Unit TI untuk mencapai tingkat 3 berdasarkan 18 kontrol CIS dan 20 kontrol NIST SP 800-53 rev 5 yang dapat diterapkan untuk mengendalikan risiko siber saat ini.

Selanjutnya pada penelitian yang berjudul Perancangan Kerangka Kerja Keamanan Siber Menggunakan NIST *CYBERSECURITY FRAMEWORK* DAN CIS *CONTROLS* (Mahendra, 2023), peneliti memanfaatkan kerangka kerja NIST Cybersecurity dan kerangka kerja CIS *Controls* sebagai kerangka kerja yang digunakan dalam manajemen risiko keamanan siber pada Kementerian PUPR. Hasil penelitian didapatkan bahwa didapatkan 32 rekomendasi dan mengusulkan rencana aksi dengan isu-isu prioritas tinggi dan sedang. Manajemen risiko menggunakan kerangka kerja NIST *Cybersecurity* dan CIS *Controls* terbukti dapat mengukur kematangan keamanan siber pada infrastruktur aplikasi sehingga dapat mengurangi kemungkinan terjadinya serangan siber.

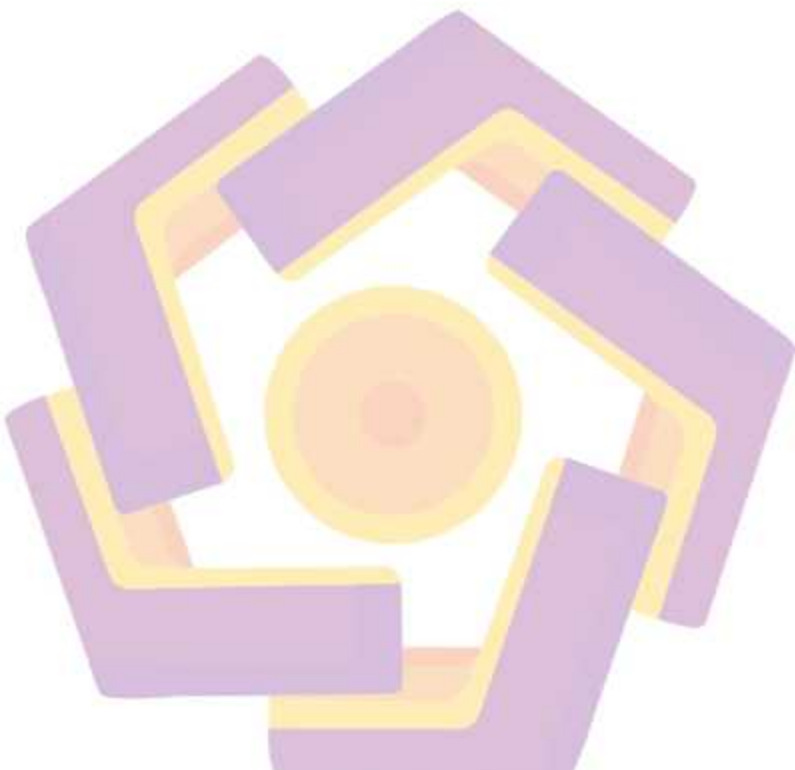
Lalu pada penelitian lainnya (Sulistyowati, 2020) yang berjudul *Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS* dilakukan penelitian terhadap organisasi ABC, yaitu salah satu lembaga pemerintah yang mengelola infrastruktur kritis dan ekonomi digital di Indonesia. Hasil penelitian awal ditemukan bahwa kesiapan pengelolaan keamanan informasi masih belum optimal. Maka dari itu, dilakukan analisis terhadap standar keamanan NIST, ISO 27002, COBIT, dan PCI DSS, yang merupakan standar keamanan organisasi ABC dalam mengelola TIK melalui tugas dan fungsi yang diberikan. Selanjutnya, hasil analisis tersebut digunakan sebagai bahan untuk merancang kerangka kematangan keamanan siber melalui empat pendekatan standar yang telah menjadi dasar pengelolaan TIK. Konsep yang diusulkan dengan dua puluh satu kategori keamanan

siber terintegrasi diharapkan menjadi modal dalam mengukur kinerja pengelolaan TIK di organisasi ABC.

Selanjutnya pada penelitian yang berjudul Audit Keamanan Siber Menggunakan Kerangka Kerja CIS CSC, NIST CSF, dan COBIT 2019 (Fadila et, al., 2023), peneliti melakukan integrasi *framework* CIS CSC (*Center for Internet Security Critical Security Controls*), NIST CSF (*National Institute of Standards and Technology Cybersecurity Framework*) dan COBIT 2019 (*Control Objective for Information Technologies*) untuk melakukan perhitungan level kapabilitas pada Dinas Komunikasi dan Informatika Kota Pontianak, sehingga dihasilkan 19 rekomendasi aktivitas untuk dilakukan agar mencapai level keamanan siber yang diinginkan, kemudian dilakukan pemetaan aktivitas rekomendasi ke dalam action priority matrix, 10 aktivitas masuk ke dalam kuadran *Quick Wins*, dan 9 aktivitas yang masuk ke dalam kuadran *Major Projects*.

Lalu pada penelitian yang berjudul *Information Security Maturity Model For NIST Cyber Security Framework* (Almuhammadi dan Alsaleh, 2017), peneliti melakukan komparasi secara komprehensif terhadap NIST CSF, COBIT 5, ISO/IEC 27001:2013 dan ISF. Hasil komparasi akan mengisi gap dari masing-masing kerangka kerja sehingga membentuk *Capability Maturity Model* baru. Disimpulkan bahwa NIST CSF tidak secara memadai menangani proses penilaian kepatuhan. Evaluasi model kematangan mempertimbangkan definisi level skala dan area yang dinilai. Di kedua dimensi tersebut, tidak ada pemetaan satu-satu antara model kematangan yang berbeda. Sehingga diusulkan model kematangan baru

dengan skala lima level dan mencakup dua puluh dua kategori NIST CSF dengan penambahan proses penilaian kepatuhan.



2.2. Keaslian Penelitian

Tabel 2. 1. Matriks literatur review dan posisi penelitian
Evaluasi dan Audit Tata Kelola Keamanan Siber Menggunakan NIST *Cyber Security Framework*, ISO/IEC 27002 dan CIS *Controls* v8

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	*Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS V8 and ISO/IEC 27002*	Ivan Bashofi, Muhammad Salman (2022)	Mengoptimalkan implementasi manajemen kemanan informasi dengan menggunakan NIST CSF, CIS *Controls* v8 dan ISO/IEC 27002:2013	Hasil penelitian menghasilkan 21 kategori kendali yang diharapkan menjadi alat yang dapat meningkatkan performa dari manajemen keamanan informasi pada organisasi	*Framework* ISO/IEC 27002 masih menggunakan versi tahun 2013. Belum adanya hasil audit dan evaluasi yang menggunakan integrasi tiga *framework* tersebut	Penelitian ini akan menggunakan *framework* ISO/IEC 27002:2022 dan akan melakukan evaluasi dan audit menggunakan hasil integrasi dari tiga framework tersebut
2	*Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8*	Amiruddin, Hafizh Ghozie Afiansyah, Hernowo Adi Nugroho (2021)	Membuat rencana risiko siber dengan menggunakan NIST CSF sebagai kerangka utama dan CIS *Controls* v8 serta NIST SP 800-53 Rev 5 untuk mendefinisikan kontrol dan rekomendasi tindakan	Hasil penelitian menemukan 42 skenario risiko di Unit TI di mana 12 diterima dan 30 diredam. Ada 14 rekomendasi tindakan untuk Unit TI untuk mencapai tingkat 3 berdasarkan 18 kontrol CIS dan 20 kontrol NIST SP 800-53 rev 5 yang dapat diterapkan	Penelitian sudah dilakukan secara baik dan komprehensif. Namun penelitian terbatas terhadap manajemen risiko	Dalam penelitian yang akan dilakukan, peneliti akan melakukan evaluasi dan audit terhadap objek penelitian menggunakan NIST CSF, ISO/IEC 27002:2022 dan CIS *Controls* v8 sehingga arah dan keluaran rekomendasi akan berbeda

Tabel 2. 1. Matriks literatur review dan posisi penelitian
Evaluasi dan Audit Tata Kelola Keamanan Siber Menggunakan NIST *Cyber Security Framework*, ISO/IEC 27002 dan CIS *Controls* v8 (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
3	Perancangan Kerangka Kerja Keamanan Siber Menggunakan NIST CYBERSECURITY FRAMEWORK DAN CIS CONTROLS	Vicky Mahendra (2023)	Memanfaatkan kerangka kerja NIST *Cybersecurity* dan kerangka kerja CIS *Controls* sebagai kerangka kerja yang digunakan dalam manajemen risiko keamanan siber pada Kementerian PUPR	Hasil penelitian didapatkan bahwa didapatkan 32 rekomendasi dan mengusulkan rencana aksi dengan isu-isu prioritas tinggi dan sedang. Manajemen risiko menggunakan kerangka kerja NIST *Cybersecurity* dan CIS *Controls* terbukti dapat mengukur kematangan keamanan siber pada infrastruktur aplikasi sehingga dapat mengurangi kemungkinan terjadinya serangan siber	Pemetaan NIST CSF dan CIS *Controls* v8 berpotensi adanya kontrol yang *unmapped*, sehingga dirasa perlu untuk menambah satu referensi *framework* tambahan seperti ISO/IEC 27002 ataupun NIST 800-53	Penelitian yang akan dilakukan menggunakan tiga kerangka kerja untuk meminimalisir terjadinya kontrol di NIST CSF yang *unmapped*

Tabel 2. 1. Matriks literatur review dan posisi penelitian
Evaluasi dan Audit Tata Kelola Keamanan Siber Menggunakan NIST *Cyber Security Framework*, ISO/IEC 27002 dan CIS *Controls* v8 (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
4	*Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS*	Diah Sulistyowati, Fitri Handayani, Yohan Suryanto (2020)	Melakukan komparasi terhadap kerangka kerja NIST CSF, COBIT, ISO/IEC 27002 dan PCI DSS dan merancang kerangka keamanan siber menggunakan empat kerangka kerja tersebut	Sintesis kerangka kerja yang ada menjadi kerangka kerja baru yang komprehensif memungkinkan organisasi ABC untuk mengukur tingkat kematangan keamanan siber secara efektif. Dua puluh satu kategori ini berfungsi sebagai panduan untuk perbaikan organisasi, dengan potensi penyempurnaan lebih lanjut melalui validasi dan pemetaan subkategori	Belum adanya pemetaan hingga sub category pada NIST CSF, dan belum dilakukannya audit maupun evaluasi menggunakan hasil integrasi keempat kerangka kerja tersebut	Penelitian yang akan dilakukan akan dilakukan pemetaan hingga sub category NIST CSF dan dilakukan evaluasi serta audit terhadap objek penelitian

Tabel 2. 1. Matriks literatur review dan posisi penelitian
Evaluasi dan Audit Tata Kelola Keamanan Siber Menggunakan NIST *Cyber Security Framework*, ISO/IEC 27002 dan CIS *Controls* v8 (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
5	Audit Keamanan Siber Menggunakan Kerangka Kerja CIS CSC, NIST CSF, dan COBIT 2019	Viny Fadila, Nurul Mutiah, Renny Puspita Sari (2023)	Peneliti melakukan integrasi framework CIS CSC (*Center for Internet Security Critical Security Controls*), NIST CSF (*National Institute of Standards and Technology Cybersecurity Framework*) dan COBIT 2019 (*Control Objective for Information Technologies*) untuk melakukan perhitungan level kapabilitas pada Dinas Komunikasi dan Informatika Kota Pontianak	Dihasilkan 19 rekomendasi aktivitas untuk dilakukan agar mencapai level keamanan siber yang diinginkan, kemudian dilakukan pemetaan aktivitas rekomendasi ke dalam *action priority matrix*, 10 aktivitas masuk ke dalam kuadran *Quick Wins*, dan 9 aktivitas yang masuk ke dalam kuadran *Major Projects*	Penelitian agar dilakukan terhadap responden kuesioner yang tepat, kuesioner ditujukan kepada orang yang mengerti bidang penelitian agar jawaban yang diberikan lebih valid	Penelitian yang akan dilakukan menggunakan NIST CSF sebagai kerangka kerja utama, sehingga akan berbeda kontrol yang akan diaudit maupun yang dievaluasi

Tabel 2. 1. Matriks literatur review dan posisi penelitian
Evaluasi dan Audit Tata Kelola Keamanan Siber Menggunakan NIST *Cyber Security Framework*, ISO/IEC 27002 dan CIS *Controls* v8 (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
6	*INFORMATION SECURITY MATURITY MODEL FOR NIST CYBER SECURITY FRAMEWORK*	Sultan Almuhammadi, Majeed Alsaleh (2017)	Melakukan komparasi secara komprehensif terhadap NIST CSF, COBIT 5, ISO/IEC 27001:2013 dan ISF. Hasil komparasi akan mengisi gap dari masing-masing kerangka kerja sehingga membentuk *Capability Maturity Model* baru	NIST CSF tidak secara memadai menangani proses penilaian kepatuhan. Evaluasi model kematangan mempertimbangkan definisi level skala dan area yang dinilai. Di kedua dimensi tersebut, tidak ada pemetaan satu-satu antara model kematangan yang berbeda.Sehingga diusulkan model kematangan baru dengan skala lima level dan mencakup dua puluh dua kategori NIST CSF dengan penambahan proses penilaian kepatuhan	Kerangka kerja yang digunakan menggunakan versi yang sudah lampau, sehingga perlu adanya pembaharuan penelitian menggunakan kerangka kerja versi terbaru.	Penelitian yang akan dilakukan menggunakan NIST CSF sebagai kerangka kerja utama, dan menjadikan ISO/IEC 27002:2022 dan CIS *Controls* v8 sebagai referensi terhadap kontrol yang ada di dalam NIST CSF. Batasan yang ditetapkan adalah tidak mengulas seberapa memadainya NIST CSF sebagai kerangka kerja.

2.3. Landasan Teori

2.3.1. NIST CSF

NIST CSF berfokus sebagai panduan *cybersecurity activities* dan mempertimbangkan risiko keamanan siber sebagai bagian dari proses dalam manajemen risiko. NIST CSF dikembangkan untuk meningkatkan manajemen risiko dan dapat digunakan untuk organisasi di semua sektor, terlepas dari ukuran, tingkat risiko keamanan siber, atau kecanggihan keamanan siber. Organisasi dapat menentukan hal-hal yang penting dalam kegiatan untuk dapat memprioritaskan di bidang keamanan siber sehingga NIST CSF digunakan untuk mengurangi dan mengelola risiko keamanan siber dengan baik. Komponen pada NIST CSF lebih tepat untuk organisasi yang berkecimpung di bidang teknologi karena ruang lingkupnya yang berupa teknikal kontrol, analisa log dan insiden (Praneet, 2020). NIST CSF memiliki pendekatan berbasis risiko dalam mengelola risiko keamanan siber yang terdiri dari tiga bagian yaitu *Framework Core*, *Framework Implementation Tiers*, dan *Framework Profile* (NIST, 2018).

2.3.1.1. *Framework Core*

Framework Core terdiri dari tiga komponen utama yang saling melengkapi untuk membantu organisasi dalam mengembangkan, menerapkan, dan memperkuat program keamanan siber mereka. Ketiga komponen ini adalah *Identify* (Identifikasi), *Protect* (Perlindungan), dan *Detect* (Deteksi), serta ada juga komponen *Respond* (Tanggap) dan *Recover* (Pemulihan) yang melengkapi siklus tanggapan dan pemulihan setelah serangan (NIST, 2018).

Gambar 2. 1. Struktur Framework Core

Seluruh komponen tersebut dapat dilihat fungsi dan kategorinya pada tabel di bawah berikut.

Tabel 2. 2. *Functions dan Categories Framework Core*

Function Unique Identifier	*Function*	*Categories Unique Identifier*	*Categories*
ID	*Identify*	ID.AM	*Asset Management*
		ID.BE	*Business Environment*
		ID.GV	*Governance*
		ID.RA	*Risk Assessment*
		ID.RM	*Risk Management Strategy*
		ID.SC	*Supply Chain Risk Management*
PR	*Protect*	PR.AC	*Identity Management and Access Control*
		PR.AT	*Awareness and Training*
		PR.DS	*Data Security*
		PR.IP	*Information Protection*
		PR.MA	*Maintenance*
		PR.PT	*Protective Technology*

Tabel 2. 2. *Functions dan Categories Framework Core* (Lanjutan)

Function Uniqe Identifier	*Function*	*Categories Unique Identifier*	*Categories*
DE	*Detect*	DE.AE	*Anomalies and Events*
		DE.CM	*Security Continuous Monitoring*
		DE.DP	*Detection Processes*
RS	*Respond*	RS.RP	*Response Planning*
		RS.CO	*Communications*
		RS.AN	*Analysis*
		RS.MI	*Mitigation*
		RS.IM	*Improvements*
RC	*Recover*	RC.RP	*Recovery Planning*
		RC.IM	*Improvements*
		RC.CO	*Communications*

a. *Identify* (ID)

Komponen identifikasi fokus pada pemahaman organisasi terhadap aset, kerentanan, dan ancaman keamanan siber yang relevan. Langkah-langkah yang termasuk dalam komponen ini meliputi identifikasi dan pemetaan aset penting, mengevaluasi risiko, mengembangkan pemahaman tentang kerentanan yang ada, dan memahami ancaman yang mungkin terjadi.

b. *Protect* (PR)

Komponen proteksi bertujuan untuk mengimplementasikan langkah-langkah perlindungan yang efektif untuk mengurangi risiko yang diidentifikasi pada tahap identifikasi. Ini meliputi langkah-langkah seperti penerapan kontrol akses yang kuat, kebijakan keamanan yang jelas, tindakan pencegahan malware, enkripsi data, pengelolaan identitas, dan perlindungan

fisik terhadap infrastruktur kritis. Perlindungan ini membantu organisasi menjaga integritas dan kerahasiaan data serta melindungi sistem mereka dari serangan.

c. *Detection* (DE)

Komponen deteksi berkaitan dengan pengembangan dan implementasi kemampuan deteksi untuk mengidentifikasi adanya serangan atau insiden keamanan siber yang sedang berlangsung atau telah terjadi. Hal ini mencakup penerapan sistem pendeteksian intrusi, analisis log, pemantauan jaringan, dan mekanisme deteksi lainnya untuk mengenali pola-pola yang mencurigakan. Kemampuan deteksi yang efektif memungkinkan organisasi untuk mengetahui ketika serangan terjadi sehingga dapat segera merespons dan meminimalkan dampak yang ditimbulkan.

d. *Respond* (RS)

Komponen respon bertujuan untuk mengembangkan rencana dan prosedur tanggap darurat serta melaksanakan tindakan yang tepat saat terjadi serangan.

e. *Recover* (RC)

Komponen pemulihan berkaitan dengan upaya pemulihan setelah serangan, termasuk pemulihan data, pemulihan operasional, dan pembelajaran dari kejadian tersebut untuk memperbaiki keamanan siber di masa depan.

2.3.1.2. *Framework Implementation Tiers*

Framework Implementation Tiers (Tingkatan Implementasi Kerangka Kerja) adalah komponen penting dalam NIST CSF yang membantu organisasi dalam mengevaluasi tingkat kedewasaan dan kemampuan mereka dalam menerapkan praktik keamanan siber. *Framework Implementation Tiers* terdiri dari empat tingkatan, yaitu *Partial* (Tingkat Partial), *Risk Informed* (Tingkat Informasi Risiko), *Repeatable* (Tingkat Terulang), dan *Adaptive* (Tingkat Adaptif) (NIST, 2018). Penjelasan dari *tier* tesebut terdapat pada Tabel 2.3.

Tabel 2. 3. *Framework Implementation Tiers*

Tier	***Risk Management Process***	***Integrates Risk Management Program***	***External Participation***
1 (*Partial*)	Manajemen risiko keamanan siber belum dibentuk sehingga prioritas aktivitas keamanan siber belum diketahui.	Kesadaran mengenai risiko keamanan siber masih terbatas.	Organisasi tidak menerima dan memberikan informasi dari pihak lain.
2 (*Risk Informed*)	Manajemen risiko keamanan siber diterapkan namun belum adanya kebijakan yang mengatur hal tersebut.	Terdapat kesadaran mengenai risiko keamanan siber namun belum dilakukan pendekatan untuk mengelola hal tersebut.	Organisasi memahami perannya dalam skala yang lebih besar namun penyampaian dan penerimaan informasi masih belum berjalan dengan baik.
3 *(Repeatable)*	Manajemen risiko siber telah diterapkan dan terdapat kebijakan yang mengaturnya. Penerapan keamanan siber diperbaharui secara berkala.	Terdapat pendekatan untuk mengelola risiko keamanan siber. Metode yang digunakan tersedia untuk merespon perubahan risiko secara efektif.	Organisasi memahami keterkaitan dengan pihak luar sehingga memiliki peran dan saling tergantung pada skala yang lebih besar

Tabel 2. 3. *Framework Implementation Tiers* (Lanjutan)

Tier	*Risk Management Process*	*Integrates Risk Management Program*	*External Participation*
4 *(Adaptive)*	Penerapan manajemen risiko keamanan siber berdasarkan aktivitas keamanan siber sebelumnya dan saat ini. Dapat beradaptasi dengan ancaman yang berubah dan merespon dengan cepat dan tepat.	Terdapat pendekatan menggunakan kebijakan, proses, dan prosedur berdasarkan informasi risiko untuk mengelola dan menangani keamanan siber.	Organisasi memahami peranannya dengan pihak luar dan membagikan informasi secara internal dan eksternal.

2.3.1.3. *Framework Profile*

Framework Profile adalah konfigurasi yang dipilih dari kategori, subkategori, dan praktik keamanan siber yang terkait dengan NIST CSF. Profil ini mencerminkan tujuan keamanan siber yang spesifik, risiko yang relevan, dan persyaratan khusus yang ada dalam organisasi (NIST, 2018).

Framework Profile membantu organisasi dalam mengadopsi pendekatan yang disesuaikan dengan konteks mereka sendiri. Dengan membangun profil yang sesuai, organisasi dapat menentukan langkah-langkah konkret yang perlu diambil untuk meningkatkan keamanan siber mereka.

2.3.2. ISO/IEC 27002

ISO/IEC 27002, yang sebelumnya dikenal sebagai ISO/IEC 17799, memberikan panduan umum untuk mengelola keamanan informasi dan menguraikan serangkaian kendali keamanan yang dapat diimplementasikan. Standar ini meliputi aspek-aspek penting dalam keamanan informasi, termasuk

kebijakan keamanan, organisasi keamanan, aset informasi, keamanan fisik dan lingkungan, pengelolaan komunikasi dan operasional, pengendalian akses, pengembangan dan pemeliharaan sistem, manajemen keamanan, pemantauan, evaluasi, dan pemulihan (ISO/IEC, 2022).

Gambar 2. 2. Pengendalian ISO/IEC 27002:2022

ISO/IEC 27002:2022 memiliki 4 ketegori pengendalian dan 93 kendali pengamanan, yaitu:

a. Organizational (37 kendali pengamanan)
b. People (8 kendali pengamanan)
c. Physical (14 kendali pengamanan)
d. Technological (34 kendali pengamanan)

2.3.3. CIS Controls v8

CIS *Controls* adalah serangkaian tindakan dan aktivitas yang diprioritaskan secara kolektif sehingga membentuk serangkaian praktik terbaik

defense-in-depth untuk mengurangi serangan dan ancaman yang paling umum terjadi pada sistem serta jaringan. Serangkaian aktivitas tersebut dikembangkan oleh komunitas pakar TI yang menggunakan pengalamannya untuk menciptakan praktik terbaik. Komunitas tersebut mengembangkan CIS *Controls* dari berbagai sektor termasuk retail, manufaktur, kesehatan, pendidikan, pemerintahan, pertahanan, dan lainnya (CIS, 2021).

CIS *Controls* melakukan pengategorian untuk menentukan aktivitas keamanan siber yang diprioritaskan sesuai dengan keadaan organisasi. Pengategorian tersebut disebut dengan CIS *Implementation Groups* (IGs). IGs adalah kategori yang dinilai sendiri untuk organisasi berdasarkan atribut keamanan siber yang ada pada organisasi. Setiap IG mengidentifikasi subset yang ada pada CIS Controls dan dibangun berdasarkan IG sebelumnya. Jika organisasi dinilai sebagai IG2 maka syarat yang ada pada IG1 harus terpenuhi, hal tersebut juga berlaku pada IG3 yang harus melengkapi syarat yang ada pada IG1 dan IG2. Dengan begitu, organisasi dapat memprioritaskan penerapan controls berdasarkan IG yang ditentukan. Menurut CIS (2021), terdapat 3 (tiga) kriteria yang harus diperhatikan dalam menentukan IG suatu organisasi, yaitu:

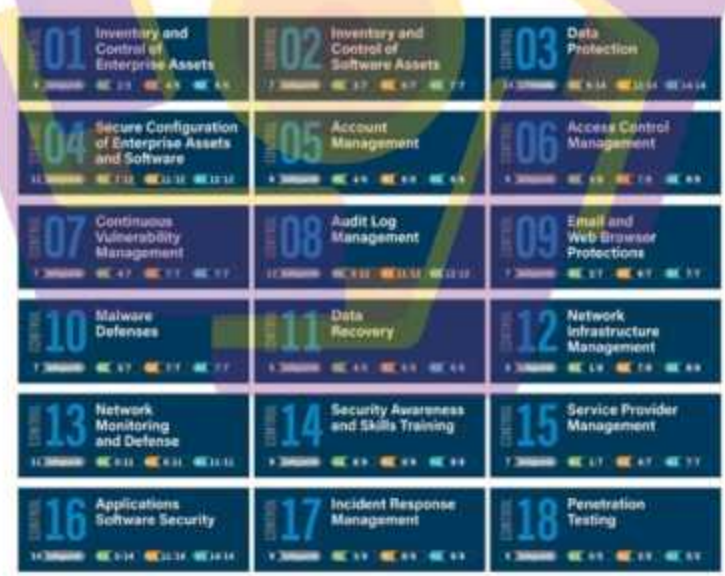
a. Tingkat *sensitive* dan *critical* dari data serta layanan yang ditawarkan oleh organisasi.
b. Tingkat keahlian sumber daya manusia.
c. Penempatan sumber daya yang sesuai untuk menerapkan aktivitas keamanan siber.

CIS (2021) mengemukakan bahwa IGs dibagi menjadi 3 (tiga) jenis yang menjelaskan keadaan dan kondisi organisasi berdasarkan atribut keamanan siber, yaitu:

a. *Implementation Group* 1 (IG1): Organisasi IG1 berukuran kecil hingga menengah, biasanya hanya memiliki kurang lebih 10 personil. Organisasi IG1 memiliki keahlian TI dan aktivitas keamanan siber yang terbatas sehingga belum mampu untuk melindungi aset, data, informasi, dan personil organisasi. Organisasi dinilai masih rendah dalam sensitivitas data termasuk data personil dan keuangan. Oleh karena itu, kontrol yang diterapkan berfokus pada menggagalkan serangan umum.
b. *Implementation Group* 2 (IG2): Organisasi IG2 berukuran sedang hingga besar, biasanya organisasi regional dapat dikategorikan pada jenis ini. Organisasi IG2 mempekerjakan personil yang bertanggung jawab dalam mengelola dan melindungi infrastruktur TI. Pada organisasi ini telah mendukung adanya layanan dan infrastruktur TI pada setiap bagian atau departemen yang memiliki risiko yang berbeda. Organisasi IG2 sudah melindungi data sensitif dan dapat mengatasi gangguan layanan yang mudah. Kontrol pada jenis ini membantu personil untuk mengatasi peningkatan kompleksitas operasional. Terdapat beberapa sub-kontrol yang bergantung pada teknologi dan keahlian yang dimiliki organisasi.
c. *Implementation Group* 3 (IG3) Organisasi IG3 berukuran besar, biasanya telah mempekerjakan ratusan personil. Organisasi IG3 mempekerjakan pakar keamanan yang memiliki spesialis dalam berbagai aspek keamanan siber.

Sistem dan data yang berisikan data sensitif telah diatur dan dikelola oleh peraturan dan kebijakan. Organisasi IG3 harus menerapkan CIA (confidentiality, integrity, availability) pada sistem dan layanan yang ada. Serangan yang berhasil merusak akan menyebabkan kerugian yang besar sehingga sub-kontrol yang dipilih harus meredakan serangan yang canggih dan mengurangi dampak serangan.

CIS Control v8 memberikan cara yang terbukti untuk melindungi sistem teknologi informasi dan data dari serangan siber. Pendekatan ini mengikuti standar keamanan yang diakui secara global dan mencakup 18 kontrol utama dengan 153 sub kontrol sebagai pedoman yang lebih rinci seperti yang ditunjukkan pada Gambar 3.



Gambar 2. 3. CIS *Controls* v8

BAB III

METODE PENELITIAN

3.1. Jenis, Sifat, dan Pendekatan Penelitian

Penelitian ini bersifat deskriptif, dengan menggambarkan dan menganalisis fenomena. Penelitian ini menggunakan metode studi kasus terhadap Tata Kelola Keamanan Siber pada Pusat Data menggunakan NIST CSF, ISO/IEC 27002:2022 dan CIS *Controls* v8, dengan tujuan untuk mengevaluasi dan mengaudit serta memberikan hasil rekomendasi terhadap pengelolaan Pusat Data.

Penentuan lokasi studi kasus di Diskominfo Kota Tangerang Selatan, karena Pusat Data adalah salah satu layanan yang menjadi prioritas. Seluruh Sistem Elektronik yang dimiliki oleh seluruh Perangkat Daerah menggunakan layanan Pusat Data untuk menunjang operasionalnya, sehingga menjadi urgensi untuk melaksanaan audit dan evaluasi terhadap penerapan keamanan siber di Pusat Data Diskominfo Kota Tangerang Selatan

Penelitian yang dilakukan merupakan pendekatan penelitian kualitatif, yaitu suatu pendekatan penelitian yang berfokus pada interpretasi, pemahaman mendalam, dan konteks pada tata kelola keamanan siber di pusat data Diskominfo Kota Tangerang Selatan. Hasil dari penelitian ini adalah laporan evaluasi dan audit serta rekomendasi terkait tata kelola keamanan siber di Diskominfo Kota Tangerang Selatan.

3.2. Metode Pengumpulan Data

Tahapan pengumpulan data menggunakan langkah sebagai berikut:

a. Wawancara

Wawancara digunakan sebagai teknik pengumpulan data dalam melakukan studi pendahuluan untuk menemukan permasalahan yang harus diteliti, juga untuk mengetahui hal-hal dari responden yang lebih mendalam (Sugiyono, 2013). Pengumpulan data melalui teknik wawancara dilakukan secara terstruktur dengan mengajukan pertanyaan yang telah ditentukan sebelumnya.

b. Observasi

Observasi merupakan teknik pengumpulan data yang dilakukan oleh peneliti tanpa berinteraksi langsung dengan obyek penelitian. Teknik ini digunakan untuk mengamati perilaku dan proses kerja. Observasi dibedakan menjadi dua yaitu partisipan observasi dan non-partisipan observasi (Ahyar, 2020).

c. Kuesioner

Menurut Sugiyono (2013), kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawab.

3.3. Metode Analisis Data

Analisis data pada penelitian ini menggunakan beberapa metode, yaitu:

a. Analisis komparatif: Digunakan untuk uji perbedaan atau uji korelasi untuk membandingkan variabel dan hubungan antara kerangka kerja NIST CSF, ISO/IEC 27002, dan CIS *Controls* v8.

b. Koding dan Kategorisasi: Dilakukan koding dan kategorisasi dari hasil analisis komparatif antara kerangka kerja NIST CSF, ISO/IEC 27002 dan CIS *Controls* v8. Metode ini dilakukan agar terjadi integrasi antara kerangka kerja tersebut.

c. Audit dan evaluasi akan dilakukan dengan mengidentifikasi kondisi keamanan siber di Pusat Data Kota Tangerang Selatan saat ini. Identifikasi akan dilakukan menggunakan hasil integrasi kerangka kerja yang dirinci menjadi pertanyaan-pertanyaan yang diajukan kepada pengelola Pusat Data Kota Tangerang Selatan. Jawaban dari pertanyaan tersebut akan disesuaikan dengan *tier* yang ada pada kerangka kerja NIST CSF.

d. Rekomendasi akan diberikan sesuai dengan hasil audit dan evaluasi menggunakan hasil integrasi kerangka kerja.

3.4. Alur Penelitian

Metode penelitian yang digunakan pada penelitian ini dapat mencakup beberapa langkah sebagai berikut:

a. Studi Literatur: Melakukan tinjauan pustaka yang komprehensif untuk memahami konsep dan teori yang terkait dengan tata kelola keamanan siber, NIST CSF, ISO/IEC 27002, dan CIS *Controls* v8. Tinjauan literatur ini akan membantu membangun landasan teoritis penelitian dan memperoleh

pemahaman yang mendalam tentang kerangka kerja dan praktik keamanan siber yang relevan.

b. Studi Kasus: Melakukan studi kasus di Pusat Data Dinas Komunikasi dan Informatika Kota Tangerang Selatan untuk menganalisis dan mengevaluasi implementasi tata kelola keamanan siber yang ada. Langkah ini dapat melibatkan pengumpulan data melalui wawancara dengan pihak terkait, observasi langsung, dan analisis dokumen terkait keamanan siber.

c. Pengumpulan Data: Mengumpulkan data yang relevan dengan menggunakan teknik seperti wawancara dengan pemangku kepentingan terkait, pengamatan langsung, dan analisis dokumen terkait kebijakan, prosedur, dan tata kelola keamanan siber yang ada di Pusat Data. Data yang dikumpulkan dapat meliputi informasi tentang kebijakan keamanan, struktur organisasi, prosedur pengelolaan risiko, sistem keamanan yang ada, dan catatan kejadian keamanan sebelumnya.

d. Analisis Data: Menganalisis data yang telah dikumpulkan untuk mengevaluasi keefektifan dan kepatuhan terhadap NIST CSF, ISO/IEC 27002, dan CIS *Controls* v8. Analisis data dapat mencakup perbandingan antara praktik keamanan yang ada dengan persyaratan dan rekomendasi dari kerangka kerja yang dipilih, identifikasi kelemahan atau celah keamanan yang mungkin ada, serta penilaian risiko yang terkait dengan sistem dan data yang terlibat.

e. Evaluasi dan Rekomendasi: Berdasarkan analisis data, melakukan evaluasi terhadap kepatuhan terhadap kerangka kerja dan standar keamanan yang dipilih, serta mengidentifikasi area yang perlu perbaikan atau peningkatan.

Berdasarkan temuan tersebut, memberikan rekomendasi yang spesifik dan tindakan perbaikan yang dapat dilakukan untuk meningkatkan tata kelola kemanan siber di Pusat Data.

Gambar 3. 1. Langkah Penelitian

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1. Analisis Komparatif

Analisis komparatif dilakukan antara kedua *framework*, yang hasilnya dapat dilihat pada Tabel 4.1.

Tabel 4. 1. Analisis Komparatif

Framework	Fungsi	Kategori dan Sub Kategori
NIST CSF	1. *Identification* 2. *Protect* 3. *Detection* 4. *Respond* 5. *Recovery*	Terdiri dari 23 kategori dan 108 sub kategori
ISO/IEC 27002	Sebagai referensi untuk menentukan dan mengimplementasikan kontrol penanganan risiko keamanan informasi dalam sistem manajemen keamanan informasi (SMKI) berdasarkan ISO/IEC 27001	Terdiri dari 4 kategori dengan total 93 kontrol
CIS *Controls* v8	Memanfaatkan pengalaman komunitas individu dan perusahaan untuk meningkatkan keamanan melalui berbagi ide, alat, pembelajaran, dan tindakan kolektif.	Terdiri dari 18 kontrol dan 153 sub kontrol

4.2. Integrasi Kerangka Kerja

Langkah selanjutnya adalah pengkodean subkategori dan subkontrol. Untuk menetapkan bagaimana kedua kerangka kerja tersebut terintegrasi, peneliti memberikan kode ke subkategori kerangka NIST CSF (ditunjukkan pada Tabel 4.2.), di mana 'A' mewakili NIST CSF, 'A.1' mewakili kategori Manajemen Aset di NIST CSF dan 'A.1.1' mewakili sub kategori ID.AM-1 dalam kategori *Asset Management* di NIST CSF, dan seterusnya.

Tabel 4. 2. Kodifikasi Sub Kategori NIST CSF

Kategori	Sub Kategori	ID
Asset Management	ID.AM-1	A.1.1
	ID.AM-6	A.1.6
Business Environment	ID.BE-1	A.2.1
	ID.BE-5	A.2.5
Governance	ID.GV-1	A.3.1
	ID.GV-4	A.3.4
Risk Assessment	ID.RA-1	A.4.1
	ID.RA-6	A.4.6
Risk Management Strategy	ID.RM-1	A.5.1
	ID.RM-3	A.5.3
Supply Chain Risk Management	ID.SC-1	A.6.1
	ID.SC-5	A.6.5
Identity Management, Authentication and Access Control	PR.AC-1	A.7.1
	PR.AC-7	A.7.7
Awareness and Training	PR.AT-1	A.8.1
	PR.AT-5	A.8.5

Tabel 4. 2. Kodifikasi Sub Kategori NIST CSF (Lanjutan)

Kategori	Sub Kategori	ID
Data Security	PR.DS-1	A.9.1
	PR.DS-8	A.9.8
Information Protection Processes and Procedures	PR.IP-1	A.10.1
	PR.IP-12	A.10.12
Maintenance	PR.MA-1	A.11.1
	PR.MA-2	A.11.2
Protective Technology	PR.PT-1	A.12.1
	PR.PT-5	A.12.5
Anomalies and Events	DE.AE-1	A.13.1
	DE.AE-5	A.13.5
Security Continuous Monitoring	DE.CM-1	A.14.1
	DE.CM-8	A.14.8
Detection Processes	DE.DP-1	A.15.1
	DE.DP-5	A.15.5
Response Planning	RS.RP-1	A.16.1
Communications	RS.CO-1	A.17.1
	RS.CO-5	A.17.5
Analysis	RS.AN-1	A.18.1
	RS.AN-5	A.18.5
Mitigation	RS.MI-1	A.19.1
	RS.MI-3	A.19.3
Improvements	RS.IM-1	A.20.1
	RS.IM-2	A.20.2
Recovery Planning	RC.RP-1	A.21.1
Improvements	RC.IM-1	A.22.1

Tabel 4. 2. Kodifikasi Sub Kategori NIST CSF (Lanjutan)

Kategori	Sub Kategori	ID
	RC.IM-2	A.22.2
Communications systems, victims, other CSIRTs, and vendors).	RC.CO-1	A.23.1
	RC.CO-3	A.23.3

Pada Tabel 4.3. peneliti menetapkan kode ke kontrol pada ISO/IEC 27002, di mana 'B' mewakili ISO/IEC 27002, 'B.1' mewakili kategori *Organisational* pada ISO/IEC 27002 dan 'B.1.1' mewakili control *Policies for information security* di ISO/IEC 27002, dan seterusnya.

Tabel 4. 3. Kodifikasi Kontrol ISO/IEC 27002

Kategori	Kontrol	ID
Organisational	*Policies for information security*	B.1.1
	Documented operating procedures	B.1.37
People	*Screening*	B.2.1
	Information security event reporting	B.2.8
Physical	*Physical security perimeters*	B.3.1
	Secure disposal or re-use of equipment	B.3.14
Technological	*User endpoint devices*	B.4.1
	Protection of information systems during audit testing	B.4.34

Pada Tabel 4.4. peneliti menetapkan kode ke subkontrol CIS Controls v8, di mana 'C' mewakili CIS Controls v8, 'C.1' mewakili kontrol *Inventory and Control of Enterprise Assets* di CIS Controls v8 dan 'C.1.1' mewakili *Establish and Maintain Detailed Enterprise Asset Inventory* di CIS Controls v8, dan seterusnya.

Tabel 4. 4. Kodifikasi Sub Kontrol CIS *Controls* v8

Kontrol	Sub Kontrol	ID
Inventory and Control of Enterprise Assets	*Establish and Maintain Detailed Enterprise Asset Inventory*	C.1.1
	Use a Passive Asset Discovery Tool	C.1.5
Inventory and Control of Software Assets	*Establish and Maintain a Software Inventory*	C.2.1
	Allowlist Authorized Scripts	C.2.7
Data Protection	*Establish and Maintain a Data Management Process*	C.3.1
	Log Sensitive Data Access	C.3.14
Secure Configuration of Enterprise Assets and Software	*Establish and Maintain a Secure Configuration Process*	C.4.1
	Separate Enterprise Workspaces on Mobile End-User Devices	C.4.12
Account Management	*Establish and Maintain an Inventory of Accounts*	C.5.1
	Centralize Account Management	C.5.6
Access Control Management	*Establish an Access Granting Process*	C.6.1
	Define and Maintain Role-Based Access Control	C.6.8
Continuous Vulnerability Management	*Establish and Maintain a Vulnerability Management Process*	C.7.1
	Remediate Detected Vulnerabilities	C.7.7
Audit Log Management	*Establish and Maintain an Audit Log Management Process*	C.8.1
	Collect Service Provider Logs	C.8.12

Tabel 4. 4. Kodifikasi Sub Kontrol CIS *Controls* v8 (Lanjutan)

Kontrol	Sub Kontrol	ID
Email and Web Browser Protections	*Ensure Use of Only Fully Supported Browsers and Email Clients*	C.9.1
	Deploy and Maintain Email Server Anti-Malware Protections	C.9.7
Malware Defenses	*Deploy and Maintain Anti-Malware Software*	C.10.1
	Use Behavior-Based Anti-Malware Software	C.10.7
Data Recovery	*Establish and Maintain a Data Recovery Process*	C.11.1
	Test Data Recovery	C.11.5
Network Infrastructure Management	*Ensure Network Infrastructure is Up-to-Date*	C.12.1
	Establish and Maintain Dedicated Computing Resources for All Administrative	C.12.8
Network Monitoring and Defense	*Centralize Security Event Alerting*	C.13.1
	Tune Security Event Alerting Thresholds	C.13.11
Security Awareness and Skills Training	*Establish and Maintain a Security Awareness Program*	C.14.1
	Conduct Role-Specific Security Awareness and Skills Training	C.14.9
Service Provider Management	*Establish and Maintain an Inventory of Service Providers*	C.15.1
	Securely Decommission Service Providers	C.15.7
Application Software Security	*Establish and Maintain a Secure Application Development Process*	C.16.1
	Conduct Threat Modeling	C.16.14

Tabel 4. 4. Kodifikasi Sub Kontrol CIS *Controls* v8 (Lanjutan)

Kontrol	Sub Kontrol	ID
Incident Response Management	*Designate Personnel to Manage Incident Handling*	C.17.1
	Establish and Maintain Security Incident Thresholds	C.17.9
Penetration Testing	*Establish and Maintain a Penetration Testing Program*	C.18.1
	Perform Periodic Internal Penetration Tests	C.18.5

Peneliti kemudian melakukan analisis terhadap ketiga *framework* tersebut untuk mengelompokkan control ISO/IEC 27002 dan subkontrol CIS Controls v8 dengan subkategori NIST CSF. Pengelompokan tersebut didasarkan pada kesamaan tujuan masing-masing kontrol, subkategori dan subkontrol. Sebagai contoh, pada *function Identify* NIST CSF memiliki sub kategori A.1.1 yang menjelaskan bahwa perangkat fisik dan sistem dalam organisasi harus diinventarisasi. Sub kategori tersebut selaras dengan kontrol pada ISO/IEC 27002 yang menyatakan bahwa suatu inventori informasi dan aset terkait lainnya, termasuk pemiliknya, sebaiknya dikembangkan dan dipelihara, yang dikodifikasi sebagai kontrol B.1.9 pada penelitian ini. Sedangkan pada sub kontrol CIS *Controls* v8, hal tersebut selaras dengan C.1.1 yang menyatakan bahwa organisasi menetapkan dan memelihara inventarisasi aset terperinci. Hasil pengelompokan dapat dilihat pada Tabel 4.5.

Tabel 4. 5. Pemetaan Seluruh Sub Kategori dan Sub Kontrol

Function	Kategori	NIST CSF ID	ISO/IEC 27002 ID	CIS Controls v8 ID
IDENTIFY	*Asset Management*	A.1.1	B.1.9	C.1.1
		A.1.2	B.1.9	C.2.1, C.2.2, C.16.4
		A.1.3	B.1.14	C.3.8
		A.1.4	B.3.9	C.12.4
		A.1.5	B.1.12	C.3.2, C.3.7
		A.1.6	B.1.2	C.14.1
	Business Environment	A.2.1	B.1.21, B.1.22	-
		A.2.2	-	-
		A.2.3	-	-
		A.2.4	B.3.4, B.3.11, B.3.12, B.4.6	-
		A.2.5	B.1.29, B.3.5, B.4.14	-
	Governance	A.3.1	B.1.1	C.14.1
		A.3.2	B.1.2, B.1.4	C.15.2, C.17.4
		A.3.3	B.1.31, B.1.32, B.1.33	-
		A.3.4		-
	Risk Assessment	A.4.1	B.4.8	C.7.1, C.7.2, C.7.4
		A.4.2	B.1.7, B.4.16	-
		A.4.3		-
		A.4.4		-
		A.4.5	B.4.8	C.3.7, C.7.6
		A.4.6		-

Tabel 4. 5. Pemetaan Seluruh Sub Kategori dan Sub Kontrol (Lanjutan)

Function	Kategori	NIST CSF ID	ISO/IEC 27002 ID	CIS Controls v8 ID
IDENTIFY	*Risk Management Strategy*	A.5.1		-
		A.5.2		-
		A.5.3		-
	Supply Chain Risk Management	A.6.1	B.1.19, B.1.20, B.1.21, B.1.22	C.15.2
		A.6.2	B.1.22	C.15.1, C.15.3, C.15.5
		A.6.3	B.1.19, B.1.20, B.1.21	C.15.4
		A.6.4	B.1.22	C.15.5
		A.6.5	B.1.29	C.11.1
PROTECT	*Identity Management, Authentication and Access Control*	A.7.1	B.1.16, B.1.17, B.1.18, B.4.5	C.4.7, C.5.1, C.5.3, C.5.5, C.6.1, C.6.2, C.6.6, C.6.7, C.13.9, C.15.7
		A.7.2	B.3.1, B.3.2, B.3.3, B.3.4, B.3.12	-
		A.7.3	B.1.14, B.2.7, B.4.20	C.4.11, C.6.4, C.6.6, C.12.7, C.13.5
		A.7.4	B.1.15, B.2.8, B.4.2, B.4.3, B.4.18	C.3.3, C.5.4, C.6.8
		A.7.5	B.1.14, B.4.20, B.4.22	C.3.12, C.9.2, C.9.3, C.9.6, C.12.2, C.12.8, C.13.4, C.16.14

Tabel 4. 5. Pemetaan Seluruh Sub Kategori dan Sub Kontrol (Lanjutan)

Function	Kategori	NIST CSF ID	ISO/IEC 27002 ID	CIS Controls v8 ID
PROTECT		A.7.6	B.1.29, B.1.15, B.1.18, B.2.8, B.4.2, B.4.3, B.4.18	-
		A.7.7		C.6.3, C.6.4, C.6.5, C.12.3, C.12.6, C.12.7, C.13.5
	Awareness and Training	A.8.1	B.2.3	C.14.1, C.14.2, C.14.3, C.14.4, C.14.5, C.14.6, C.14.7, C.14.8, C.14.9, C.16.9
		A.8.2	B.1.2, B.2.3	C.14.9, C.16.9
		A.8.3	B.1.2, B.2.3	C.15.4
		A.8.4	B.1.2, B.2.3	C.14.9
		A.8.5	B.3.4	C.14.9
	Data Security	A.9.1	B.4.8	C.3.11, C.16.11
		A.9.2	B.1.10, B.4.20, B.1.14, B.4.26	C.3.10, C.12.3, C.12.6, C.16.11
		A.9.3	B.4.8, B.3.10, B.3.14	C.1.1, C.3.5
		A.9.4	B.4.13	-
		A.9.5	B.1.3, B.1.10, B.1.13, B.1.14, B.1.15, B.2.1, B.2.2, B.2.5, B.4.2, B.4.3, B.4.17, B.4.4, B.4.22, B.4.26	C.3.13, C.3.13, C.16.14

Tabel 4. 5. Pemetaan Seluruh Sub Kategori dan Sub Kontrol (Lanjutan)

Function	**Kategori**	**NIST CSF ID**	**ISO/IEC 27002 ID**	**CIS Controls v8 ID**
PROTECT		A.9.6	B.4.7, B.4.19, B.4.26	C.11.5
		A.9.7	B.4.31	C.16.8
		A.9.8	B.3.13	C.16.14
	Information Protection Processes and Procedures	A.10.1	B.4.32, B.4.9, B.4.19	C.2.7, C.4.11, C.4.2, C.4.3, C.9.1, C.9.4, C.16.7
		A.10.2	B.1.8, B.4.25, B.4.27	C.16.5, C.16.10, C.16.12
		A.10.3	B.4.32, B.4.9, B.4.19	-
		A.10.4	B.1.29, B.1.33, B.4.13	C.11.2, C.11.3
		A.10.5	B.3.4, B.3.5, B.3.11, B.3.12	-
		A.10.6	B.3.10, B.3.14, B.4.8	C.3.1, C.3.5
		A.10.7	-	C.16.14, C.18.1
		A.10.8	B.1.27	-
		A.10.9	B.1.3, B.1.24, B.1.29	C.11.1, C.17.1, C.17.3, C.17.4
		A.10.10	B.1.3	C.17.7
		A.10.11	B.1.34, B.2.1, B.2.5	C.6.2

Tabel 4. 5. Pemetaan Seluruh Sub Kategori dan Sub Kontrol (Lanjutan)

Function	Kategori	NIST CSF ID	ISO/IEC 27002 ID	CIS Controls v8 ID
PROTECT		A.10.12	B.4.8, B.4.36	C.7.6
	Maintenance	A.11.1	B.3.2, B.3.10, B.3.13	-
		A.11.2	B.1.19, B.1.22, B.3.13	C.13.5
	Protective Technology	A.12.1	B.4.15, B.4.17, B.4.34	C.8.2, C.8.4, C.8.8, C.8.11
		A.12.2	B.1.1, B.1.10, B.3.7, B.3.10	C.3.9, C.10.3
		A.12.3	B.1.15	C.2.7, C.13.10
		A.12.4	B.1.14, B.4.20	-
		A.12.5	B.1.29, B.4.14	C.11.4
DETECT	*Anomalies and Events*	A.13.1	B.4.16	C.3.8
		A.13.2	B.1.24, B.1.25	C.8.11
		A.13.3	-	C.8.2, C.8.5, C.8.6, C.8.7, C.8.8, C.8.12
		A.13.4	-	-
		A.13.5	-	C.13.11
	Security Continuous Monitoring	A.14.1	B.4.16	C.8.5, C.13.2, C.13.3, C.13.6, C.13.7, C.13.8
		A.14.2	B.3.4	-
		A.14.3	B.4.15	-

Tabel 4. 5. Pemetaan Seluruh Sub Kategori dan Sub Kontrol (Lanjutan)

Function	Kategori	NIST CSF ID	ISO/IEC 27002 ID	CIS Controls v8 ID
DETECT		A.14.4	B.4.7	C.9.7, C.10.1, C.10.2, C.10.4, C.10.5, C.10.6, C.10.7
		A.14.5	B.4.16, B.4.19	-
		A.14.6	B.4.30, B.1.22	C.15.6
		A.14.7	B.4.16	C.1.3, C.1.4, C.1.5, C.2.3, C.2.4, C.2.5, C.2.6, C.9.6
		A.14.8	B.4.8	C.7.5
	Detection Processes	A.15.1	B.1.2	C.17.1, C.17.4
		A.15.2	B.1.34	-
		A.15.3	B.4.29	-
		A.15.4	B.2.8	C.17.5
		A.15.5	B.1.27	-
RESPOND	*Response Planning*	A.16.1	B.1.26	-
	Communications	A.17.1	B.1.2, B.1.24	C.17.2, C.17.4
		A.17.2	B.2.8	C.17.5
		A.17.3	B.2.8	C.17.5
		A.17.4	-	C.17.5
		A.17.5	-	-
	Analysis	A.18.1	B.1.26, B.4.15, B.4.16	C.8.11, C.16.3, C.16.6

Tabel 4. 5. Pemetaan Seluruh Sub Kategori dan Sub Kontrol (Lanjutan)

Function	Kategori	NIST CSF ID	ISO/IEC 27002 ID	CIS Controls v8 ID
RESPOND		A.18.2	B.1.27	-
		A.18.3	B.1.28	-
		A.18.4	B.1.25	C.17.9
		A.18.5	B.1.26	C.16.2
	Mitigation	A.19.1	B.1.26, B.4.7	-
		A.19.2	B.4.8	-
		A.19.3	B.1.27	-
	Improvements	A.20.1	-	C.17.8
		A.20.2	-	C.17.8
RECOVER	*Recovery Planning*	A.21.1	B.1.26	-
	Improvements	A.22.1	-	-
		A.22.2	-	-
	Communications	A.23.1	-	-
		A.23.2	-	-
		A.23.3	-	-

Hasil pengelompokan pada Tabel 4.5 disesuaikan kembali menjadi pemetaan pada Tabel 4.6 agar lebih mudah dalam pembacaan hasil integrasi kerangka kerja.

Tabel 4. 6. Penyesuaian Integrasi Kerangka Kerja

Function	*Category*	*Subcategory*	*Informative References*
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-1**	- **ISO/IEC 27002:2022** A.5.9
			- **CIS Control V8** 1.1
		ID.AM-2	- **ISO/IEC 27002:2022** A.5.9
			- **CIS Control V8** 2.1, 2.2, 16.4
		ID.AM-3	- **ISO/IEC 27002:2022** A.5.14
			- **CIS Control V8** 3.8

Tabel 4. 6. Penyesuaian Integrasi Kerangka Kerja (Lanjutan)

Function	*Category*	*Subcategory*	*Informative References*
		ID.AM-4	· **ISO/IEC 27002:2022** A.7.9
			· **CIS Control V8** 12.4
		ID.AM-5	· **ISO/IEC 27002:2022** A.5.12
			· **CIS Control V8** 3.2, 3.7
		ID.AM-6	· **ISO/IEC 27002:2022** A.5.2
			· **CIS Control V8** 14.1
	Business Environment (ID.BE)	**ID.BE-1**	· **ISO/IEC 27002:2022** A.5.21, A.5.22
		ID.BE-2	-
		ID.BE-3	-
		ID.BE-4	· **ISO/IEC 27002:2022** A.7.4, A.7.11, A.7.12, 8.6
		ID.BE-5	· **ISO/IEC 27002:2022** A.7.5, A.5.29, A.8.14
	Governance (ID.GV)	**ID.GV-1**	· **ISO/IEC 27002:2022** A.5.1
			· **CIS Control V8** 14.1
		ID.GV-2	· **ISO/IEC 27002:2022** A.5.2, A.5.4
			· **CIS Control V8** 15.2, 17.4
		ID.GV-3	· **ISO/IEC 27002:2022** A.5.31, A.5.32, A.5.33
		ID.GV-4	
	Risk Assessment (ID.RA)	**ID.RA-1**	· **ISO/IEC 27002:2022** A.8.8
			· **CIS Control V8** 7.1, 7.2, 7.4
		ID.RA-2	· **ISO/IEC 27002:2022** A.8.16, A.5.7
		ID.RA-3	-
		ID.RA-4	-
		ID.RA-5	· **ISO/IEC 27002:2022** A.8.8
			· **CIS Control V8** 3.7, 7.6
		ID.RA-6	-
	Risk Management Strategy (ID.RM)	**ID.RM-1**	-
		ID.RM-2	-
		ID.RM-3	-
	Supply Chain Risk Management (ID.SC)	**ID.SC-1**	· **ISO/IEC 27002:2022** A.5.19, A.5.20, A.5.21, A.5.22
			· **CIS Control V8** 15.2
		ID.SC-2	· **ISO/IEC 27002:2022** A.5.22
			· **CIS Control V8** 15.1, 15.3, 15.5
		ID.SC-3	· **ISO/IEC 27002:2022** A.5.19, A.5.20, A.5.21

Tabel 4. 6. Penyesuaian Integrasi Kerangka Kerja (Lanjutan)

Function	*Category*	*Subcategory*	*Informative References*
			· **CIS Control V8** 15.4
		ID.SC-4	· **ISO/IEC 27002:2022** A.5.22
			· **CIS Control V8** 15.5
		ID.SC-5	· **ISO/IEC 27002:2022** A.5.29
			· **CIS Control V8** 11.1
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC)**	**PR.AC-1**	· **ISO/IEC 27002:2022** A.5.16, A.5.17, A.5.18, A.8.5
			· **CIS Control V8** 4.7, 5.1, 5.3, 5.5, 6.1, 6.2, 6.6, 6.7, 13.9, 15.7
		PR.AC-2	· **ISO/IEC 27002:2022** A.7.1, A.7.2, A.7.3, A.7.4, A.7.12
		PR.AC-3	· **ISO/IEC 27002:2022** A.5.14, A.6.7, A.8.20
			· **CIS Control V8** 4.11, 6.4, 6.6, 12.7, 13.5
		PR.AC-4	· **ISO/IEC 27002:2022** A.5.15, A.6.8, A.8.2, A.8.3, A.8.18
			· **CIS Control V8** 3.3, 5.4, 6.8
		PR.AC-5	· **ISO/IEC 27002:2022** A.5.14, A.8.20, A.8.22
			· **CIS Control V8** 3.12, 9.2, 9.3, 9.6, 12.2, 12.8, 13.4, 16.14
		PR.AC-6	· **ISO/IEC 27002:2022** A.5.29, A.6.8, A.5.15, A.5.18, A.8.2, A.8.3, A.8.18
		PR.AC-7	· **CIS Control V8** 6.3, 6.4, 6.5, 12.3, 12.6, 12.7, 13.5
	Awareness and Training (PR.AT)	**PR.AT-1**	· **ISO/IEC 27002:2022** A.6.3
			· **CIS Control V8** 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9, 16.9, 17.3
		PR.AT-2	· **ISO/IEC 27002:2022** A.5.2, A.6.3
			· **CIS Control V8** 14.9, 16.9
		PR.AT-3	· **ISO/IEC 27002:2022** A.5.2, A.6.3
			· **CIS Control V8** 15.4
		PR.AT-4	· **ISO/IEC 27002:2022** A.5.2, A.6.3
			· **CIS Control V8** 14.9
		PR.AT-5	· **ISO/IEC 27002:2022** A.7.4
			· **CIS Control V8** 14.9
	Data Security (PR.DS)	**PR.DS-1**	· **ISO/IEC 27002:2022** A.8.8
			· **CIS Control V8** 3.11, 16.11
		PR.DS-2	· **ISO/IEC 27002:2022** A.5.10, A.8.20, A.5.14, A.8.26

Tabel 4. 6. Penyesuaian Integrasi Kerangka Kerja (Lanjutan)

Function	*Category*	*Subcategory*	*Informative References*
			· **CIS Control V8** 3.10, 12.3, 12.6, 16.11
		PR.DS-3	· **ISO/IEC 27002:2022** A.8.8, A.7.10, A.7.14
			· **CIS Control V8** 1.1, 3.5
		PR.DS-4	· **ISO/IEC 27002:2022** A.8.13
		PR.DS-5	· **ISO/IEC 27002:2022** A.5.3, A.6.1, A.6.2, A.6.5, A.5.13, A.5.10, A.5.15, A.8.2, A.8.3, A.8.17, A.8.4, A.8.22, A.5.14, A.8.26
			· **CIS Control V8** 3.13, 3.13, 16.14
		PR.DS-6	· **ISO/IEC 27002:2022** A.8.7, A.8.19, A.8.26
			· **CIS Control V8** 11.5
		PR.DS-7	· **ISO/IEC 27002:2022** A.8.31
			· **CIS Control V8** 16.8
		PR.DS-8	· **ISO/IEC 27002:2022** A.7.13
			· **CIS Control V8** 16.14
	Information Protection Processes and Procedures (PR.IP)	**PR.IP-1**	· **ISO/IEC 27002:2022** A.8.32, A.8.9, A.8.19
			· **CIS Control V8** 2.7, 4.1, 4.2, 4.3, 9.1, 9.4, 16.7
		PR.IP-2	· **ISO/IEC 27002:2022** A.5.8, A.8.25, A.8.27
			· **CIS Control V8** 16.5, 16.10, 16.12
		PR.IP-3	· **ISO/IEC 27002:2022** A.8.32, A.8.9, A.8.19
		PR.IP-4	· **ISO/IEC 27002:2022** A.8.13, A.5.29, A.5.33
			· **CIS Control V8** 11.2, 11.3
		PR.IP-5	· **ISO/IEC 27002:2022** A.7.4, A.7.5, A.7.11, A.7.12
		PR.IP-6	· **ISO/IEC 27002:2022** A.8.8, A.7.10, A.7.14
			· **CIS Control V8** 3.1, 3.5
		PR.IP-7	· **CIS Control V8** 16.14, 18.1
		PR.IP-8	· **ISO/IEC 27002:2022** A.5.27
		PR.IP-9	· **ISO/IEC 27002:2022** A.5.24, A.5.29, A.5.3
			· **CIS Control V8** 11.1, 17.1, 17.3, 17.4
		PR.IP-10	· **ISO/IEC 27002:2022** A.5.3
			· **CIS Control V8** 17.7

Tabel 4. 6. Penyesuaian Integrasi Kerangka Kerja (Lanjutan)

Function	*Category*	*Subcategory*	*Informative References*
		PR.IP-11	· **ISO/IEC 27002:2022** A.6.1, A.6.5, A.5.34
			· **CIS Control V8** 6.2
		PR.IP-12	· **ISO/IEC 27002:2022** A.8.8, A.5.36
			· **CIS Control V8** 7.6
	Maintenance (PR.MA)	PR.MA-1	· **ISO/IEC 27002:2022** A.7.2, A.7.10, A.7.13
		PR.MA-2	· **ISO/IEC 27002:2022** A.7.13, A.5.19, A.5.22
			· **CIS Control V8** 13.5
	Protective Technology (PR.PT)	PR.PT-1	· **ISO/IEC 27002:2022** A.8.15, A.8.17, A.8.34
			· **CIS Control V8** 8.2, 8.4, 8.8, 8.11
		PR.PT-2	· **ISO/IEC 27002:2022** A.5.1, A.5.10, A.7.7, A.7.10
			· **CIS Control V8** 3.9, 10.3
		PR.PT-3	· **ISO/IEC 27002:2022** A.5.15
			· **CIS Control V8** 2.7, 13.10
		PR.PT-4	· **ISO/IEC 27002:2022** A.8.20, A.5.14
		PR.PT-5	· **ISO/IEC 27002:2022** A.5.29, A.8.14
			· **CIS Control V8** 11.4
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1	· **ISO/IEC 27002:2022** A.8.16
			· **CIS Control V8** 3.8
		DE.AE-2	· **ISO/IEC 27002:2022** A.5.24, A.5.25
			· **CIS Control V8** 8.11
		DE.AE-3	· **CIS Control V8** 8.2, 8.5, 8.6, 8.7, 8.8, 8.12
		DE.AE-4	-
		DE.AE-5	· **CIS Control V8** 13.11
	Security Continuous Monitoring (DE.CM)	DE.CM-1	· **ISO/IEC 27002:2022** A.8.16
			· **CIS Control V8** 8.5, 13.2, 13.3, 13.6, 13.7, 13.8
		DE.CM-2	· **ISO/IEC 27002:2022** A.7.4
		DE.CM-3	· **ISO/IEC 27002:2022** A.8.15
		DE.CM-4	· **ISO/IEC 27002:2022** A.8.7
			· **CIS Control V8** 9.7, 10.1, 10.2, 10.4, 10.5, 10.6, 10.7
		DE.CM-5	· **ISO/IEC 27002:2022** A.8.16, A.8.19

Tabel 4. 6. Penyesuaian Integrasi Kerangka Kerja (Lanjutan)

Function	*Category*	*Subcategory*	*Informative References*
		DE.CM-6	· **ISO/IEC 27002:2022** A.8.30, A.5.22
			· **CIS Control V8** 15.6
		DE.CM-7	· **ISO/IEC 27002:2022** A.8.16
			· **CIS Control V8** 1.3, 1.4, 1.5, 2.3, 2.4, 2.5, 2.6, 9.6
		DE.CM-8	· **ISO/IEC 27002:2022** A.8.8
			· **CIS Control V8** 7.5
	Detection Processes (DE.DP)	DE.DP-1	· **ISO/IEC 27002:2022** A.5.2
			· **CIS Control V8** 17.1, 17.4
		DE.DP-2	· **ISO/IEC 27002:2022** A.5.34
		DE.DP-3	· **ISO/IEC 27002:2022** A.8.29
		DE.DP-4	· **ISO/IEC 27002:2022** A.6.8
			· **CIS Control V8** 17.5
		DE.DP-5	· **ISO/IEC 27002:2022** A.5.27
RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1	· **ISO/IEC 27002:2022** A.5.26
	Communications (RS.CO)	RS.CO-1	· **ISO/IEC 27002:2022** A.5.2, A.5.24
			· **CIS Control V8** 17.2, 17.4
		RS.CO-2	· **ISO/IEC 27002:2022** A.6.8
			· **CIS Control V8** 17.5
		RS.CO-3	· **ISO/IEC 27002:2022** A.6.8
			· **CIS Control V8** 17.5
		RS.CO-4	· **CIS Control V8** 17.5
		RS.CO-5	-
	Analysis (RS.AN)	RS.AN-1	· **ISO/IEC 27002:2022** A.8.15, A.8.16, A.5.26
			· **CIS Control V8** 8.11, 16.3, 16.6
		RS.AN-2	· **ISO/IEC 27002:2022** A.5.27
		RS.AN-3	· **ISO/IEC 27002:2022** A.5.28
		RS.AN-4	· **ISO/IEC 27002:2022** A.5.25
			· **CIS Control V8** 17.9
		RS.AN-5	· **CIS Control V8** 16.2
	Mitigation (RS.MI)	RS.MI-1	· **ISO/IEC 27002:2022** A.5.26
		RS.MI-2	· **ISO/IEC 27002:2022** A.8.27, A.5.26
		RS.MI-3	· **ISO/IEC 27002:2022** A.8.8
	Improvements (RS.IM)	RS.IM-1	· **ISO/IEC 27002:2022** A.5.27

Tabel 4. 6. Penyesuaian Integrasi Kerangka Kerja (Lanjutan)

Function	*Category*	*Subcategory*	*Informative References*
			· **CIS Control V8** 17.8
		RS.IM-2	· **CIS Control V8** 17.8
RECOVER (RC)	**Recovery Planning (RC.RP)**	**RC.RP-1**	· **ISO/IEC 27002:2022** A.5.26
	Improvements (RC.IM)	**RC.IM-1**	-
		RC.IM-2	-
	Communications (RC.CO)	**RC.CO-1**	-
		RC.CO-2	-
		RC.CO-3	-

Setelah penyesuaian integrasi kerangka kerja, hasil integrasi kerangka kerja akan digunakan sebagai dasar pertanyaan pada *Tools* Evaluasi sebagaimana contoh yang tercantum pada Tabel 4.7 yang akan diajukan pada *stakeholders* untuk mengidentifikasi kondisi saat ini.

Tabel 4. 7. Contoh Pertanyaan dalam *Tools* Evaluasi

Function	*Category*	*Subcategory*	No	Pertanyaan
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	1	Apakah organisasi memiliki inventaris lengkap yang mencakup semua perangkat fisik dan sistem yang digunakan dalam operasional?
			2	Apakah organisasi memastikan bahwa inventaris perangkat fisik diperbarui secara berkala untuk mencakup perangkat baru dan perangkat yang tidak lagi digunakan?
			3	Apakah organisasi menggunakan alat penemuan aktif untuk mengidentifikasi perangkat yang terhubung ke jaringan dan memperbarui inventaris perangkat keras?

Tabel 4. 7. Contoh Pertanyaan dalam *Tools* Evaluasi (Lanjutan)

Function	*Category*	*Subcategory*	No	Pertanyaan
			4	Apakah organisasi memastikan bahwa semua aset informasi diberi label dan diklasifikasikan sesuai dengan kepentingannya?
			5	Apakah ada prosedur untuk memastikan bahwa perangkat yang hilang atau dicuri segera dilaporkan dan ditindaklanjuti?
			6	Bagaimana organisasi melacak lokasi fisik dan status kepemilikan perangkat?
			7	Bagaimana organisasi menangani perangkat yang teridentifikasi tetapi tidak diotorisasi untuk terhubung ke jaringan?
			8	Apakah ada kebijakan yang mengatur langkah-langkah yang harus diambil ketika perangkat tidak diotorisasi ditemukan?

4.3. Identifikasi Kondisi Saat Ini Menggunakan Integrasi Kerangka Kerja

Setelah pemetaan dan integrasi kerangka kerja dilakukan, maka langkah selanjutnya ialah mengidentifikasi kondisi keamanan siber di Pusat Data Kota Tangerang Selatan saat ini. Identifikasi akan dilakukan menggunakan hasil integrasi kerangka kerja yang dirinci menjadi pertanyaan-pertanyaan pada *Tools* Evaluasi secara lengkap yang terlampir pada Lampiran, dan diajukan kepada pengelola Pusat Data Kota Tangerang Selatan. Sebagai contoh pertanyaan yang diberikan, pada *function Identify*, kategori *Asset Management*, sub kategori ID.AM-1 pada NIST CSF, kontrol A.5.9 pada ISO/IEC 27002, dan sub kontrol 1.1 pada CIS *Controls* v8 adalah "Apakah organisasi memiliki inventaris lengkap yang mencakup semua perangkat fisik dan sistem yang digunakan dalam operasional?".

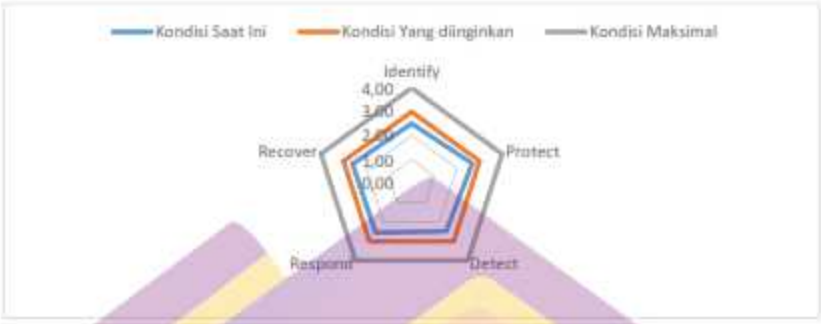
Jawaban dari pertanyaan tersebut akan disesuaikan dengan *tier* yang ada pada kerangka kerja NIST CSF, yaitu *tier* 1 (*partial*) dengan kondisi bahwa belum ada dokumentasi terkait dengan inventaris aset perangkat fisik, *tier* 2 (*risk informed*) dengan kondisi adanya inventaris aset perangkat fisik, tetapi tidak mencakup semua perangkat atau tidak diperbarui secara berkala, *tier* 3 (*repeatable*) dengan kondisi inventaris aset perangkat fisik lengkap dan diperbarui secara berkala, atau *tier* 4 (*adaptive*) dengan kondisi inventaris aset perangkat fisik lengkap, akurat, dan diperbarui secara real-time dengan teknologi otomatisasi.. Setelah data dikumpulkan, didapatkan hasil bahwa Pusat Data Kota Tangerang Selatan berada pada *tier* 2 pada seluruh *function* sesuai dengan Tabel 4.8.

Setelah identifikasi kondisi saat ini telah didefinisikan, tahapan selanjutnya ialah mengidentifikasi kondisi yang ingin dicapai. Setelah dilakukan identifikasi, kondisi yang diinginkan untuk setiap *function* yaitu berada pada *tier* 3 NIST CSF, yaitu *repeatable*.

Tabel 4. 8. Hasil Identifikasi Kondisi Saat Ini dan Kondisi yang Ingin Dicapai

Function	**Kondisi Saat Ini**	**Kondisi yang Ingin Dicapai**
Identify	2,51	3
Protect	2,68	3
Detect	2,48	3
Respond	2,56	3
Recover	2,6	3
Total Rata-Rata	**2**	**3**

Hasil identifikasi juga dapat dilihat dalam bentuk bagan pada Gambar 5.



Gambar 4. 1. Bagan Hasil Identifikasi

4.4. Hasil Evaluasi

Dari hasil identifikasi kondisi saat ini, dalam *function Identify* Pusat Data Kota Tangerang Selatan memiliki kelemahan dalam pencatatan katalog sistem informasi eksternal, identifikasi peran rantai pasok, dan uji coba rencana respons insiden. Organisasi juga belum secara optimal menerapkan pencatatan aset perangkat fisik dan lunak, penerapan *Data Masking* dan *Data Leakage Prevention*, evaluasi rutin terhadap kegiatan *Security Awareness*, dan manajemen risiko pemasok.

Pada *function Protect*, memiliki kelemahan pada *security awareness* terhadap pemasok, implementasi *Data Leakage Prevention Tools*, *integrity monitoring* dan enkripsi terhadap *portable media*. Organisasi juga belum secara optimal menerapkan peningkatan kapasitas pegawai terkait keamanan siber, dokumentasi terhadap insiden dan penanganannya, penerapan redundansi layanan, dan pengujian terhadap rencana respons insiden.

Lalu pada *function Detect*, memiliki kelemahan pada penerapan pembatasan ekstensi *file* dan *script*, monitoring terhadap penggunaan aplikasi di tiap-tiap aset,

proses uji coba deteksi, dan reviu serta evaluasi terhadap proses deteksi. Organisasi juga belum secara optimal menerapkan penggunaan anti malware secara terpusat, kepatuhan proses deteksi terhadap standar, dan peningkatan kapasitas personil terhadap kegiatan deteksi.

Pada *function Respond,* organisasi memiliki kelemahan yaitu belum diterapkannya pelaksanaan digital forensik, dan pengujian rencana respons. Organisasi juga belum secara optimal pelaksanaan investigasi terhadap insiden sampai akar masalah, dan pembaruan strategi rencana respons sesuai dengan tren insiden saat ini.

Pada *function Recover,* organisasi memiliki kelemahan yaitu belum dilakukannya evaluasi terhadap rencana pemulihan setelah insiden organisasi. Organisasi juga belum secara optimal mereviu dan melakukan pembaruan terhadap dokumen BCP.

Tabel 4. 9. Analisis Kesenjangan

Function	**Kondisi saat ini**	**Kondisi yang ingin dicapai**	**Kesenjangan**
Identify	2,51	3	0,49
Protect	2,71	3	0,29
Detect	2,28	3	0,72
Respond	2,56	3	0,44
Recover	2,5	3	0,5

4.5. Hasil Rekomendasi

Di tahap akhir penelitian ini, peneliti membuat hasil rekomendasi yang harus dilakukan untuk mengatasi kesenjangan untuk mencapai kondisi yang diinginkan.

Adapun rekomendasi yang diberikan adalah sebagai berikut (rincian terdapat pada Lampiran):

Tabel 4. 10. Rincian Rekomendasi

No.	Rekomendasi	Tenggat Waktu Pengerjaan
1.	Menerapkan active discovery asset tools seperti Cacti, Nagios, Solarwind.	Q4 2024
2.	Mengoptimalkan dan memantau pelaksanaan Prosedur dalam kebijakan Manajemen Aset	Q4 2024
3.	Menerapkan pembatasan user untuk menginstall aplikasi sehingga perlu hak akses khusus	Q4 2024
4.	Membuat kebijakan atau prosedur terkait penanganan perangkat lunak yang tidak diotorisasi	Q4 2024
5.	Mengoptimalkan dan memantau pelaksanaan Kebijakan Data Masking dan DLP	Q4 2024
6.	Mengoptimalkan proses pemulihan dan pengujian data cadangan	Q4 2024
7.	Memperbarui katalog layanan hingga sistem informasi eksternal	Q1 2025
8.	Mengoptimalkan proses untuk memperbarui katalog layanan	Q1 2025
9.	Membuat kebijakan atau prosedur untuk mengendalikan akses ke sistem informasi eksternal	Q1 2025
10.	Merencanakan program evaluasi terhadap pemahaman Security Awareness yang diberikan	Q1 2025
11.	Membuat rincian peran fungsi dari tiap rantai pasok	Q4 2024
12.	Membuat jalur komunikasi yang mudah dilakukan ke tiap rantai pasok	Q4 2024
13.	Membuat kerangka kerja untuk melakukan manajemen risiko terkait rantai pasok	Q1 2025
14.	Melakukan penilaian risiko terhadap rantai pasok dan lakukan pemantauan	Q1 2025
15.	Mengoptimalkan proses review terhadap pihak ketiga	Q4 2024
16.	Melakukan pengujian terhadap skenario yang telah ditetapkan di dalam dokumen BCP	Q4 2024

Tabel 4.10. Rincian Rekomendasi (Lanjutan)

No.	Rekomendasi	Tenggat Waktu Pengerjaan
17.	Melakukan review terhadap dokumen BIA	Q4 2024
18.	Lakukan perencanaan uji coba skenario pemulihan dan respons dengan pemasok pada BCP	Q4 2024
19.	Mengoptimalkan dan memantau pengelolaan dan evaluasi user account pengguna di sistem	Q4 2024
20.	Mengoptimalkan dan memantau pelaksanaan prosedur alih data dan informasi	Q1 2025
21.	Lakukan penjadwalan terhadap pelatihan terhadap seluruh pegawai dan pimpinan	Q1 2025
22.	Lakukan security awareness secara formal ke pihak ketiga	Q1 2025
23.	Pembuatan prosedur penyimpanan data-at-rest	Q4 2024
24.	Lakukan pengadaan redundansi, seperti genset dan colocation server	Akan disesuaikan dengan ketersediaan anggaran
25.	Lakukan pemantauan terhadap pelaksanaan pemisahan environment development dan production	Q1 2025
26.	Lakukan pemantauan terhadap pelaksanaan versioning	Q4 2024
27.	Lakukan pemantauan terhadap penerapan kebijakan retensi data	Q1 2025
28.	Membuat prosedur khusus untuk dapat mengukur dan mengevaluasi efektivitas teknologi proteksi	Q1 2025
29.	Lakukan enkripsi terhadap media portable	Q4 2024
30.	Lakukan penerapan failsafe, load balancing, dan hot swap secara menyeluruh di semua sistem	Akan disesuaikan dengan kebutuhan sistem
31.	Lakukan penerapan anti malware yang bisa dikontrol secara terpusat	Akan disesuaikan dengan ketersediaan anggaran
32.	Lakukan pembatasan penggunaan script yang bisa didokumentasikan di dalam Standar Konfigurasi maupun Whitelist Aplikasi	Q1 2025
33.	Lakukan pemantauan terhadap pihak ketiga dan layanan-layanan eksternal yang terhubung	Q4 2024
34.	Lakukan peningkatan konsistensi terhadap kegiatan deteksi	Q4 2024
35.	Lakukan dokumentasi terkait kepatuhan persyaratan dan regulasi mengenai deteksi	Q1 2025
36.	Lakukan pengujian proses deteksi untuk memastikan efektivitas proses	Q1 2025

Tabel 4.10. Rincian Rekomendasi (Lanjutan)

No.	Rekomendasi	Tenggat Waktu Pengerjaan
37.	Lakukan evaluasi proses deteksi dan dokumentasikan	Q1 2025
38.	Lakukan proses analisis akar masalah secara konsisten terhadap seluruh insiden	Q4 2024
39.	Lakukan pembuatan prosedur untuk Digital Forensik	Q4 2024
40.	Lakukan pembuatan prosedur penanganan insiden sesuai dengan kategori insiden	Q1 2025

Setelah pemberian rekomendasi, diharapkan organisasi mampu melaksanakan seluruh rekomendasi yang diberikan agar dapat memenuhi kondisi yang diinginkan seperti yang ditampilkan pada Tabel 4.10. Pusat Data Dinas Komunikasi dan Informatika Kota Tangerang Selatan diharapkan melaksanakan dan mengelola usulan rekomendasi yang telah ditetapkan dan disetujui oleh *top management* sesuai dengan tenggat waktu yang telah disepakati.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan evaluasi kondisi saat ini yang dilakukan terhadap Pusat Data Kota Tangerang Selatan menggunakan kerangka kerja hasil dari pemetaan kerangka kerja ISO/IEC 27002 dan CIS Controls v8 ke dalam kerangka kerja NIST CSF, didapatkan hasil skor 2.51 pada *function Identify*, 2.68 pada *function Protect*, 2.48 pada *function Detect*, 2.56 pada *function Respond*, dan 2.6 pada *function Recover*. Berdasarkan hasil evaluasi tersebut, terdapat kesenjangan 0.49 pada *function Identify*, 0.32 pada *function Protect*, 0.52 pada *function Detect*, 0.44 pada *function Respond*, dan 0.4 pada *function Recover* terhadap identifikasi kondisi yang diinginkan, yaitu 3 pada seluruh *function*. Berdasarkan hasil tersebut, peneliti merumuskan rekomendasi, di mana terdapat 40 (empat puluh) rekomendasi untuk keseluruhan *function*.

Penelitian ini menemukan bahwa kerangka kerja NIST CSF yang diintegrasikan dengan ISO/IEC 27002 dan CIS *Controls* v8 dapat digunakan sebagai alat evaluasi penerapan keamanan siber di Pusat Data Kota Tangerang Selatan. NIST CSF tidak memadai jika digunakan sendiri dalam evaluasi penerapan keamanan siber, karena beberapa konsepnya kurang lengkap dan tidak cukup detail untuk mengukur tingkat penerapan keamanan siber.

Pemetaan antara ketiga kerangka kerja ini juga memberikan panduan yang lebih jelas dan terstruktur dalam mengidentifikasi, melindungi, mendeteksi,

merespons, dan memulihkan diri dari insiden siber. Dengan demikian, penerapan keamanan siber yang lebih efektif dan efisien dapat tercipta untuk mengurangi risiko dan dampak yang diakibatkan oleh ancaman siber, sehingga *Service Level Agreement* (SLA) dan kualitas layanan di Pusat Data Kota Tangerang Selatan dapat meningkat.

5.2. Saran

Dalam penelitian ini, integrasi kerangka kerja dapat dilakukan lebih komprehensif, dengan mengikutsertakan metode *Implementation Group* pada CIS *Controls* v8 agar evaluasi dapat disesuaikan dengan level *Implementation Group* pada organisasi. Pada penelitian ini, NIST CSF yang digunakan adalah versi 1.1. Dimungkinkan untuk penelitian selanjutnya menggunakan kerangka kerja dengan versi yang paling terbaru agar hasil integrasi kerangka kerja dapat menghasilkan kerangka kerja yang lebih komprehensif. Bahkan kerangka kerja lain pun dapat diintegrasikan pula untuk mengisi sub kategori NIST CSF yang belum dapat dipetakan oleh ISO/IEC 27002 maupun CIS *Controls* v8.

DAFTAR PUSTAKA

Ahyar, H. (2020). Buku Metode Penelitian Kualitatif & Kuantitatif (A. Husnu (ed.); 1 ed.). CV. Pustaka Ilmu Group.

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. Computer Science & Information Technology (CS & IT), 7(3), 51-62.

Amiruddin, A., Afiansyah, H. G., & Nugroho, H. A. (2021, October). Cyber-Risk Management Planning Using NIST CSF v1. 1, NIST SP 800-53 Rev. 5, and CIS Controls v8. In 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS (pp. 19-24). IEEE.

Bashofi, I., & Salman, M. (2022, June). Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. In 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom) (pp. 58-62). IEEE.

BSSN. (2023). Laporan Tahunan Honeynet Project 2023.

CIS. (2021). CIS Controls CIS Controls Version 8.

Fadila, V., Mutiah, N., & Sari, R. P. Cyber Security Audit using CIS CSC, NIST CSF and COBIT 2019 Framework. CESS (Journal of Computer Engineering, System and Science), 8(2), 271-283.

ISO/IEC. (2022). International Standard ISO/IEC 27002, 4th ed., vol. 4.

Jufri Mt., Hendayun M., Suharto T. (2017). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. Second International Conference on Informatics and Computing (ICIC).

Mahendra, V. I. C. K. Y. (2023). Perancangan Kerangka Kerja Keamanan Siber Menggunakan NIST Cybersecurity Framework dan CIS Controls. Universitas Bina Nusantara, Jakarta.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

Pemerintah Indonesia. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182. Sekretariat Negara. Jakarta.

Roy P Prameet. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. IEEE.

Straub, Jeremy. (2020). Software Engineering: The First Line of Defense for Cybersecurity. IEEE 11th International Conference on Software Engineering and Service Science (ICSESS).

Sugiyono. (2013). Metode Penelitian Kuantitatif, Kualitatif Dan R &. D. Bandung Alfabeta.

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), 225-230.

Wali Kota Tangerang Selatan. (2022). Peraturan Wali Kota Tangerang Selatan Nomor 56 Tahun 2022 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi, Dan Tata Kerja Dinas Komunikasi Dan Informatika. Berita Daerah Kota Tangerang Selatan Tahun 2022 Nomor 62. Pemerintah Kota Tangerang Selatan.

LAMPIRAN

Tools Evaluasi

Function	Category	Subcategory	No	Pertanyaan	Level Implementasi	Keterangan	Level Kondisi yang diinginkan	Rekomendasi
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	1	Apakah organisasi memiliki inventaris lengkap yang mencakup semua perangkat fisik dan sistem yang digunakan dalam operasional?	3	Inventaris lengkap dan diperbarui secara berkala dan sudah disahkan oleh Top Management di dalam dokumen Asset Register	3	Sudah Tercapai
			2	Apakah organisasi memastikan bahwa inventaris perangkat fisik diperbarui secara berkala untuk mencakup perangkat baru dan perangkat yang tidak lagi digunakan?	3	Proses revisi formal dan dokumentasi ada untuk memperbarui inventaris secara berkala	3	Sudah Tercapai
			3	Apakah organisasi menggunakan *active discovery asset tools* untuk mengidentifikasi perangkat yang terhubung ke jaringan dan memperbarui inventaris perangkat secara?	1	Tidak ada penggunaan *active discovery asset tools*	3	Menerapkan *active discovery asset tools* seperti Cacti, Nagios, Solarwind
			4	Apakah organisasi memastikan bahwa semua aset informasi diberi label dan diklasifikasikan sesuai dengan kepentingannya?	3	Proses pelabelan dan klasifikasi ditempkan secara konsisten dan diperbarui secara berkala	3	Sudah Tercapai
			5	Apakah ada prosedur untuk memastikan bahwa perangkat yang hilang atau dicuri segera dilaporkan dan ditindaklanjuti?	2	Prosedur dalam kebijakan Manajemen Aset, tetapi tidak selalu diterapkan atau tidak efektif	3	Mengoptimalkan dan memantau pelaksanaan Prosedur dalam kebijakan Manajemen Aset
			6	Bagaimana organisasi melacak lokasi fisik dan status kepemilikan perangkat?	3	Proses pelacakan aset secara formal dan diterapkan secara konsisten, berupa dokumen Rekap Keluar Masuk Aset	3	Sudah Tercapai

			7	Bagaimana organisasi menangani perangkat yang teridentifikasi tetapi tidak diotorisasi untuk terhubung ke jaringan?	3	Sudah dilakukan penerapan *captive portal* terhadap jaringan	3	Sudah Tercapai
		ID.AM-2: Software platforms and applications within the organization are inventoried	1	Apakah organisasi memiliki inventaris lengkap yang mencakup semua platform perangkat lunak dan aplikasi yang digunakan dalam operasional?	3	Sudah dilakukan inventarisasi perangkat lunak ada dalam dokumen Asset Register	3	Sudah Tercapai
			2	Bagaimana organisasi memastikan bahwa inventaris perangkat lunak diperbarui secara berkala untuk mencakup perangkat lunak baru dan perangkat lunak yang tidak lagi digunakan?	3	Proses untuk memperbarui inventaris perangkat lunak ada dalam Sistem Keamanan Informasi	3	Sudah Tercapai
			3	Bagaimana organisasi memastikan bahwa hanya perangkat lunak yang diotorisasi yang dimuat pada sistem?	2	Kebijakan ada dalam Dokumen Whitelist Aplikasi, tetapi tidak selalu diterapkan atau efektif.	3	Menerapkan pembatasan *user* untuk menginstall aplikasi sehingga perlu hak akses khusus
			4	Apakah ada kebijakan dan prosedur untuk mencegah perangkat lunak tidak diotorisasi yang ditemukan?	1	Tidak ada kebijakan atau prosedur formal untuk penanganan perangkat lunak tidak diotorisasi.	3	Membuat kebijakan atau prosedur terkait penanganan perangkat lunak yang tidak diotorisasi
		ID.AM-3: Organizational communication and data flows are mapped	1	Apakah organisasi memiliki dokumentasi topologi yang mencakup semua sistem dan jaringan?	3	Dokumentasi Topologi Jaringan dan lokasi VM sudah tersedia	3	Sudah Tercapai
			2	Apakah organisasi memiliki kebijakan dan prosedur untuk melindungi data dan privasi sesuai dengan peraturan yang berlaku?	2	Kebijakan dan prosedur ada dalam Kebijakan Data Masking dan DLP, tetapi tidak selalu diterapkan.	3	Mengoptimalkan dan memantau pelaksanaan Kebijakan Data Masking dan DLP
			3	Bagaimana organisasi memastikan bahwa kebijakan dan prosedur perlindungan data diperbarui untuk mencerminkan perubahan dalam peraturan?	3	Proses formal dan dokumentasi ada untuk memperbarui kebijakan dan prosedur secara berkala setiap sekali dalam setahun dalam bentuk review kebijakan dan prosedur	3	Sudah Tercapai

			4	Apakah organisasi memiliki proses dan alat yang memadai untuk memulihkan data dari cadangan?	2	Proses pemulihan data ada, tetapi tidak selalu diuji	3	Mengoptimalkan proses pemulihan dan pengujian data cadangan
			5	Apakah ada kebijakan yang mengatur frekuensi dan metode pelaporan pemulihan data dari cadangan?	2	Kebijakan ada dalam bentuk Dokumen Kebijakan Pengendalian Teknologi, tetapi tidak selalu diterapkan atau tidak efektif.	3	Mengoptimalkan proses pemulihan dan pengujian data cadangan
			1	Apakah organisasi memiliki katalog lengkap yang mencakup semua sistem informasi eksternal yang digunakan?	2	Katalog layanan ada dimuat di dalam Notion, namun tidak mencakup semua sistem informasi eksternal	3	Memperbarui katalog layanan hingga sistem informasi eksternal
			2	Bagaimana organisasi memastikan bahwa katalog sistem informasi eksternal diperbarui secara berkala?	2	Proses untuk memperbarui katalog ada, tetapi tidak selalu diputuhi.	3	Mengoptimalkan proses untuk memperbarui katalog layanan
			3	Apakah organisasi memiliki kebijakan dan prosedur untuk mengendalikan akses ke sistem informasi eksternal?	1	Belum ada kebijakan dan prosedur untuk mengendalikan akses ke sistem informasi eksternal	3	Membuat kebijakan atau prosedur untuk mengendalikan akses ke sistem informasi eksternal
		ID.AM-4: External information systems are catalogued	4	Bagaimana organisasi memastikan bahwa hanya pihak yang berwenang yang memiliki akses ke sistem informasi eksternal?	1	Belum ada kebijakan dan prosedur untuk mengendalikan akses ke sistem informasi eksternal	3	Membuat kebijakan atau prosedur untuk mengendalikan akses ke sistem informasi eksternal
			5	Bagaimana organisasi memastikan bahwa data yang disimpan, ditransmisikan, dan diproses oleh sistem informasi eksternal dilindungi?	1	Belum ada kebijakan dan prosedur untuk mengendalikan akses ke sistem informasi eksternal	3	Membuat kebijakan atau prosedur untuk mengendalikan akses ke sistem informasi eksternal
			6	Apakah organisasi menggunakan enkripsi untuk melindungi data saat disimpan dan ditransmisikan oleh sistem informasi eksternal?	1	Belum ada kebijakan dan prosedur untuk mengendalikan akses ke sistem informasi eksternal	3	Membuat kebijakan atau prosedur untuk mengendalikan akses ke sistem informasi eksternal
			7	Bagaimana organisasi mengelola risiko terkait penggunaan sistem informasi eksternal?	1	Belum ada kebijakan dan prosedur untuk mengendalikan akses ke sistem informasi eksternal	3	Membuat kebijakan atau prosedur untuk mengendalikan akses ke sistem informasi eksternal

		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	1	Apakah organisasi memiliki proses untuk mengklasifikasikan aset berdasarkan nilai bisnis, kritikalitas, dan klasifikasi keamanan?	3	Proses formal dan diterapkan secara konsisten untuk mengklasifikasikan aset, terhitung dalam dokumen Asset Register	3	Sudah Tercapai
			2	Bagaimana organisasi memastikan bahwa prioritas aset diperbarui sesuai dengan perubahan nilai bisnis atau kritikalitas?	3	Proses ada, ditetapkan tiap 1 tahun sekali atau jika ada penhbaruan Asset Register	3	Sudah Tercapai
			3	Apakah organisasi memiliki kebijakan dan prosedur untuk memastikan bahwa aset jarak jauh mematuhi kebijakan keamanan yang ditetapkan?	3	Untuk *end point* sudah diterapkan VPN untuk bisa melakukan *remote access*	3	Sudah Tercapai
			4	Bagaimana organisasi memantau dan mengelola aset jarak jauh untuk memastikan kepatuhan terhadap kebijakan keamanan?	3	Untuk *end point* sudah diterapkan Wazuh agar log bisa dipantau	3	Sudah Tercapai
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	1	Apakah organisasi telah menetapkan peran dan tanggung jawab keamanan siber untuk seluruh tenaga kerja dan pemangku kepentingan pihak ketiga?	3	Peran dan tanggung jawab ditetapkan dan didokumentasikan dengan baik dalam Matriks RASCI, dan SK Tim Sistem Manajemen Keamanan Informasi, mencakup seluruh tenaga kerja dan pihak ketiga.	3	Sudah Tercapai
			2	Bagaimana organisasi memastikan bahwa peran dan tanggung jawab ini dikomunikasikan dan dipahami oleh semua pihak yang terlibat?	3	Proses komunikasi dilakukan menggunakan email dan SISUMAKER, serta grup Whatsapp khusus	3	Sudah Tercapai
			3	Apakah organisasi memiliki program kesadaran keamanan yang memastikan bahwa semua personel sadar dan mengikuti kebijakan serta prosedur keamanan?	3	Program Security Awareness dilakukan secara berkala, selama 2 kali dalam setahun	3	Sudah Tercapai
			4	Apakah ada evaluasi rutin untuk mengukur efektivitas	1	Tidak ada evaluasi formal untuk program kesadaran keamanan.	3	Merencanakan program evaluasi terhadap pemahaman *Security Awareness* yang diberikan.

				program kesadaran keamanan?				
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	1	Apakah organisasi telah mengidentifikasi peran mereka dalam rantai pasokan?	2	Peran diidentifikasi, tetapi tidak selalu jelas atau terdokumentasi dengan baik	3	Membuat rincian peran fungsi dari tiap rantai pasok
			2	Bagaimana organisasi memastikan bahwa peran mereka dalam rantai pasokan dikomunikasikan dengan jelas kepada semua pemangku kepentingan internal dan eksternal?	2	Proses komunikasi ada, tetapi tidak selalu efektif atau lengkap	3	Membuat jalur komunikasi yang mudah dilakukan ke tiap rantai pasok
			3	Apakah organisasi memiliki kerangka kerja manajemen risiko yang mencakup identifikasi dan penilaian risiko yang terkait dengan peran mereka dalam rantai pasokan?	1	Tidak ada kerangka kerja formal untuk manajemen risiko terkait rantai pasokan.	3	Membuat kerangka kerja untuk melakukan manajemen risiko terkait rantai pasok
			4	Apakah ada mekanisme untuk memantau dan meninjau efektivitas rencana penanganan risiko yang terkait dengan rantai pasokan secara berkala?	1	Tidak ada mekanisme untuk memantau atau meninjau efektivitas rencana penanganan risiko yang terkait dengan rantai pasokan.	3	Melakukan penilaian risiko terhadap rantai pasok dan lakukan pemantauan
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	1	Apakah organisasi telah mengidentifikasi semua entitas dari pihak ketiga yang berkontribusi atau memiliki ketergantungan pada operasionalnya?	3	Sudah terdokumentasikan dalam dokumen Daftar Pihak Ketiga	3	Sudah Tercapai
			2	Apakah ada proses formal untuk memantau kinerja dan kepatuhan entitas dalam rantai pasokan terhadap standar dan kebijakan organisasi?	2	Sudah ada prosesnya dalam bentuk Review Pihak Ketiga, namun penerapannya belum optimal	3	Mengoptimalkan proses review terhadap pihak ketiga
			3	Apakah ada prosedur untuk secara berkala meninjau dan memperbarui informasi tentang ketergantungan dan	3	Sudah ada prosedur review dokumen Daftar Pihak Ketiga, sekali dalam setahun	3	Sudah Tercapai

				peran entitas dalam rantai pasokan?				
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	1	Apakah organisasi telah mendefinisikan struktur tata kelola keamanan siber secara jelas, termasuk peran dan tanggung jawab teams?	3	Organisasi telah mendefinisikannya dalam Dokumen Kebijakan Keamanan Informasi	3	Sudah Tercapai
			2	Bagaimana organisasi mengkomunikasikan peran dan tanggung jawab terkait keamanan siber kepada seluruh anggota timdan pihak terkait?	3	Organisasi secara berkala mengkomunikasikannya melalui Security Awareness yang dilakukan 2 kali dalam setahun	3	Sudah Tercapai
			3	Apakah ada proses untuk secara berkala menilai dan mengevaluasi efektivitas struktur tata kelola keamanan siber dan peran terkait?	3	Penilaian dan evaluasi ada berupa review yang dilakukan 1 tahun sekali dalam Rapat Tinjauan Manajemen	3	Sudah Tercapai
			4	Apakah organisasi memiliki mekanisme untuk memperbarui dan memperbaiki struktur tata kelola keamanan siber berdasarkan umpan balik atau perubahan dalam ancaman dan lingkungan bisnis?	3	Mekanisme pembaruan ada berupa review yang dilakukan 1 tahun sekali dalam Rapat Tinjauan Manajemen	3	Sudah Tercapai
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	1	Apakah organisasi telah mengidentifikasi ketergantungan dan fungsi kritis yang diperlukan untuk penyampaian layanan kritis?	3	Sudah dilakukan dan didokumentasikan dengan Daftar Layanan Kritis	3	Sudah Tercapai
			2	Apakah organisasi memiliki proses untuk mengelola hubungan dengan pemasok yang mendukung penyampaian layanan kritis?	3	Sudah dilakukan via grup chat dengan pemasok	3	Sudah Tercapai
			3	Apakah organisasi memiliki prosedur kesinambungan bisnis untuk memastikan pemulihan fungsi kritis	2	Organisasi telah memiliki dokumen BCP, namun belum dilakukan pengujian terhadap skenario BCP secara berkala	3	Melakukan pengujian terhadap skenario yang telah ditetapkan di dalam dokumen BCP

				dalam hal gangguan atau bencana?				
			4	Apakah persyaratan keamanan informasi dimasukkan dalam kontrak dengan pemasok?	3	Dimasukkan dalam kontrak dan ada kewajiban pemasok untuk menandatangani NDA	3	Sudah Tercapai
			5	Apakah sistem informasi organisasi dirancang dan dikelola untuk memenuhi persyaratan ketersediaan dan kapasitas untuk fungsi dan layanan kritis?	2	Sudah ada redundansi di pengelolaan bandwidth, namun belum dilakukan redundansi dalam pengelolaan listrik dan colocation server	3	Melakukan pengadaan genset dan colocation server
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	1	Apakah organisasi memiliki prosedur formal untuk memastikan ketahanan layanan kritis selama keadaan darurat atau serangan?	2	Organisasi telah memiliki dokumen BCP, namun belum dilakukan pengujian terhadap skenario BCP secara berkala	3	Melakukan pengujian terhadap skenario yang telah ditetapkan di dalam dokumen BCP
			2	Apakah ada mekanisme untuk menilai dan memperbarui persyaratan ketahanan berdasarkan umpan balik, perubahan dalam ancaman, atau perubahan dalam lingkungan operasi?	3	Mekanisme pembaruan ada berupa review yang dilakukan 1 tahun sekali dalam Rapat Tinjauan Manajemen	3	Sudah Tercapai
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	1	Apakah organisasi telah menetapkan kebijakan keamanan siber yang formal dan terdokumentasi?	3	Organisasi telah menetapkan Kebijakan Keamanan Informasi	3	Sudah Tercapai
			2	Bagaimana organisasi mengkomunikasikan kebijakan keamanan siber kepada seluruh anggota organisasi dan pihak terkait?	3	Organisasi telah secara berkala mengkomunikasikan Kebijakan Keamanan Informasi 2 kali dalam setahun, atau jika ada perubahan	3	Sudah Tercapai
			3	Apakah organisasi memiliki proses untuk memantau kepatuhan terhadap kebijakan keamanan siber?	3	Ada dalam Sasaran Keamanan Informasi yang tertuang dalam dokumen Kebijakan Keamanan Informasi	3	Sudah Tercapai

	management of cybersecurity risk.		4	Apakah ada proses untuk meninjau dan memperbarui kebijakan keamanan siber secara berkala?	3	Mekanisme pembaruan ada berupa review yang dilakukan 1 tahun sekali dalam Rapat Tinjauan Manajemen	3	Sudah Tercapai
			5	Apakah organisasi menyediakan pelatihan dan kesadaran terkait kebijakan keamanan siber kepada karyawan dan pemangku kepentingan lainnya?	3	Organisasi telah secara berkala mengkomunikasikan Kebijakan Keamanan Informasi 2 Lib dalam setahun, atau jika ada perubahan	3	Sudah Tercapai
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	1	Apakah organisasi telah mendefinisikan peran dan tanggung jawab keamanan siber secara jelas untuk anggota internal dan mitra eksternal?	3	Peran dan tanggung jawab sudah didefinisikan untuk anggota internal, untuk mitra eksternal sudah didefinisikan dalam Daftar Kontak Khusus	3	Sudah Tercapai
			2	Apakah organisasi memiliki proses untuk memantau pemenuhan peran dan tanggung jawab keamanan siber oleh anggota internal dan mitra eksternal?	3	Mekanisme pemantauan ada berupa review yang dilakukan 1 tahun sekali dalam Rapat Tinjauan Manajemen	3	Sudah Tercapai
			3	Apakah ada proses untuk meninjau dan memperbarui peran dan tanggung jawab keamanan siber secara berkala?	3	Mekanisme pemantauan ada berupa review dokumen yang dilakukan 1 tahun	3	Sudah Tercapai
			4	Apakah peran dan tanggung jawab terkait penanganan insiden keamanan siber didefinisikan dan dikomunikasikan dengan jelas kepada semua pemangku kepentingan internal dan eksternal?	3	Peran dan tanggung jawab terkait penanganan insiden sudah didefinisikan sesuai dengan Tugas dan Fungsi dari masing masing stakeholders	3	Sudah Tercapai
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy	1	Bagaimana organisasi memastikan bahwa kewajiban hukum dan regulasi terkait keamanan siber dipahami secara menyeluruh?	3	Kewajiban hukum dan regulasi sudah didaftarkan di dalam Dokumen Master List, dan dijelaskan dalam program *Security Awareness*	3	Sudah Tercapai

		and civil liberties obligations, are understood and managed	2	Apakah organisasi memiliki proses untuk memantau dan menjaga kepatuhan terhadap kewajiban hukum dan regulasi secara berkala?	3	Dilakukan uji kerentanan secara berkala untuk bisa mengetahui apa ada kebocoran data pada sistem	3	Sudah Tercapai
		ID.GV-4: Governance and risk management processes address cybersecurity risks	1	Bagaimana organisasi mengintegrasikan risiko keamanan siber ke dalam proses tata kelola dan manajemen risiko yang ada?	3	Sudah ada prosedur Manajemen Risiko Keamanan Informasi yang mendefinisikan risiko keamanan siber dalam Daftar Ancaman (Threat) dan Kerentanan (Vulnerability)	3	Sudah Tercapai
			2	Bagaimana organisasi melakukan penilaian risiko untuk mengidentifikasi risiko keamanan siber yang relevan?	3	Sudah ada prosedur Manajemen Risiko Keamanan Informasi untuk mengidentifikasi risiko keamanan siber, dan ditetapkan dalam dokumen Risk Register	3	Sudah Tercapai
			3	Apa langkah-langkah yang diambil oleh organisasi untuk mengelola dan mengurangi risiko keamanan siber yang telah diidentifikasi?	3	Sudah dilakukan identifikasi mitigasi dalam dokumen Risk Register	3	Sudah Tercapai
			4	Siapa yang bertanggung jawab dalam organisasi untuk pengelolaan risiko keamanan siber dan bagaimana tanggung jawab tersebut didefinisikan?	3	Pengelolaan risiko sudah diidentifikasi dalam dokumen Risk Register, yaitu pemilik aset/layanan	3	Sudah Tercapai
			5	Apakah ada mekanisme pemantauan yang diterapkan untuk menilai efektivitas proses manajemen risiko keamanan siber?	3	Mekanisme pemantauan dilakukan tiap sekali dalam setahun untuk memantau efektivitas mitigasi yang telah ditetapkan dalam Risk Register	3	Sudah Tercapai
			6	Bagaimana informasi mengenai risiko keamanan siber dilaporkan dan dikomunikasikan kepada pemangku kepentingan internal dan eksternal?	3	Risk Register ditetapkan oleh Pengelola Pusat Data, dan dikomunikasikan melalui Security Awareness	3	Sudah Tercapai
	Risk Assessment (ID.RA): The organization understands the	**ID.RA-1:** Asset vulnerabilities are identified and documented	1	Bagaimana organisasi mengidentifikasi dan mendokumentasikan kerentanan pada aset/sistem?	3	Dilakukan secara berkala dalam merumuskan risiko, dan dilakukan uji kerentanan secara berkala pada aset aplikasi	3	Sudah Tercapai

	cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.		2	Apakah organisasi melakukan pemindaian kerentanan secara rutin? Seberapa sering dan bagaimana hasilnya dikelola?	3	Dilakukan secara berkala sekali dalam sebulan, dan didokumentasikan pada dokumen hasil Penetration Test	3	Sudah Tercapai
			3	Bagaimana organisasi menilai dan memprioritaskan kerentanan untuk menentukan langkah remediasi?	3	Langkah remediasi dilakukan melihat terhadap nilai kritikasi dari kerentanan menggunakan CVSS	3	Sudah Tercapai
			4	Apa proses yang digunakan organisasi untuk merespons dan memperbaiki kerentanan yang telah diidentifikasi?	3	Proses menggunakan best practice sesuai dengan kerentanan yang ditemukan	3	Sudah Tercapai
			5	Bagaimana organisasi mendokumentasikan kerentanan yang teridentifikasi dan tindak lanjut yang dilakukan?	3	Kerentanan didokumentasikan dalam laporan Penetration Testing berikut dengan langkah remediasinya	3	Sudah Tercapai
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	1	apakah telah dilaksanakan monitoring terhadap jaringan, sistem dan aplikasi untuk melihat anomali untuk mengambil tindakan yang tepat?	3	sudah dilaksikan secara berkala	3	Sudah Tercapai
			2	apakah organisasi telah memiliki cyber threat intelligence?	3	sudah ada di wazuh	3	Sudah Tercapai
		ID.RA-3: Threats, both internal and external, are identified and documented	1	Bagaimana organisasi mengidentifikasi ancaman internal dan eksternal?	3	ancaman sudah diidentifikasi dalam dokumen Risk Register, dengan dipedomani oleh prosedur Manajemen Risiko Keamanan Informasi	3	Sudah Tercapai
			2	Bagaimana organisasi mendokumentasikan ancaman yang telah diidentifikasi?	3	Ancaman didokumentasikan dalam Risk Register	3	Sudah Tercapai
			3	Bagaimana organisasi menilai risiko yang terkait dengan ancaman yang diidentifikasi?	3	Penilaian risiko dilakukan dengan dipedomani oleh prosedur Manajemen Risiko Keamanan Informasi	3	Sudah Tercapai

			4	Apa langkah-langkah yang diambil organisasi untuk mengelola dan merespons ancaman yang telah diidentifikasi?	3	Untuk pengelolaan ancaman dilakukan sesuai dengan mitigasi yang telah ditetapkan dalam Risk Register. Untuk ancaman yang berada di SIEM, direspons dengan Active Response pada SIEM	3	Sudah Tercapai
			5	Apakah organisasi memiliki mekanisme untuk memantau dan memperbarui informasi mengenai ancaman?	3	Ancaman siber dapat dipantau melalui SIEM, dan informasi dapat diperbarui melalui Threat Intelligence di dalam SIEM	3	Sudah Tercapai
			6	Bagaimana informasi mengenai ancaman dikomunikasikan kepada pemangku kepentingan?	3	Analisa terhadap ancaman didokumentasikan dalam pelaporan yang dilakukan tiap 3 bulan sekali ke Top Management. Ancaman yang terdapat di Risk Register akan direviu dan ditetapkan oleh Top Management	3	Sudah Tercapai
		ID.RA-4: Potential business impacts and likelihoods are identified	1	Bagaimana organisasi mengidentifikasi potensi dampak bisnis yang dapat terjadi akibat kerentanan atau ancaman?	2	Organisasi telah mengidentifikasi dampak ke dalam dokumen Risk Register dan dokumen Business Impact Analysis (BIA), namun untuk dokumen Business Impact Analysis masih perlu dilakukan revisi.	3	Melakukan review terhadap dokumen BIA
			2	Apakah ada mekanisme untuk meninjau dan memperbarui penilaian dampak bisnis dan kemungkinan terjadinya?	2	Organisasi telah menetapkan waktu untuk revisi dokumen BIA, namun belum dilaksanakan	3	Melakukan review terhadap dokumen BIA
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	1	Bagaimana organisasi menggunakan informasi mengenai ancaman, kerentanan, kemungkinan terjadinya, dan dampak untuk menentukan tingkat risiko?	3	Organisasi telah menetapkan prosedur Manajemen Risiko Keamanan Informasi yang terdiri dari ancaman, kerentanan, kemungkinan terjadinya dan dampak untuk menentukan tingkat risiko	3	Sudah Tercapai
			2	Bagaimana organisasi memprioritaskan risiko berdasarkan hasil penilaian?	3	Prioritas ditetapkan atas dasar penilaian tingkat risiko dalam dokumen Risk Register yang dipedomani oleh prosedur Manajemen Risiko Keamanan Informasi	3	Sudah Tercapai
			3	Bagaimana organisasi menerapkan kontrol berdasarkan penilaian risiko?	3	Kontrol diterapkan secara bersama-sama oleh Tim Sistem Manajemen Keamanan Informasi yang ditetapkan oleh Top Management	3	Sudah Tercapai
			4	Bagaimana organisasi mendokumentasikan hasil dari penilaian risiko dan tindakan yang diambil?	3	Hasil penilaian risiko dan tindakan yang diambil didokumentasikan dalam dokumen Risk Register	3	Sudah Tercapai

			5	Apakah ada mekanisme untuk meninjau dan memperbarui penilaian risiko?	3	Dokumen Risk Register direviu tiap sekali dalam setahun sesuai dengan Sasaran SMKI yang ditetapkan dalam dokumen Kebijakan Sistem Manajemen Keamanan Informasi	3	Sudah Tercapai
		ID.RA-6: Risk responses are identified and prioritized	1	Bagaimana organisasi mengidentifikasi berbagai respons terhadap risiko yang dinilai?	3	Sudah dilakukan dengan kriteria risiko yang ada dalam prosedur Manajemen Risiko Keamanan Informasi	3	Sudah Tercapai
			2	Bagaimana organisasi memprioritaskan respons risiko?	3	Respons risiko diprioritaskan sesuai dengan penilaian risiko, sesuai dengan Manajemen Risiko Keamanan Informasi	3	Sudah Tercapai
			3	Bagaimana keputusan diambil terkait respons risiko?	3	Keputusan diambil sesuai dengan Risk Appetite yang telah ditentukan dalam prosedur Manajemen Risiko Keamanan Informasi	3	Sudah Tercapai
			4	Bagaimana respons risiko diimplementasikan dan dipantau?	3	Respons risiko diimplementasikan sesuai dengan Risk Appetite, dan dipantau sesuai dengan tenggat waktu yang ditetapkan di tiap-tiap risiko	3	Sudah Tercapai
			5	Apakah ada mekanisme untuk meninjau dan memperbarui respons risiko?	3	Dokumen Risk Register direviu tiap sekali dalam setahun sesuai dengan Sasaran SMKI yang ditetapkan dalam dokumen Kebijakan Sistem Manajemen Keamanan Informasi	3	Sudah Tercapai
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	1	Bagaimana organisasi membentuk dan mendokumentasikan proses manajemen risiko?	3	Proses manajemen risiko ditetapkan dengan Risk Register, yang ditetapkan sesuai dengan prosedur Manajemen Risiko Keamanan Informasi	3	Sudah Tercapai
			2	Bagaimana proses manajemen risiko dikelola untuk memastikan efektivitasnya?	3	Setiap proses manajemen risiko dijamarkan dalam prosedur Manajemen Risiko Keamanan Informasi. Prosedur tersebut direviu setiap sekali dalam setahun	3	Sudah Tercapai
			3	Bagaimana organisasi melibatkan pemangku kepentingan dalam proses manajemen risiko?	3	Proses manajemen risiko yang didokumentasikan lewat Risk Register melibatkan seluruh pemilik aset/layanan, dan ditetapkan oleh Top Management	3	Sudah Tercapai
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	1	Bagaimana organisasi menentukan tingkat toleransi risiko?	3	Tingkat toleransi risiko ditetapkan dalam prosedur Manajemen Risiko Keamanan Informasi oleh Top Management	3	Sudah Tercapai
			2	Bagaimana organisasi mengkomunikasikan toleransi risiko?	3	Toleransi risiko dikomunikasikan melalui kegiatan Security Awareness	3	Sudah Tercapai

			3	Bagaimana pemangku kepentingan dilibatkan dalam penetapan dan ekspresi toleransi risiko?	3	Toleransi risiko ditetapkan dalam prosedur Manajemen Risiko Keamanan Informasi yang disusunkan oleh *stakeholders* dan ditetapkan oleh Top Management	3	Sudah Tercapai
			4	Bagaimana organisasi memastikan pemahaman dan kepatuhan terhadap toleransi risiko?	3	Dilakukan komunikasi terhadap semua *stakeholders* mengenai toleransi risiko yang telah ditetapkan dalam prosedur Manajemen Risiko Keamanan Informasi melalui kegiatan *Security Awareness*	3	Sudah Tercapai
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	1	Bagaimana organisasi melakukan analisis risiko terkait infrastruktur kritis?	3	Organisasi telah mengidentifikasi dampak kekritisan infrastruktur menggunakan tools yang telah diberikan oleh BSSN	3	Sudah Tercapai
			2	Bagaimana pemangku kepentingan dilibatkan dalam analisis risiko?	3	Proses manajemen risiko yang didokumentasikan lewat Risk Register melibatkan seluruh pemilik aset/layanan, dan ditetapkan oleh Top Management	3	Sudah Tercapai
			3	Bagaimana hasil analisis risiko didokumentasikan dan dikomunikasikan?	3	Hasil analisis risiko tertuangkan dalam dokumen Risk Register, dan dikomunikasikan melalui kegiatan *Security Awareness*	3	Sudah Tercapai
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	1	Bagaimana organisasi mengidentifikasi dan menetapkan proses manajemen risiko untuk rantai pasokan?	2	Organisasi telah memiliki kebijakan mengenai proses manajemen risiko untuk rantai pasok, namun belum diterapkan secara optimal	3	Membuat kerangka kerja untuk melakukan manajemen risiko terkait rantai pasok
			2	Bagaimana penilaian risiko dilakukan terkait hubungan pihak ketiga?	1	Penilaian risiko terkait hubungan dengan pihak ketiga belum dilakukan	3	Melakukan penilaian risiko terhadap rantai pasok dan lakukan pemantauan
			3	Bagaimana risiko terkait rantai pasokan dipantau dan ditinjau?	1	Pemantauan dan peninjauan risiko terkait rantai pasok belum dilakukan	3	Melakukan penilaian risiko terhadap rantai pasok dan lakukan pemantauan
			4	Bagaimana pemangku kepentingan dilibatkan dalam proses manajemen risiko rantai pasokan?	1	Belum dilakukan	3	Melakukan penilaian risiko terhadap rantai pasok dan lakukan pemantauan
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are	1	Bagaimana organisasi mengidentifikasi dan memprioritaskan pemasok dan mitra pihak ketiga?	3	Organisasi telah mengidentifikasi pemasok dalam dokumen Daftar Pihak Ketiga	3	Sudah Tercapai
			2	Bagaimana penilaian risiko dilakukan untuk pemasok dan mitra pihak ketiga?	1	Belum dilakukan penilaian risiko untuk pemasok dan pihak ketiga	3	Melakukan penilaian risiko terhadap rantai pasok dan pihak ketiga dan lakukan pemantauan

		identified, prioritized, and assessed using a cyber supply chain risk assessment process	3	Bagaimana risiko terkait pihak ketiga dipantau dan ditinjau?	1	Belum dilakukan pemantauan dan peninjauan terkait risiko pihak ketiga	3	Melakukan penilaian risiko terhadap rantai pasok dan pihak ketiga,dan lakukan pemantauan
			4	Bagaimana organisasi memastikan persyaratan keamanan dalam kontrak dengan pihak ketiga?	3	Persyaratan keamanan dalam kontrak sudah dituangkan dalam dokumen kontrak dan NDA	3	Sudah Tercapai
			5	Bagaimana informasi tentang pihak Ketiga diintegrasikan ke dalam inventaris aset?	1	Belum ada kolom pihak ketiga dalam Asset Register	3	Menambahkan isian pihak ketiga dalam Asset Register untuk tiap-tiap aset
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	1	Bagaimana organisasi memastikan kontrak mencakup persyaratan untuk mengelola risiko keamanan siber?	3	Persyaratan keamanan dalam kontrak sudah dituangkan dalam dokumen kontrak dan NDA	3	Sudah Tercapai
			2	Bagaimana risiko terkait hubungan kontraktual dievaluasi?	2	Prosedur sudah ada, namun belum dilakukan evaluasi mengenai risiko terkait hubungan kontraktual	3	Lakukan evaluasi risiko terhadap pihak ketiga sesuai dengan prosedur
			3	Bagaimana kepatuhan terhadap persyaratan kontrak dipantau?	3	Dilakukan pemantauan kepatuhan terhadap pihak ketiga oleh PPK dan PPTK	3	Sudah Tercapai
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	1	Bagaimana penilaian rutin dilakukan untuk memastikan pemenuhan kewajiban kontrak?	3	Pemenuhan kewajiban kontrak dievaluasi dan dituangkan dalam Berita Acara Pemeriksaan Hasil Pekerjaan (BAPHP)	3	Sudah Tercapai
			2	Bagaimana risiko terkait pihak ketiga dipantau dan ditinjau secara rutin?	1	Belum dilakukan evaluasi mengenai risiko terkait hubungan kontraktual	3	Lakukan evaluasi risiko terhadap pihak ketiga sesuai dengan prosedur
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	1	Bagaimana perencanaan respons dan pemulihan dilakukan dengan pemasok dan mitra?	3	Perencanaan respons dan pemulihan yang terkait dengan pihak ketiga telah ditetapkan dalam kontrak dan SLA	3	Sudah Tercapai
			2	Bagaimana rencana diuji bersama pemasok dan mitra?	1	Belum ada rencana respons diuji bersama dengan pemasok	3	Lakukan perencanaan uji coba skenario pemulihan dan respons dengan pemasok pada BCP

			3	Bagaimana koordinasi dilakukan selama pengujian?	1	Belum ada rencana respons diuji bersama dengan pemasok	3	Lakukan perencanaan uji coba skenario pemulihan dan respons dengan pemasok pada BCP
			4	Bagaimana hasil pengujian dievaluasi?	1	Belum dilakukan pengujian	3	Lakukan perencanaan uji coba skenario pemulihan dan respons dengan pemasok pada BCP
			5	Bagaimana dokumentasi hasil pengujian dilakukan?	1	Belum dilakukan pengujian	3	Lakukan perencanaan uji coba skenario pemulihan dan respons dengan pemasok pada BCP
				Nilai Total	**301**	**2.508333333**	**360**	

Function	Category	Subcategory	No	Pertanyaan	Level Implementasi	Keterangan	Level Kondisi yang diinginkan	Rekomendasi
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	1	apakah organisasi telah mengelola dan mengevaluasi user account penggguna di sistem?	2	belum dilakukan secara berkala	3	Mengoptimalkan dan memantau pengelolaan dan evaluasi user account penggguna di sistem
			2	apakah organisasi telah menonaktifkan user account default pada perangkat/sistem?	3	sudah dilakukan berkala	3	Sudah Tercapai
			3	apakah sudah ada penetapan hak akses yang berbeda di tiap user account?	3	sudah dilaksanakan berkala	3	Sudah Tercapai
		PR.AC-2: Physical access to assets is managed and protected	1	apakah ada penetapan lokasi restricted untuk memproteksi area terbatas yang berisi informasi dan aset?	3	ada lokasi data center dengan perimeter keamanan	3	Sudah Tercapai
			2	apakah sudah tersedia kontrol pengamanan terhadap area aman?	3	sudah ada kontrol pengamanan	3	Sudah Tercapai
			3	apakah ada desain dan implementasi terkait area aman?	3	ada desain dan implementasi area aman	3	Sudah Tercapai
			4	apakah ada monitoring terhadap area aman?	3	ada akses doorlock dan cctv	3	Sudah Tercapai
			5	apakah ada proteksi terhadap kabel listrik maupun data?	3	sudah ada proteksi terhadap kabel	3	Sudah Tercapai
		PR.AC-3: Remote access is managed	1	apakah ada kebijakan dan prosedur terkait remote akses?	3	sudah ada kebijakan terkait remote akses	3	Sudah Tercapai

			2	apakah ada evaluasi terhadap user account remote akses?	3	sudah ada evaluasi secara berkala	3	Sudah Tercapai
		PRAC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	1	Apakah organisasi telah menetapkan daftar kontrol akses fisik dan data?	3	sudah ada	3	Sudah Tercapai
			2	apakah ada pembatasan hak akses yang berbeda antara administrator dan pengguna biasa?	3	sudah ada dibagi role	3	Sudah Tercapai
			3	apakah dilakukan peninjauan terhadap hak akses secara berkala?			3	
			4	apakah organisasi telah menetapkan prosedur atau mekanisme pelaporan aktivitas yang mencurigakan?	3	sudah ada prosedur dan mekanisme pelaporan	3	Sudah Tercapai
			5	apakah ada pembatasan terhadap penggunaan program utilitas yang mampu memodifikasi sistem dan kontrol aplikasi?	3	ada sesuai dengan role	3	Sudah Tercapai
		PRAC-5: Network integrity is protected (e.g., network segregation, network segmentation)	1	apakah organisasi menggunakan DNS filtering terhadap domain yang berbahaya?	3	dilakukan, menggunakan dns nawala	3	Sudah Tercapai
			2	apakah organisasi melakukan filtering terhadap ekstensi tertentu di mail server?	3	ada telah dikonfigurasi	3	Sudah Tercapai
			3	apakah organisasi menerapkan segementasi jaringan	3	ada telah dikonfigurasi	3	Sudah Tercapai
			4	Apakah organisasi memiliki kebijakan atau prosedur terkait alih data dan informasi? Termasuk dokumentasi penerapannya?	2	sudah ada kebijakan dan prosedur namun belum ada dokumentasi penerapan	3	Mengoptimalkan dan memantau pelaksanaan prosedur alih data dan informasi
			5	apakah ada konfigurasi kontrol firewall dalam jaringan?	3	sudah ada konfigurasi	3	Sudah Tercapai
		PRAC-6: Identities are proofed and	1	apakah ada pembatasan hak akses administrator?	3	ada, sesuai role	3	Sudah Tercapai

		bound to credentials and asserted in interactions	2	apakah ada pembatasan terhadap akses fisik, data dan informasi?	3	ada, sesuai dengan role	3	Sudah Tercapai
			3	apakah ada kebijakan atau prosedur mengenai kontrol akses terhadap fisik dan logikal?	3	ada	3	Sudah Tercapai
			4	apakah user account sudah mengacu ke personil tertentu?	3	sudah, 1 account 1 personil	3	Sudah Tercapai
			5	apakah ada pencatatan log terhadap aktivitas user account?	3	sudah ada logging terhadap user	3	Sudah Tercapai
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	1	apakah organisasi telah menerapkan MFA?	3	sudah dilakukan berupa VPN dan SSH	3	Sudah Tercapai
			2	apakah ada pembatasan akses SSH?	3	ada, hanya divisi tertentu yg bisa mengakses ssh	3	Sudah Tercapai
			3	apakah jaringan telah menggunakan protokol yang aman (misal 802.1x, WPA2, dll)?	3	sudah	3	Sudah Tercapai
			4	apakah organisasi menerapkan kewajiban VPN akses terhadap akses server?	3	sudah dilakukan	3	Sudah Tercapai
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	1	apakah organisasi melakukan security awareness terhadap semua pegawai secara berkala?	3	sudah dilakukan secara berkala	3	Sudah Tercapai
			2	apakah organisasi melakukan peningkatan kapasitas terhadap semua pegawai terkait topik keamanan informasi/siber?	2	sudah, namun tidak berkala	3	Lakukan penjadwalan terhadap pelatihan terhadap pegawai
			3	apakah organisasi telah menetapkan peran dan tanggung jawab masing masing personil dan menginformasikannya?	3	sudah dilakukan	3	Sudah Tercapai
		PR.AT-2: Privileged users understand	1	apakah organisasi melakukan security	3	sudah dilakukan secara berkala	3	Sudah Tercapai

		their roles and responsibilities		awareness terhadap administrator?				
			2	Apakah ada dokumentasi yang menggambarkan peran dan tanggung jawab pengguna dengan hak istimewa terkait keamanan informasi?	3	ada di dalam dokumen matriks hak akses	3	Sudah Tercapai
			3	Apakah ada program pelatihan untuk meningkatkan kapabilitas untuk administrator?	2	ada namun tidak terjadwal secara berkala	3	Lakukan penjadwalan terhadap pelatihan terhadap pegawai
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	1	apakah organisasi melakukan security awareness terhadap pihak ketiga?	1	tidak didokumentasikan	3	Lakukan *security awareness* secara formal ke pihak ketiga
			2	apakah organisasi telah mengisyaratkan ayarat keamanan informasi saat melakukan perjanjian kerjasama dengan pihak ketiga?	3	sudah dilakukan	3	Sudah Tercapai
		PR.AT-4: Senior executives understand their roles and responsibilities	1	apakah organisasi melakukan security awareness terhadap pimpinan?	3	sudah dilakukan berkala	3	Sudah Tercapai
			2	Apakah ada dokumentasi yang menggambarkan peran dan tanggung jawab pimpinan terkait keamanan informasi?	3	ada dalam Matriks RASCI dan SK Tim SMKI	3	Sudah Tercapai
			3	Apakah ada program pelatihan untuk meningkatkan kapabilitas untuk pimpinan?	1	Belum ada program pelatihan untuk meningkatkan kapabilitas pimpinan	3	Lakukan penjadwalan terhadap pelatihan terhadap pimpinan
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	1	apakah organisasi melakukan security awareness terhadap tim keamanan siber?	3	sudah dilaksanakan security awareness secara berkala	3	Sudah Tercapai
			2	Apakah ada dokumentasi yang menggambarkan peran dan tanggung jawab personil yang menangani keamanan	3	Sudah ada dalam dokumen Matriks RASCI dan SK Tim SMKI	3	Sudah Tercapai

				siber terkait keamanan informasi?				
			3	Apakah ada program pelatihan untuk meningkatkan kapabilitas untuk tim keamanan siber?	3	Sudah ada program pelatihan dari BSSN	3	Sudah Tercapai
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	1	apakah organisasi telah menerapkan enkripsi pada data/informasi sensitif yang disimpan (enkripsi password, enkripsi DB, enkripsi data)?	3	sudah dilakukan enkripsi	3	Sudah Tercapai
			2	Apakah ada prosedur yang diterapkan untuk melindungi data-at-rest dari ancaman fisik dan lingkungan?	2	Data-at-rest disimpan dalam media yang terenkripsi, namun belum ada prosedur khusus untuk data-at-rest	3	Pembuatan prosedur penyimpanan data-at-rest
			3	Apakah ada kebijakan untuk memastikan keamanan data selama transmisi dan penyimpanan?	3	Sudah ada di dalam Dokumen Kebijakan Pengendalian Organisasi	3	Sudah Tercapai
			4	Apakah ada mekanisme untuk memantau dan menegakkan kebijakan keamanan data saat disimpan?	3	Sudah ada mekanismenya dengan menggunakan File Integrity Monitoring di Wazuh	3	Sudah Tercapai
		PR.DS-2: Data-in-transit is protected	1	apakah organisasi telah menerapkan enkripsi pada data/informasi sensitif yang transit (TLS, SSL)?	3	sudah dilakukan berupa SSL	3	Sudah Tercapai
			2	Apakah ada perjanjian kerahasiaan atau non-disclosure agreement (NDA) yang diterapkan untuk melindungi data yang ditransmisikan?	3	Sudah ada NDA terkait transmisi data	3	Sudah Tercapai
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	1	Apakah organisasi telah menetapkan kebijakan atau prosedur manajemen aset mencakup akuisisi, penghapusan, pemindahan?	3	sudah ada kebijakan dan penerapannya	3	Sudah Tercapai
			2	apakah organisasi telah menetapkan asset register?	3	sudah ada asset register dan direview berkala	3	Sudah Tercapai

		PR.DS-4: Adequate capacity to ensure availability is maintained	1	Apakah ada prosedur untuk mengelola kapasitas dan memastikan ketersediaan layanan?	3	sudah dilakukan pengelolaan kapasitas tiap 3 bulan sekali	3	Sudah Tercapai
		PR.DS-5: Protections against data leaks are implemented	1	apakah organisasi menggunakan sistem Data Leakage Prevention/Intelegent?	1	Organisasi belum menerapkan DLP	3	
			2	apakah organisasi melakukan penetration testing/vulnerability assessment secara berkala?	3	sudah dilakukan berkala	3	Sudah Tercapai
			3	apakah organisasi menerapkan NDA kepada stakeholders (pengelola, pimpinan, pihak ketiga)?	3	sudah diterapkan	3	Sudah Tercapai
			4	apakah organisasi memiliki fasilitas redundansi untuk memenuhi persyaratan availabilitas?	2	belum semua fasilitasi memiliki redundansi	3	Lakukan pengadaan redundansi, seperti genset dan colocation server
			5	apakah organisasi telah menggunakan NTP dalam sinkronisasi waktu?	3	sudah dilakukan penerapan NTP pada perangkat	3	Sudah Tercapai
			6	Apakah sudah ada kebijakan klasifikasi aset dan implementasinya?	3	Sudah ada kebijakan klasifikasi aset dan sudah diimplementasikan dan dicatat dalam dokumen Asset Register	3	Sudah Tercapai
			7	Apakah informasi dilindungi melalui web dengan menggunakan konfigurasi umum dan penfilteran konten yang sesuai?	3	Sudah dilakukan konfigurasi yang umum menyesuaikan dengan dokumen Standar Konfigurasi	3	Sudah Tercapai
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	1	apakah ada mekanisme integrity monitoring terhadap software, firmware dan informasi?	3	ada mekanisme di wazuh	3	Sudah Tercapai
		PR.DS-7: The development and testing environment(s) are separate from the	1	apakah ada mekanisme pemisahan lingkungan development dan lingkungan production?	2	sudah ada namun belum konsisten dilakukan	3	Lakukan pemantauan terhadap pelaksanaan pemisahan environment development dan production

		production environment						
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	1	Apakah ada kebijakan dan prosedur yang mendukung pemeriksaan integritas perangkat keras?	3	mekanisme FI dilakukan saat pembelian hardware dengan perekrekan serial number di perangkat dan di box	3	Sudah Tercapai
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	1	apakah organisasi telah menciptakan standar konfigurasi bagi hardware, software, jaringan?	3	ada standar konfigurasi	3	Sudah Tercapai
			2	apakah organisasi menerapkan penjustisian sesi otomatis terhadap sistem?	3	sudah dilakukan penguncian sesi, selama waktu tertentu	3	Sudah Tercapai
			3	apakah organisasi telah menerapkan whitelist sistem apa saja yang boleh diinstall?	2	sudah dilakukan pencatatan whitelist, namun belum diterapkan secara konsisten	3	Menerapkan pembatasan user untuk menginstall aplikasi sehingga perlu hak akses khusus
			4	apakah organisasi telah menerapkan versioning manajemen perubahan?	2	sudah dilakukan namun belum konsisten	3	Lakukan pemantauan terhadap pelaksanaan versioning
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	1	Apakah organisasi memiliki dan menerapkan SDLC untuk mengelola sistem?	3	Sudah memiliki kebijakan SDLC dan diterapkan secara konsisten	3	Sudah Tercapai
			2	Apakah kebijakan pengembangan aman diterapkan dalam SDLC?	3	sudah ada bab yan mengatur tentang standar keamanan dalam dokumen kebijakan Secure SDLC	3	Sudah Tercapai
			3	Apakah peran dan tanggung jawab untuk setiap tahap SDLC telah ditentukan dan didokumentasikan?	3	Sudah ada SK Tim dalam tiap-tiap proses pengembangan	3	Sudah Tercapai
			4	Bagaimana organisasi melakukan pengujian keamanan selama tahap pengembangan dan implementasi?	3	Dilakukan berupa penetration testing yang didokumentasikan sebelum proses rilis	3	Sudah Tercapai

		PR.IP-3: Configuration change control processes are in place	1	Apakah organisasi memiliki dan menerapkan proses kontrol perubahan konfigurasi?	3	Kontrol perubahan konfigurasi diterapkan dengan proses manajemen perubahan yang dilokumentasikan di dalam Notion	3	Sudah Tercapai
			2	Bagaimana organisasi memastikan bahwa setiap perubahan konfigurasi diuji kemanannya sebelum diterapkan?	3	ada proses uji coba perubahan konfigurasi dengan memantau log aktivitas setelah perubahan konfigurasi dilakukan	3	Sudah Tercapai
		PR.IP-4: Backups of information are conducted, maintained, and tested	1	apakah organisasi telah melakukan backup berkala?	3	sudah dilakukan backup berkala	3	Sudah Tercapai
			2	apakah organisasi melakukan pengujian terhadap file backup secara berkala?	2	dilakukan uji file backup namun tidak dilakukan secara optimal	3	Mengoptimalkan proses pemulihan dan pengujian data cadangan
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	1	apakah organisasi telah menetapkan dan menerapkan kebijakan prosedur kontrol akses?	3	sudah ada dan diterapkan	3	Sudah Tercapai
			2	apakah organisasi telah menetapkan dan menerapkan kebijakan prosedur BCP?	2	kebijakan BCP sudah ditetapkan, namun penerapan belum optimal	3	Melakukan pengujian terhadap skenario yang telah ditetapkan di dalam dokumen BCP
			3	apakah organisasi telah menerapkan proteksi terhadap kabel listrik maupun data?	3	sudah diproteksi	3	Sudah Tercapai
		PR.IP-6: Data is destroyed according to policy	1	Apakah organisasi memiliki kebijakan untuk penghancuran data?	2	sudah ada kebijakannya namun penerapan belum konsisten	3	Lakukan pemantauan terhadap penerapan kebijakan retensi data
			2	Bagaimana organisasi mengelola retensi data dan memastikan data dihancurkan sesuai kebijakan?	2	sudah ada daftar retensi masing-masing data, namun belum diterapkan penghancuran sesuai dengan kebijakan	3	Lakukan pemantauan terhadap penerapan kebijakan retensi data
		PR.IP-7: Protection processes are improved	1	apakah organisasi telah melaksanakan penetration testing/vuln assessment secara berkala?	3	sudah dilakukan secara berkala	3	Sudah Tercapai
			2	Bagaimana organisasi mengimplementasikan	3	dilakukan sesuai dengan rekomendasi remediasi di laporan penetration testing	3	Sudah Tercapai

				perbaikan berdasarkan hasil evaluasi dan umpan balik?				
			3	Bagaimana organisasi menggunakan sifatnya ancaman untuk mengidentifikasi area perbaikan dalam proses perlindungan?	3	Organisasi sudah menggunakan *threat intelligence* dalam Wazuh	3	Sudah Tercapai
		PR.IP-8: Effectiveness of protection technologies is shared	1	Apakah organisasi memiliki mekanisme untuk mengukur efektivitas teknologi proteksi yang digunakan?	1	Tidak ada mekanisme untuk mengukur efektivitas teknologi proteksi	3	Membuat prosedur khusus untuk dapat mengukur dan mengevaluasi efektivitas teknologi proteksi
			2	Bagaimana hasil evaluasi efektivitas teknologi proteksi dibagikan dengan pemangku kepentingan internal dan eksternal yang relevan?	1	belum ada evaluasi efektivitas teknologi proteksi	3	Membuat prosedur khusus untuk dapat mengukur dan mengevaluasi efektivitas teknologi proteksi
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	1	Apakah organisasi memiliki rencana respons insiden dan kesinambungan bisnis yang terdokumentasi?	3	rencana respons insiden didokumentasikan dalam Handbook penanganan insiden	3	Sudah Tercapai
			2	Bagaimana organisasi menguji dan melatih staf dalam pelaksanaan rencana respons dan pemulihan?	1	belum ada pengujian dan pelatihan staf dalam pelaksanaan rencana respons	3	Lakukan pengujian skenario yang tertuang di dalam BCP
			3	Bagaimana organisasi memastikan informasi dan aset secara teratur dicadangkan dan dapat dipulihkan?	2	organisasi sudah memiliki kebijakan backup dan backup dilakukan secara berkala. Namun proses uji coba pemulihan belum dilakukan secara berkala	3	Mengoptimalkan proses pemulihan dan pengujian data cadangan
			4	Bagaimana organisasi memastikan konfigurasi yang aman untuk perangkat keras dan perangkat lunak dalam rencana respons dan pemulihan?	3	sudah ada standar konfigurasi yang diterapkan	3	Sudah Tercapai
			5	Bagaimana organisasi mengelola dan memperbarui rencana respons dan pemulihan?	3	pembaruan dilakukan tiap tahun, dan dilakukan Rapat Tinjauan Manajemen	3	Sudah Tercapai

			1	Apakah organisasi memiliki jadwal yang terdokumentasi untuk pengujian rencana respons dan pemulihan?	2	sudah ada jadwal pengujian rencana respons, namun belum dilaksanakan secara optimal	3	Lakukan pengujian skenario yang tertuang di dalam BCP
		PRJP-10: Response and recovery plans are tested	2	Bagaimana hasil pengujian rencana respons dan pemulihan didokumentasikan dan ditindaklanjuti?	1	Belum dilakukan pengujian secara terdokumentasi	3	Lakukan pengujian skenario yang tertuang di dalam BCP
			3	Apakah pelatihan tanggapan insiden melibatkan pengujian rencana pemulihan bencana?	1	Belum dilakukan pelatihan terkait pengujian rencana pemulihan bencana	3	Lakukan pengujian skenario yang tertuang di dalam BCP
		PRJP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	1	apakah organisasi telah menetapkan dan menerapkan kebijakan SDM mencakup pengadaan, screening, maupun exit clearance)?	3	sudah ada dan diterapkan	3	Sudah Tercapai
		PRJP-12: A vulnerability management plan is developed and implemented	1	Apakah organisasi memiliki rencana manajemen kerentanan yang terdokumentasi?	3	sudah ada rencana manajemen kerentanan dengan melakukan vulnerability assessment tiap bulan	3	Sudah Tercapai
			2	Apa prosedur yang diterapkan untuk mengatasi kerentanan yang ditemukan?	3	dilakukan remediasi sesuai dengan rekomendasi terhadap kerentanan yang ditemukan	3	Sudah Tercapai
	Maintenance (PRMA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PRMA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	1	Apakah proses pemeliharaan dan perbaikan aset organisasi dilakukan sesuai dengan kebijakan yang telah ditetapkan?	3	dilakukan pemeliharaan aset secara berkala	3	Sudah Tercapai
			2	Bagaimana organisasi memantau dan melacak pemeliharaan dan perbaikan yang dilakukan pada aset?	3	setiap pemeliharaan dan perbaikan dilakukan proses pelaporan terhadap pemeliharaan dan perbaikan yang dilakukan	3	Sudah Tercapai
		PRMA-2: Remote maintenance of organizational assets is approved, logged, and performed in a	1	apakah organisasi melakukan perawatan aset secara remote dengan berkala dan dicatat serta dilaporkan?				Sudah Tercapai

		manner that prevents unauthorized access	2	apakah ada pengelolaan hak akses remote bagi pihak ketiga?				Sudah Tercapai
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1**: Auditing records are determined, documented, implemented, and reviewed in accordance with policy	1	apakah organisasi sudah menerapkan pencatatan dan review logging sistem secara berkala?	3	Review log sudah dilakukan selama 3 bulan sekali	3	Sudah Tercapai
			2	apakah organisasi menerapkan standar sinkronisasi waktu (NTP)?	3	Sudah diterapkan NTP terhadap perangkat	3	Sudah Tercapai
		PR.PT-2: Removable media is protected and its use restricted according to policy	1	apakah organisasi menerapkan enkripsi terhadap storage media portable?	1	tidak didokumentasikan	3	Lakukan enkripsi terhadap media portable
			2	apakah organisasi menerapkan kebijakan prosedur clear desk dan clear screen?	3	sudah diterapkan	3	Sudah Tercapai
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	1	Apakah organisasi menerapkan prinsip fungsionalitas minimum dalam konfigurasi sistem?	3	sudah dilakukan sesuai dengan dokumen Standar Konfigurasi	3	Sudah Tercapai
			2	Bagaimana organisasi memastikan bahwa konfigurasi sistem sesuai dengan prinsip fungsionalitas minimum?	3	Sudah dilakukan pemantauan terhadap konfigurasi sistem melalui UAT, Pentest dan Vulnerability Assessment	3	Sudah Tercapai
		PR.PT-4: Communications and control networks are protected	1	apakah organisasi telah menerapkan kontrol keamanan (firewall, IDS, IPS, SIEM)?	3	ada firewall dan SIEM	3	Sudah Tercapai
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	1	Apakah arsitektur seperti failsafe, load balancing, dan hot swap diterapkan untuk memenuhi persyaratan ketahanan dalam situasi normal dan buruk?	2	Sudah diterapkan namun belum secara keseluruhan sistem	3	Lakukan penerapan failsafe, load balancing, dan hot swap secara menyeluruh di semua sistem
			2	Apa kebijakan dan prosedur yang diterapkan untuk mengelola dan mengawasi mekanisme proteksi?	3	Terdapat prosedur monitoring terhadap sistem yang diterapkan secara baiat	3	Sudah Tercapai
				Nilai Total	**281**	**2,676190476**	**318**	

Function	Category	Subcategory	No	Pertanyaan	Jawaban	Keterangan	Level Kondisi yang diinginkan	Rekomendasi
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	1	Apakah baseline operasi jaringan dan aliran data yang telah ditetapkan dan dikelola?	3	sudah ada data yang didokumentasikan dalam bentuk data VM dan topologi jaringan	3	Sudah Tercapai
			2	Bagaimana organisasi memantau dan mencatat operasi jaringan serta aliran data untuk mendeteksi aktivitas anomali?	3	Pemantauan dilakukan menggunakan Wazuh dan Zabbix	3	Sudah Tercapai
			3	Apakah infrastruktur jaringan didokumentasikan dengan baik dan aman?	3	Infrastruktur jaringan didokumentasikan dalam topologi jaringan	3	Sudah Tercapai
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	1	Apakah organisasi menganalisis kejadian yang terdeteksi untuk memahami target dan metode serangan?	3	Dilakukan analisis kejadian menggunakan reflentesi dan OWASP	3	Sudah Tercapai
			2	Apakah ada tim atau individu yang ditugaskan untuk melakukan analisis keamanan dan apa metodologi yang mereka gunakan?	3	Sudah ada yaitu tim CSIRT yang sudah di SK	3	Sudah Tercapai
			3	Bagaimana hasil analisis insiden digunakan untuk meningkatkan langkah-langkah keamanan secara terus-menerus?	3	Dilakukan dokumentasi dalam penanganan insiden dan membagikan dokumentasi ke tim yang berwenang	3	Sudah Tercapai
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	1	apakah organisasi telah menerapkan pencatatan log?	3	dilakukan, dalam SIEM	3	Sudah Tercapai
			2	Apakah ada integrasi antara berbagai sumber data dan sensor untuk pengumpulan dan korelasi data kejadian?	3	dilakukan integrasi log yang dikumpulkan dalam SIEM	3	Sudah Tercapai
		DE.AE-4: Impact of events is determined	1	apakah organisasi telah menentukan dampak dari events?	3	ada terdapat dalam SIEM	3	Sudah Tercapai

			2	Bagaimana organisasi melakukan analisis dampak dari *events* keamanan?	3	dilakukan analisis dampak dengan menggunakan *threat intelligence* sebagai acuan	3	Sudah Tercapai
			3	Apakah organisasi memantau dampak dari *events* keamanan secara berkelanjutan?	3	dilakukan monitoring berkala terhadap insiden yang terjadi, apakah insiden tersebut sudah berhasil ditangani atau masih ada dampak yang terjadi	3	Sudah Tercapai
			4	Apakah organisasi mendokumentasikan dan melaporkan hasil penentuan dampak dari *events* keamanan?	3	penentuan dampak didokumentasikan dalam dokumentasi penanganan insiden	3	Sudah Tercapai
		DE.AE-5: Incident alert thresholds are established	1	Apakah organisasi memiliki ambang batas peringatan yang telah ditetapkan untuk insiden keamanan?	3	Ambang batas merujuk kepada skala yang berada di dalam SIEM	3	Sudah Tercapai
			2	Apakah ambang batas peringatan insiden didokumentasikan dan dikomunikasikan kepada semua pemangku kepentingan terkait?	3	Ambang batas didokumentasikan di dalam SIEM dan dikomunikasikan ke Tim CSIRT	3	Sudah Tercapai
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	1	apakah jaringan di organisasi dimonitori secara berkala?	3	dilakukan monitoring berkala	3	Sudah Tercapai
			2	apakah organisasi menggunakan EDR/XDR/IDS/IPS?	3	ada, WAZUH	3	Sudah Tercapai
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	1	Apakah lingkungan fisik organisasi dimonitor untuk mendeteksi potensi kejadian keamanan siber?	3	ada catatan lognya	3	Sudah Tercapai
		DE.CM-3: Personnel activity is monitored to detect potential	1	Apakah aktivitas personel dimonitor untuk mendeteksi potensi kejadian keamanan siber?	3	dilakukan monitoring terhadap perangkat yang digunakan oleh personel menggunakan Wazuh	3	Sudah Tercapai

		cybersecurity events	2	Bagaimana organisasi merespons aktivitas personel yang mencurigakan yang terdeteksi melalui pemantauan?	3	dilakukan blocking sesuai rules yang diaktifkan dalam fitur Active Response pada Wazuh	3	Sudah Tercapai
		DE.CM-4: Malicious code is detected	1	apakah ada anti malware pada staff server organisasi?	3	ada	3	Sudah Tercapai
			2	apakah asset di organisasi terpasang anti malware?	3	ada	3	Sudah Tercapai
			3	apakah anti malware yang terpasang diupdate secara berkala?	3	ada update otomatis	3	Sudah Tercapai
			4	apakah organisasi telah menerapkan penggunaan anti malware secara terpusat?	2	sudah namun dilakukan pada server saja (tidak pada klien)	3	Lakukan penerapan *anti malware* yang bisa dikontrol secara terpusat
		DE.CM-5: Unauthorized mobile code is detected	1	apakah ada monitoring terhadap penggunaan Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript?	1	tidak ada	3	Lakukan pembatasan penggunaan *script* yang bisa didokumentasikan di dalam Standar Konfigurasi maupun Whitelist Aplikasi
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	1	Apakah aktivitas penyedia layanan eksternal dimonitor untuk mendeteksi potensi kejadian keamanan siber?	1	belum dilakukan monitoring terhadap pemasok terkait keamanan siber	3	Lakukan pemantauan terhadap pihak ketiga dan layanan-layanan eksternal yang terhubung
			2	Apakah prosedur dan protokol untuk pemantauan aktivitas penyedia layanan eksternal sudah ditetapkan dan dilkuti?	1	belum ada penerapan pemantauan penyedia layanan eksternal	3	Lakukan pemantauan terhadap pihak ketiga dan layanan-layanan eksternal yang terhubung
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	1	apakah ada pembatasan file dengan ekstensi tertentu di mail server?	3	ada	3	Sudah Tercapai
			2	apakah ada penerapan pembatasan file ekstensi dll. so, ocx, exe, py, ps1, js, jar, deb di caramunasi?	1	tidak ada	3	
			3	apakah ada pencatatan terhadap klien DHCP?	3	ada di router	3	Sudah Tercapai
			4	apakah ada monitoring terhadap penggunaan aplikasi di setiap asset?	1	tidak ada	3	

		DE.CM-8: Vulnerability scans are performed	1	Apakah organisasi melakukan pemindaian kerentanan secara berkala?	3	dilakukan secara berkala	3	Sudah Tercapai
			2	Apakah alat dan teknologi yang digunakan untuk pemindaian kerentanan sesuai dengan standar keamanan dan diperbarui?	3	teknologi yang digunakan selalu diperbarui secara berkala	3	Sudah Tercapai
			3	Bagaimana organisasi menindaklanjuti temuan dari pemindaian kerentanan?	3	dilakukan remediasi sesuai dengan rekomendasi dari kerentanan	3	Sudah Tercapai
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	1	Apakah peran dan tanggung jawab untuk deteksi kejadian keamanan siber didefinisikan dengan jelas di organisasi?	3	ada dalam SK Tim CSIRT	3	Sudah Tercapai
			2	Apakah personel yang bertanggung jawab untuk deteksi menerima pelatihan dan pemahaman yang memadai mengenai tanggung jawab mereka?	2	dilakukan pelatihan namun belum secara optimal	3	Lakukan pelatihan ke seluruh personil Tim CSIRT
		DE.DP-2: Detection activities comply with all applicable requirements	1	Apakah kegiatan deteksi di organisasi mematuhi semua persyaratan yang berlaku, termasuk peraturan dan standar industri?	2	Kegiatan deteksi dilakukan sesuai dengan *best practice* yang ada, namun belum konsisten	3	Lakukan peningkatan konsistensi terhadap kegiatan deteksi
			2	Apakah organisasi memiliki dokumentasi dan proses yang mendukung kepatuhan terhadap persyaratan deteksi yang berlaku?	1	belum ada dokumentasi terkait kepatuhan persyaratan deteksi	3	Lakukan dokumentasi terkait kepatuhan persyaratan dan regulasi mengenai deteksi
		DE.DP-3: Detection processes are tested	1	Apakah organisasi secara berkala menguji proses deteksi untuk memastikan efektivitas dan kesiapan mereka?	1	tidak dilakukan	3	Lakukan pengujian proses deteksi untuk memastikan efektivitas proses
			2	Apakah hasil dari pengujian proses deteksi didokumentasikan dan dianalisis untuk perbaikan lebih lanjut?	1	belum dilakukan	3	Lakukan pengujian proses deteksi untuk memastikan efektivitas proses

		DE.DP-4: Event detection information is communicated	1	Apakah informasi terkait deteksi insiden dikomunikasikan dengan jelas kepada semua pemangku kepentingan yang relevan?	3	dilakukan komunikasi deteksi insiden melalui grup chat Tim CSIRT	3	Sudah Tercapai
		DE.DP-5: Detection processes are continuously improved	1	Apakah organisasi secara rutin mengevaluasi proses deteksi untuk memastikan area yang memerlukan perbaikan?	1	tidak didokumentasikan	3	Lakukan evaluasi proses deteksi dan dokumentasikan
			2	Bagaimana organisasi menyesuaikan proses deteksi untuk mengatasi ancaman atau teknik baru yang muncul?	2	proses deteksi diperbarui manual tidak didokumentasikan	3	Lakukan evaluasi proses deteksi dan dokumentasikan
				Nilai Total	**104**	**2,476190476**	**126**	

Function	Category	Subcategory	No	Pertanyaan	jawaban	keterangan	Level Kondisi yang diinginkan	Rekomendasi
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	1	Apakah organisasi memiliki prosedur dalam penanganan insiden?	3	punya dan diterapkan	3	Sudah Tercapai
			2	apakah organisasi mengeksekusi penanganan insiden sesuai dengan prosedur yang ada?	3	sesuai	3	Sudah Tercapai
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	1	apakah organisasi sudah menetapkan tim keamanan siber?	3	sudah	3	Sudah Tercapai
			2	apakah mekanisme komunikasi antar personil tim keamanan siber sudah ada?	3	sudah ada	3	Sudah Tercapai

	external support from law enforcement agencies).		3	apakah ada mekanisme komunikasi dengan pihak eksternal yang berhubungan dengan keamanan siber?	3	sudah ada	3	Sudah Tercapai
		RS.CO-2: Incidents are reported consistent with established criteria	1	Apakah organisasi memiliki kriteria yang jelas untuk pelaporan insiden keamanan siber?	3	kriteria merujuk ke referensi OWASP	3	Sudah Tercapai
			2	Bagaimana organisasi memastikan bahwa semua insiden dilaporkan sesuai dengan kriteria yang telah ditetapkan?	3	Adanya validasi laporan sesuai dengan referensi OWASP	3	Sudah Tercapai
			3	Apakah organisasi memberikan pelatihan kepada staf tentang kriteria dan prosedur pelaporan insiden?	2	belum dilakukan pelatihan secara berkala	3	
		RS.CO-3: Information is shared consistent with response plans	1	Apakah organisasi memiliki rencana respons insiden yang mencakup prosedur berbagi informasi?	3	sudah ada rencana respons insiden dan berbagi informasi dilakukan via grup chat Tim CSIRT	3	Sudah Tercapai
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	1	Apakah organisasi memiliki prosedur untuk koordinasi dengan pemangku kepentingan selama insiden keamanan siber?	3	sudah ada prosedur dan daftar kontak yang berkepentingan dengan insiden keamanan siber	3	Sudah Tercapai
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	1	apakah organisasi melakukan pertukaran informasi dengan pihak eskternal untuk mencapai kesadaran keamanan siber yang lebih luas?	3	dilakukan lewat humas tangsel, setiap ada issue mengenai keamanan siber	3	Sudah Tercapai
	Analysis (RS.AN): Analysis is conducted to ensure effective response	**RS.AN-1:** Notifications from detection systems are investigated	1	apakah dilakukan monitoring log pada jaringan, sistem, dan aplikasi?	3	dilakukan secara berkala	3	Sudah Tercapai
			2	apakah dilakukan review terhadap log?	3	Sudah dilakukan setiap 3 bulan sekali	3	Sudah Tercapai

	and support recovery activities.		3	apakah dilakukan investigasi terhadap insiden sampai akar masalahnya?	2	dilakukan namun belum konsisten	3	Lakukan proses analisis akar masalah secara konsisten terhadap seluruh insiden
		RS.AN-2: The impact of the incident is understood	1	Apakah organisasi memiliki proses yang terdokumentasi untuk mengidentifikasi dampak insiden siber terhadap operasi bisnis?	2	Ada di dalam dokumen BIA, namun belum semua bentuk insiden diidentifikasi	3	Lakukan pembaruan terhadap dokumen BIA
		RS.AN-3: Forensics are performed	1	Apakah organisasi memiliki prosedur forensik yang terdokumentasi untuk menganalisis insiden siber?	1	belum ada prosedur forensik untuk menganalisis insiden siber	3	Lakukan pembuatan prosedur untuk Digital Forensik
			2	Bagaimana organisasi melakukan investigasi forensik setelah insiden terjadi?	1	belum dilakukan	3	Lakukan pembuatan prosedur untuk Digital Forensik
			3	Apakah organisasi memiliki proses yang jelas untuk menyimpan dan melindungi bukti digital selama dan setelah investigasi forensik?	1	belum dilakukan	3	Lakukan pembuatan prosedur untuk Digital Forensik
		RS.AN-4: Incidents are categorized consistent with response plans	1	Apakah organisasi memiliki prosedur yang terdokumentasi untuk mengkategorikan insiden sesuai dengan rencana respons?	1	belum diterapkan	3	Lakukan pembuatan prosedur penanganan insiden sesuai dengan kategori insiden
			2	Bagaimana organisasi mendokumentasikan dan melaporkan hasil kategorisasi insiden?	3	kategorisasi insiden disesuaikan dengan OWASP	3	Sudah Tercapai
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security	1	Apakah organisasi memiliki proses yang terdokumentasi untuk menerima laporan kerentanan dari sumber internal dan eksternal?	3	proses penerimaan laporan sudah didokumentasikan melalui Tim CSIRT	3	Sudah Tercapai
			2	Apakah organisasi memiliki prosedur yang jelas untuk merespons kerentanan setelah analisis dilakukan?	3	Respons kerentanan sesuai dengan prosedur penanganan insiden	3	Sudah Tercapai

		bulletins, or security researchers)						
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	1	Apakah organisasi memiliki prosedur yang terdokumentasi untuk menanggulangi insiden?	3	Sudah ada prosedur penanganan insiden	3	Sudah Tercapai
			2	Bagaimana organisasi mengevaluasi efektivitas penanggulangan insiden setelah insiden terjadi?	3	dilakukan monitoring berkala terhadap sistem yang terdampak	3	Sudah Tercapai
		RS.MI-2: Incidents are mitigated	1	Apakah organisasi memiliki prosedur yang terdokumentasi untuk mitigasi insiden?	3	ada, dalam manajemen risiko	3	Sudah Tercapai
			2	Bagaimana organisasi mengevaluasi efektivitas mitigasi insiden setelah insiden terjadi?	3	evaluasi efektivitas dilakukan dengan monitoring berkala terhadap insiden setelah dilakukan mitigasi	3	Sudah Tercapai
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	1	Apakah organisasi memiliki prosedur untuk mengidentifikasi dan menilai kerentanan yang baru ditemukan?	3	ada, dalam manajemen risiko	3	Sudah Tercapai
			2	Bagaimana organisasi mendokumentasikan dan mengkomunikasikan risiko yang diterima dari kerentanan yang tidak dimitigasi?	3	dilakukan dalam risk register dan ditetapkan oleh top manajemen serta dikomunikasikan ke pihak terkait lewat kegiatan security awareness	3	Sudah Tercapai
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous	**RS.IM-1:** Response plans incorporate lessons learned	1	Apakah rencana respons insiden mencakup mekanisme untuk mengintegrasikan pelajaran yang dipetik dari insiden sebelumnya?	3	sudah dilakukan dengan mendokumentasikan penanganan insiden dan mengkomunikasikannya ke Tim CSIRT	3	Sudah Tercapai
			2	Apakah pelajaran yang dipetik diterapkan dalam latihan dan pengujian rencana respons?	1	Belum ada pengujian rencana respons	3	Lakukan perencanaan uji coba skenario pemulihan dan respons sesuai dengan BCP

	detection/response activities	RS.IM-2: Response strategies are updated	1	Seberapa sering strategi respons diperbarui untuk mencerminkan perubahan dalam lingkungan ancaman dan teknologi?	2	strategi respons diperbarui sesuai dengan tren insiden, namun tidak didokumentasikan secara optimal	3	Lakukan pembaruan dan dokumentasi terhadap strategi respons
			2	Bagaimana pembaruan dalam strategi respons dikomunikasikan kepada tim yang relevan?	3	Pembaruan dilakukan dan dikomunikasikan di grup chat Tim CSIRT dan saat Security Awareness	3	Sudah Tercapai
				Nilai Total	**82**	**2,5625**	**96**	

Function	Category	Subcategory	No	Pertanyaan	Jawaban	Keterangan	Level Kondisi yang diinginkan	Rekomendasi
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident.	1	Apakah rencana pemulihan dilaksanakan selama atau setelah insiden siber?	2	Rencana pemulihan dilaksanakan, namun tidak sesuai dengan dokumen BCP	3	Lakukan review dan pembaruan terhadap dokumen BCP
			2	Bagaimana organisasi mengevaluasi efektivitas pelaksanaan rencana pemulihan setelah insiden?	1	Belum ada evaluasi	3	Lakukan evaluasi dokumen BCP
			3	Bagaimana komunikasi dan koordinasi dilakukan selama pelaksanaan rencana pemulihan?	3	Rencana pemulihan dikomunikasikan via grup chat Tim CSIRT	3	Sudah Tercapai
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	1	Apakah pelajaran yang dipetik dari insiden sebelumnya diintegrasikan dalam rencana pemulihan?	2	integrasi dalam dokumen BCP belum dilakukan secara optimal	3	Lakukan review dan pembaruan terhadap dokumen BCP
		RC.IM-2: Recovery strategies are updated	1	Apakah ada proses yang digunakan untuk memperbarui strategi pemulihan?	3	Pembaruan BCP dilakukan sekali dalam setahun	3	Sudah Tercapai
			2	Bagaimana pemangku kepentingan dilibatkan dalam pembaruan strategi pemulihan?	3	Pemangku kepentingan melakukan pertemuan bersama terkait pembaruan BCP	3	Sudah Tercapai

			3	Bagaimana dokumentasi dan pengelolaan pembaruan strategi pemulihan dilakukan?	3	Pembaruan dokumen BCP didokumentasikan dalam bentuk hasil revisi	3	Sudah Tercapai
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	1	apakah organisasi mengelola hubungan dengan pihak publik atau pihak eksternal?	3	hubungan baik dijalankan dengan para pemeteri publik dan sistansi BSSN	3	Sudah Tercapai
		RC.CO-2: Reputation is repaired after an incident	1	apakah dilakukan pemulihan reputasi setelah terjadinya insiden?	3	ada upaya komunikasi terhadap stakeholders untuk pemulihan reputasi	3	Sudah Tercapai
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	1	apakah aktivitas recovery dikomunikasi secara internal maupun eksternal yang berkepentingan?	3	hanya dikomunikasikan secara internal	3	Sudah Tercapai
				Nilai Total	**26**	**2,6**	**30**	