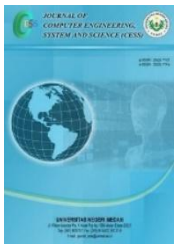
CESS
(Journal of Computing Engineering, System and Science) 8(2) July 2023 271-283

e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess



Audit Keamanan Siber Menggunakan Kerangka Kerja CIS CSC, NIST CSF, dan COBIT 2019

Cyber Security Audit using CIS CSC, NIST CSF and COBIT 2019 Framework

Viny Fadila[1*], Nurul Mutiah[2], Renny Puspita Sari[3]

[1,2,3] Program Studi Sistem Informasi, Universitas Tanjungpura
Prof.Dr.H.Hadari Nawawi, Jendral Ahmad Yani, Pontianak - Kalimantan Barat 78124
email: [1]vinyfadila@student.untan.ac.id, [2]nurul@sisfo.untan.ac.id, [3]rennysari@sisfo.untan.ac.id

A B S T R A K

Tingginya penggunaan teknologi dan informasi saat ini mengakibatkan peningkatan risiko dan ancaman keamanan data dan informasi. Dinas Komunikasi dan Informatika Kota Pontianak, dinas pemerintahan yang memanfaatkan dan menggunakan banyak teknologi informasi. Untuk mengetahui sejauh mana kemampuan Dinas Komunikasi dan Informatika Kota Pontianak dalam mengelola keamanan siber, maka diperlukan audit keamanan siber. Audit dapat dilakukan dengan menggabungkan *framework* CIS CSC (*Center for Internet Security Critical Security Controls*) untuk membatasi focus area keamanan siber aset TI serta menggunakan NIST CSF (*National Institute of Standards and Technology Cybersecurity Framework*) dan COBIT 2019 (*Control Objective for Information Technologies*) untuk melakukan perhitungan level kapabilitas. Perhitungan level kapabilitas menggunakan metode CPM (*COBIT Performance Model).* Hasil perhitungan level kapabilitas keamanan siber Dinas Komunikasi dan Informatika Kota Pontianak pada *Identify* (ID) mencapai level 3.9, *Protect* (PR) mencapai level 3.4, *Detect* (DE) mencapai level 2.5, dan *Respond* (RS) mencapai level 4. Terdapat 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*.

Kata Kunci: *COBIT 2019, NIST CSF, CIS CSC, Keamanan Siber, COBIT Performance Model.*

A B S T R A C T

The frequent use of technology and information today impacts the increased risk and threats to data and information security. Department of Information and Communications of Pontianak is the department that utilizes and uses a lot of information technology. To find out how far the Pontianak City Communication and Informatics Office is capable of managing

**Penulis Korespondensi:*
email: vinyfadila@student.untan.ac.id

cyber security, a cyber security audit is needed. Audits can be conducted by combining the CIS CSC (Center for Internet Security Critical Security Controls) framework to define the cybersecurity focus areas of IT assets and using the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) and COBIT 2019 (Control Objective for Information Technologies) to calculate the capability level. Capability level calculation uses the CPM (COBIT Performance Model) method. The results of calculating the level of cyber security capability of the Pontianak City Communication and Informatics Service for Identification (ID) reaches level 3.9, Protect (PR) reaches level 3.4, Detect (DE) reaches level 2.5, and Respond (RS) reaches level 4. There are 19 activity recommendations to be carried out in order to achieve the desired level of cybersecurity, then capture recommendation activities into the action priority matrix, 10 activities included in the Quick Wins quadrant, and 9 activities entered into the Major Projects quadrant.

Keywords: *COBIT 2019, NIST CSF, CIS CSC, Cyber Security, COBIT Performance Model.*

1. PENDAHULUAN

Saat ini, teknologi informasi digunakan pada banyak sekali bidang kehidupan. Semakin tinggi penggunaan teknologi dan informasi pada sebuah perusahaan atau organisasi, maka semakin besar pula tingkat risiko dan ancaman yang mengancam keamanan data dan informasi perusahaan tersebut. Baik pemerintah maupun perusahaan mengambil banyak langkah untuk mencegah kejahatan siber ini. Selain itu berbagai tindakan keamanan siber masih menjadi perhatian yang sangat besar bagi banyak orang [1]. Saat ini sudah banyak Dinas Pemerintahan yang memanfaatkan kemajuan teknologi dalam menunjang proses bisnisnya adalah DISKOMINFO (Dinas Komunikasi dan Informatika) Kota Pontianak.

DISKOMINFO Kota Pontianak mempunyai tugas dalam membantu Walikota Kota Pontianak dalam bidang komunikasi, informatika, statistik, dan persandian. Diskominfo memiliki tujuan untuk meningkatkan kualitas pelaksanaan Reformasi Birokrasi dan meningkatkan kualitas layanan kepada masyarakat [2]. Sebagai Dinas Pemerintahan yang memanfaatkan dan menggunakan banyak teknologi informasi, tentu perlu diperhatikan masalah keamanan informasinya.

Berdasarkan hasil observasi dan wawancara bersama Kepala Seksi Persandian dan Keamanan Informasi DISKOMINFO Kota Pontianak, diketahui bahwa pernah terjadi ancaman keamanan informasi. Tidak semua aplikasi di DISKOMINFO Kota Pontianak adalah milik pribadi, beberapa aplikasi yang berasal dari pihak ketiga, dan beberapa aplikasi tersebut masih dikelola oleh pihak pembuatnya sendiri. Kebocoran informasi tersebut datangnya dari admin pihak ketiga, selama beberapa waktu itu terjadi pergantian admin, tetapi tanpa melakukan pembaharuan password, sehingga pernah terjadi insiden admin lama login kembali dan melakukan kekacauan pada aplikasi tersebut. Insiden lainnya DISKOMINFO Kota Pontianak pernak mengalami kerusakan harddisk sehingga menyebabkan beberapa data hilang serta menghambat kegiatan operasional. Dari beberapa insiden tersebut, DISKOMINFO Kota Pontianak semakin meningkatkan tingkat kewaspadaan agar tidak terjadi insiden yang sama.

Keamanan siber atau *cyber security* memiliki banyak standar dan framework dalam melakukan audit maupun pengukuran, dalam penelitian ini, peneliti memilih menggunakan 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 dilakukan audit manajemen risiko keamanan siber pada

DISKOMINFO Kota Pontianak. CIS digunakan untuk membatasi focus area keamanan siber aset TI yang nantinya akan dipetakan ke NIST CSF. NIST CSF digunakan sebagai kerangka kerja yang akan digunakan bersamaan dengan kerangka kerja COBIT 2019 untuk melakukan perhitungan tingkat kapabilitas. Dalam melakukan perhitungan tingkat kapabilitas, penelitian ini menggunakan metode CPM (*COBIT Performance Model)*.

Berdasarkan pemaparan diatas, maka akan dilakukan audit keamanan siber menggunakan kerangka kerja CIS CSC, NIST CSF dan COBIT 2019 pada DISKOMINFO Kota Pontianak. Penelitian ini diharapkan bisa mengenali keamanan siber Dinas Komunikasi dan Informatika Kota Pontianak berada pada level berapa dan mengetahui tingkat kesenjangan (*gap*) pada keamanan siber DISKOMINFO Kota Pontianak, serta diharapkan dapat memberikan rekomendasi-rekomendasi kepada DISKOMINFO Kota Pontianak untuk melakukan perbaikan pada manajemen keamanan siber DISKOMINFO Kota Pontianak agar menjadi lebih optimal dan mencapai level yang diharapkan.

2. DASAR TEORI

2.1. Keamanan Siber

Keamanan siber bukan tentang menciptakan sistem yang tidak dapat diretas, keamanan siber adalah tentang mengurangi risiko bahwa suatu sistem akan dilanggar (*confidentiality*), dimodifikasi (*integrity*), atau terganggu (*availability*) tanpa otorisasi. Ketiga konsep ini, kerahasiaan, integritas, dan ketersediaan, merupakan fondasi inti dari setiap program keamanan siber [3]. *confidentiality* merupakan perlindungan data dari pengguna yang tidak berwenang, *integrity* melindungi data dari modifikasi oleh user yang tidak berwenang, dan *availability* memastikan data dapat diakses oleh pengguna yang berwenang untuk ditinjau atau dimodifikasi [3]

Keamanan siber masih menjadi bagian dari keamanan informasi, perbedaannya dengan keamanan informasi, keamanan siber tidak mencakup penanganan ancaman yang seperti kesalahan individu, bencana alam, atau keamanan fisik. Dapat disimpulkan bahwa keamanan siber diperlukan karena adanya ancaman yang datang dari sistem yang saling terinterkoneksi [4].

2.2. COBIT 2019

COBIT (*Control Objectives for Information and Related Technologies*) adalah seperangkat praktik dan pedoman untuk membantu manajemen mendapatkan hasil maksimal dari sumber daya TI, juga disebut sebagai kerangka kerja atau metodologi. Pada COBIT 2019, tata kelola (*governance*) dan manajemen (*management*) dibedakan. Hal ini sejalan dengan ISO/IEC 38500:2015 dan ISO/IEC 27014:2013. Tata kelola teknologi, menjelaskan keperluan penting dari sistem tata kelola untuk teknologi dan informasi perusahaan. Manajemen, prinsip dimana kerangka tata kelola dapat kita gunakan untuk membangun sistem tata kelola pada perusahaan.

Domain pada COBIT 2019 masih sama dengan domain COBIT 5 dan tidak ada perubahan nama dengan kelima domain tersebut. Hanya saja, pada domain ini sekarang berisi 40 model inti dari yang sebelumnya berjumlah 37 proses. Penambahan terjadi pada APO14. *Managed Data.* Sisanya terdapat dari perpecahan dua proses COBIT 5 karena perbedaan ukuran dan kontennya. BAI01. *Managed Programs and Project* dipecah menjadi BAI01. *Managed Programs,* dan BAI11. *Managed Projects.* Sedangkan, MEA02. *Monitor, Evaluate and Assess*

the System of Internal Control dan MEA04. *Managed Assurance.* Meskipun ISACA menyatakan bahwa secara konten tidak terlalu banyak perubahan. [7]

2.3. NIST CSF

NIST CSF (*National Institute of Standards and Technology Cybersecurity Framework*) adalah kerangka kerja keamanan siber yang bisa dipakai untuk menuntun perusahaan maupun organisasi pada kegiatan keamanan siber serta mempertimbangkan risiko yang akan terjadi. NIST CSF memberikan panduan dan tahan untuk mempertinggi keamanan siber yang didapatkan melalui analisis manajemen risiko keamanan siber (NIST CSF, Ver. 1.1).

Kerangka kerja ini terdiri dari 3 bagian, yaitu *Core, Tiers,* dan *Profile*.

1. *Core*: Merupakan inti kerangka kerja, menyediakan pedoman, standar, dan praktik industri menggunakan langkah yang bisa memberikan dampak terhadap komunikasi dan hasil aktivitas keamanan siber antar organisasi dari level pelaksanaan/pengoperasian hingga level eksekutif [5]. Terdapat 5 fungsi yang berkesinambungan dan bersamaan pada kerangka kerja *core*, yaitu *Identify, Protect, Detect, Respond,* dan *Recover.*
2. *Tier*: Menggambarkan tingkat keamanan siber manajemen risiko pada organisasi yang mematuhi kerangka kerja. Tingkatan memberikan konteks dan sejauh mana risiko keamanan siber dikelola dan sejauh mana kebutuhan bisnis dipertimbangkan dalam manajemen risiko keamanan siber.
3. *Profile*: Menampilkan hasil yang didapat dari *business needs* yang telah ditetapkan organisasi dari *Category* dan *Sub Category* Kerangka Kerja.

2.4. CIS CSC

CIS CSC *(Center of Internet Security Critical Security Controls)* adalah serangkaian perlindungan yang diprioritaskan untuk mengurangi serangan siber yang paling umum terhadap sistem dan jaringan [6]. Tujuan dari dibuatnya CIS Control bukan untuk menggantikan kerangka kerja keamanan siber, tetapi sebagai kerangka kerja alternatif sebagai panduan melakukan praktik pertahanan pada keamanan siber di organisasi maupun perusahaan. CIS Control v8 memiliki 18 butir kontrol yang terdiri dari Inventaris dan Kontrol Aset Perusahaan, Inventaris dan Kontrol Aset Perangkat Lunak, Perlindungan Data, Konfigurasi Aman Aset dan Perangkat Lunak Perusahaan, Manajemen Akun, Manajemen Akses Kontrol, Manajemen Kerentanan Berkelanjutan, Manajemen Log Audit, Perlindungan Email dan Browser Web, Pertahanan Malware, Data Pemulihan, Manajemen Infrastruktur Jaringan, Pemantauan dan Pertahanan Jaringan, Pelatihan Kesadaran dan Keterampilan Keamanan, Manajemen Penyedia Layanan, Keamanan Perangkat Lunak Aplikasi, Manajemen Respons Insiden, dan Pengujian Penetrasi

2.5. CPM

Performance management atau biasa disebut manajemen kinerja merupakan bagian penting dari tata kelola dan manajemen. Manajemen kinerja mencakup metode dan konsep, terbagi menjadi dua yaitu tingkat kapabilitas dan tingkat kematangan kinerja. COBIT 2019 menggunakan istilah CPM (*COBIT Performance Management*) untuk menggambarkan kegiatan ini, dan CPM juga termasuk bagian integral dari kerangka COBIT [8].

Tingkat kapabilitas adalah ukuran seberapa baik suatu proses diimplementasikan dan berkinerja. Tingkat kematangan adalah ukuran bagaimana proses yang terkandung dalam area fokus mencapai tingkat kemampuan tertentu, melalui kumpulan bukti mendasar yang substansial untuk mendukung tujuan perusahaan [10].

Dalam proses penilaian tingkat kapabilitas, dapat dinyatakan dengan serangkaian peringkat. Kisaran peringkat yang tersedia bergantung pada konteks dimana penilaian kinerja dibuat:

1. Terdapat metode formal yang menilai independen berdasarkan kumpulan peringkat lulus/gagal biner.
2. Metode tidak formal (biasa dipakai dalam konteks penilaian kinerja) penilaian dengan rentang peringkat yang lebih besar, seperti rangkaian berikut:
   - *Fully* — Level yang dicapai lebih dari 85%.
   - *Largely* — level yang dicapai antara 50% dan 80% .
   - *Partially* —Level yang dicapai antara 15% dan 50%.
   - *Not* — Level yang dicapai kurang dari 15%.

2.6. Action Priority Matrix

Action Priority Matrix adalah alat atau matrix yang membantu kita untuk memanfaatkan waktu sebaik-baiknya dengan memilih tugas dan peluang yang tepat untuk dikejar dengan mengerjakan tugas yang benar dalam urutan yang benar. *Action Priority Matrix* ingin memastikan bahwa kita memilih tugas-tugas yang akan memberi pengembalian paling signifikan atas investasi waktu, *Action Priority Matrix* juga ingin menghindari tugas-tugas yang tidak membuat maju (Sridharan, 2021).

Gambar 1. Gambaran Umum Model Penilaian Proses

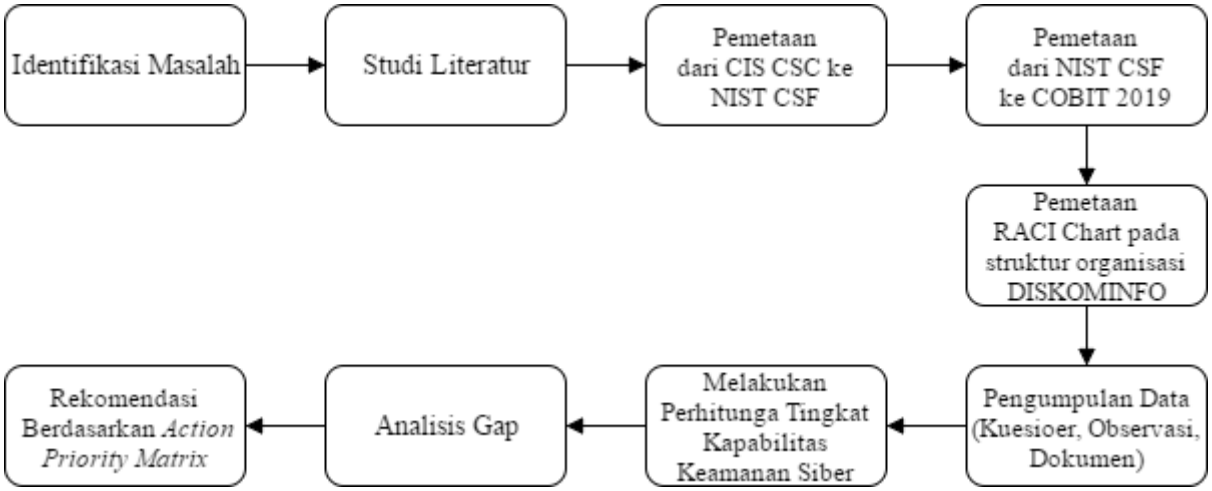
Terdiri dari 2x2. Pada sumbu X memiliki upaya yang diperlukan untuk menyelesaikan tugas, dari rendah ke tinggi. Pada sumbu Y, memiliki dampak pada hasil yang akan didapat dari menyelesaikan tugas.

- *Quick Wins:* Kuadran ini berisi tugas-tugas yang membutuhkan sedikit usaha tetapi memiliki dampak yang tinggi. Dengan demikian, kuadran ini yang harus dikerjakan terlebih dahulu.
- *Major Projects:* Kuadran ini berisikan tugas yang dapat memberi hasil (dampak) yang signifikan, tetapi mengharuskan kita untuk menginvestasikan banyak waktu ke dalamnya.

- *Fill-ins:* Kuadran ini berisikan tugas yang membutuhkan sedikit usaha untuk dilakukan, tetapi juga berdampak kecil pada hasil yang didapat
- *Thankless Task:* Pada kuadran Ini, tugas-tugas yang memiliki dampak rendah tetapi masih membutuhkan usaha yang tinggi. Kita harus menghilangkan tugas-tugas ini, karena mereka tidak sepadan dengan waktu untuk menyelesaikannya.

3. METODE

Berikut merupakan langkah-langkah yang harus dilakukan dalam menyelesaikan penelitian ini.



Gambar 2. Metode Penelitian

Penelitian diawali dengan mengidentifikasi masalah yang terjadi di DISKOMINFO Kota Pontianak. Langkah selanjutnya adalah dengan melakukan studi literatur dengan memahami penggunaan CIS CSC dan NIST CSF sebagai kerangka kerja keamanan siber dan memahami penggunaan kerangka kerja COBIT 2019 dalam melakukan perhitungan tingkat kapabilitas keamanan siber. Selanjutnya melakukan pemetaan dari control pada CIS CSC ke fungsi-fungsi di NIST CSF dan dilanjutkan dengan melakukan pemetaan dari NIST CSF ke COBIT 2019. Selanjutnya mengumpulkan data yang diperlukan dalam penelitian ini seperti pembuatan kuesioner, melakukan observasi langsung di DISKOMINFO Kota Pontianak. Tahap selanjutnya adalah menghitung tingkat kapabilitas keamanan siber pada DISKOMINFO Kota Pontianak dan mengukur kesenjangan antara tingkat kapabilitas saat ini dengan tingkat kapabilitas yang diharapkan atau *Gap Analysis.* Tahap terakhir memberikan rekomendasi perbaikan yang harus dilakukan DISKOMINFO Kota Pontianak untuk meningkatkan tingkat kapabilitas keamanan sibernya.

4. HASIL DAN PEMBAHASAN

4.1. Proses Pemetaan

Proses ini diawali dengan memetakan Sub-kontrol di CIS CSC ke Sub-kategori di NIST CSF, berikut proses pemetaan sub-kontrol di CIS CSC ke sub-kategori di NIST CSF pada kontrol 1 dapat dilihat pada tabel 1 [6].

Tabel 1. Pemetaan dari Sub-kontrol CIS CSC ke Sub-kategori NIST CSF

No	Sub-kontrol (CIS CSC)	Sub-kategori (NIST CSF)	Deskripsi Sub-kategori
01. Inventaris dan Kontrol Aset Perusahaan			
1.	Membangun dan Memelihara Aset Perusahaan Terperinci	ID-AM 1	Perangkat dan sistem di organisasi terdaftar dan diinventarisir
		PR-DS 3	Mengelola aset secara formal melalui transfer, penghapusan, dan disposisi
2.	Menangani Aset Tidak Sah		
3.	Memanfaatkan Alat Penemuan Aktif	DE-CM 7	Memantau personil, jaringan, perangkat keras, dan perangkat lunak tak berizin dilakukan.
4.	Gunakan Dynamic Host Configuration Protocol (DHCP) Logging untuk Memperbarui Inventaris Aset Perusahaan	DE-CM 7	Memantau personil, jaringan, perangkat keras, dan perangkat lunak tak berizin dilakukan.
5.	Gunakan Alat Penemuan Aset Pasif	DE-CM 7	Memantau personil, jaringan, perangkat keras, dan perangkat lunak tak berizin dilakukan.

Setelah menyelesaikan pemetaan dari sub-kontrol di CIS CSC ke sub-kategori di NIST CSF, selanjutkan dilakukan pemetaan untuk proses yang terpilih di NIST CSF berdasarkan hasil pemetaan sebelumnya, ke domain yang terdapat pada COBIT 2019. Berikut proses pemetaan dari sub-kategori NIST CSF ke domain COBIT 2019 pada kategori ID (Identify) yang dapat dilihat pada tabel 2 [9]

Tabel 2. Pemetaan Sub-kategori NIST CSF ke Domain COBIT 2019

NO	Sub-Kategori (NIST CSF)	Deskripsi Sub-Kategori	Domain (COBIT 2019)	Deskripsi Domain
1.	ID.AM-1	Perangkat dan sistem di organisasi terdaftar dan diinventarisir	BAI09.01	Mengidentifikasi dan mencatat aset saat ini
			BAI09.02	Mengelola aset penting
2.	ID.AM-2	Platform perangkat lunak dan aplikasi di dalam organisasi diinventarisir	BAI09.01	Mengidentifikasi dan mencatat aset saat ini
			BAI09.02	Mengelola aset penting
			BAI09.05	Mengelola lisensi

3.	ID.AM-3	Komunikasi dalam organisasi dan alur data dipetakan	DSS05.02	Mengelola keamanan jaringan dan konektivitas
			APO14.08	Mengelola siklus hidup aset data
4.	ID.AM 4	Sistem informasi eksternal dikatalogkan	APO02.02	Menilai kemampuan, kinerja, dan kematangan digital perusahaan saat ini.
			APO10.01	Mengidentifikasi dan mengevaluasi hubungan dan kontrak vendor.
			APO10.04	Mengelola risiko vendor
			DSS01.02	Mengelola *outsourced* layanan IT
6.	ID.AM-6	Peran dan tanggung jawab untuk seluruh tenaga kerja keamanan siber dan pemangku kepentingan pihak ketiga.	APO01.02	Mengkomunikasikan tujuan manajemen, arahan, dan keputusan yang dibuat
			APO01.05	Menetapkan peran dan tanggung jawab
			APO07.06	Mengelola staf kontrak
			APO13.01	Membangun dan memelihara sistem manajemen keamanan informasi
			DSS06.03	Mengelola peran, tanggung jawab, hak akses, dan tingkat otoritas

4.2. Pemetaan RACI *Chart*

Pada tahapan ini, dilakukan pemetaan terhadap peran yang terdapat di RACI Chart, ke peran yang sesuai dengan jabatan di DISKOMINFO Kota Pontianak

Tabel 3. Pemetaan dari RACI *Chart* ke jabatan di DISKOMINFO Kota Pontianak

Role	Jabatan di KOMINFO
Board	Kepala Dinas
Executive Committee	Kepala Dinas
Chief Executive Officer	Kepala Dinas
Chief Financial Officer	Kepala Sub Bagian Perencanaan dan Keuangan
Chief Operating Officer	Kepala Dinas

Chief Risk Officer	Kepala Seksi Persandian dan Keamanan Sistem Informasi
Chief Information Officer	Pengembangan Kebijakan Aplikasi Informatika
Chief Technology Officer	Pengembangan Kebijakan Aplikasi Informatika
Chief Digital Officer	Kepala Bidang Informasi dan Komunikasi Publik
IT Governance Board	Analis Kebijakan Sarana dan Prasarana TIK
Architecture Board	Kepala Dinas
Enterprise Risk Committee	Kepala Seksi Persandian dan Keamanan Sistem Informasi
Chief Information Security Officer	Kepala Seksi Persandian dan Keamanan Sistem Informasi
Business Process Owner	Kepala Dinas
Steering (Programs/Projects) Committee	Kepala Sub Bagian Umum dan Aparatur
Business Continuity Manager	Kepala Dinas

4.3. Pemilihan Proses Activity

Setelah menyelesaikan proses pemetaan dan mendapatkan domain COBIT 2019 yang diinginkan, selanjutnya memilih proses activity pada COBIT 2019 yang sesuai dengan deskripsi sub-kategori pada NIST CSF. Pemilihan proses activity pada sub-kategori ID.AM-1 yang terdapat domain BAI09.01 dan BAI09.02 dapat dilihat pada tabel 3

Tabel 4. Proses activity COBIT 2019 pada sub-kategori ID.AM-1

ID.AM-1 Perangkat dan sistem di organisasi terdaftar dan diinventarisir	
Domain: BAI09.01 Mengidentifikasi dan mencatat aset saat ini	*Capability*
1. Identifikasi semua aset yang dimiliki dalam daftar aset yang mencatat status saat ini. Aset dilaporkan di neraca; aset dibeli atau dibuat untuk meningkatkan nilai perusahaan atau menguntungkan operasi perusahaan (misalnya, perangkat keras dan perangkat lunak). Identifikasi semua aset yang dimiliki dan dipertahankan keselarasan dengan manajemen perubahan dan proses manajemen	2

konfigurasi, sistem manajemen konfigurasi, dan catatan akuntansi keuangan.				
2. Verifikasi keberadaan semua aset yang dimiliki dengan melakukan pemeriksaan dan rekonsiliasi persediaan fisik dan logis secara teratur. Sertakan penggunaan *search tools* perangkat lunak.				4
3. Tentukan secara teratur apakah setiap aset terus memberikan nilai. Jika demikian, perkirakan masa manfaat yang diharapkan untuk memberikan nilai.				
Proses Tata Kelola	Input		Output	
	From	Description	Description	To
ID.AM-1 Perangkat dan sistem fisik di dalam organisasi diinventarisir	BAI03.04	Pembaruan untuk aset inventaris	Hasil ulasan sesuai tujuan	APO02.02
	BAI10.02	Repositori Konfi-gurasi		
Accountable: Chief Technology Officer				
Aktivitas				
Domain BAI09.02 Mengelola aset penting				
1. Identifikasi aset yang penting dalam menyediakan kemampuan layanan dengan merujuk persyaratan dalam definisi layanan, SLA (*Service level agreements*), dan sistem manajemen konfigurasi.				
Proses Tata Kelola	Input		Output	
	From	Description	Description	
BAI09.02 Mengelola aset penting			Perjanjian pemeliharaan	
Accountable: Chief Technology Officer				

4.4. Perhitungan Level Kapabilitas

Untuk melakukan perhitungan level kapabilitas, sebelumnya dilakukan pengumpulan data menggunakan metode kuesioner yang didapat dari hasil pemilihan activity proses. Perhitungan level kapabilitas menggunakan metode CPM (COBIT Performance Metode) dengan skala pengukuran yang dapat dilihat pada tabel 4 [7]

Tabel 5. Skala Pengukuran CPM

Nilai (%)	Keterangan
0 - 14	*Not*
14 - 49	*Partially*
50 - 84	*Largely*
85 - 100	*Fully*

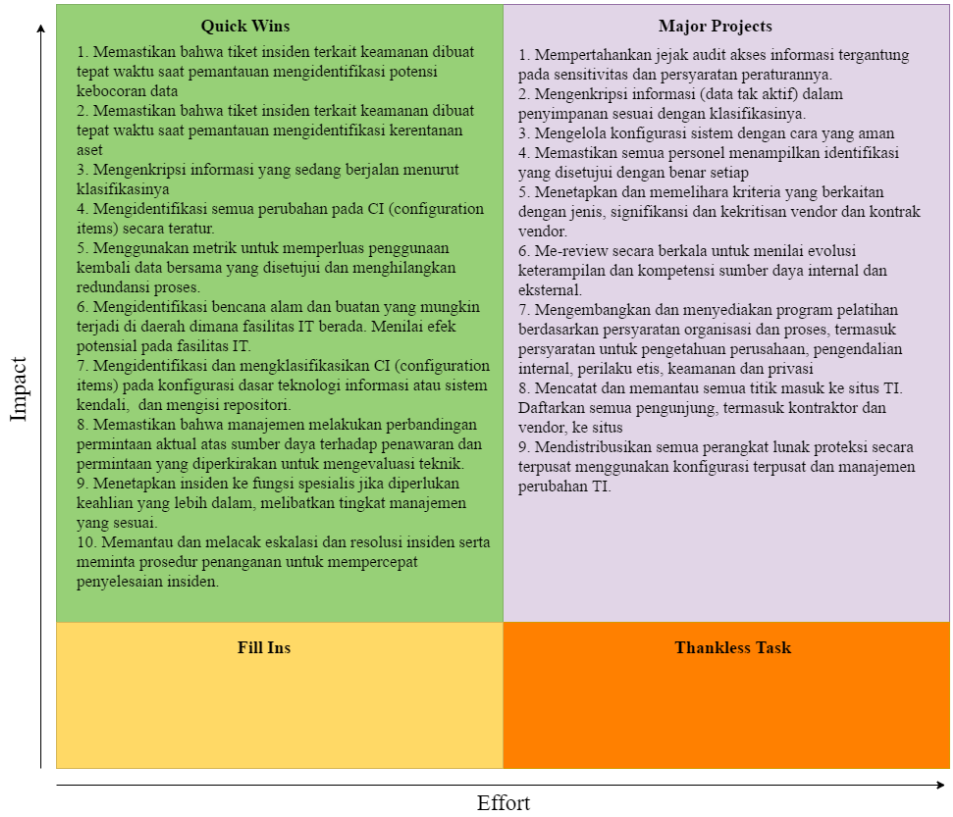
Berdasarkan hasil perhitungan level kapabilitas yang didapatkan dari pengisian kuesioner yang dilakukan oleh pihak Dinas Komunikasi dan Informatika Kota Pontianak dengan menggunakan metode CPM, didapatkan hasil pada kategori DE (*Detect*) yang dapat dilihat pada tabel 5

Tabel 6. Hasil Perhitungan Level Kapabilitas DE (*Detect*)

Kategori	Proses	Level	Jumlah pertanyaan	Ya	Jumlah	Skala	Level Saat Ini	Level yang diharapkan	GAP
Detect (DE)									
DE.AE-1	Garis dasar pengoprasian jaringan dan alur data yang diharapkan untuk penggunaan dan sistem ditetapkan dan dikelola.	2	1	1	100%	Fully	2	2	0
DE.CM-4	Kode berbahaya dideteksi	2	2	2	100%	Fully	4	3	1
		3	1	0	0%	Not			
		4	1	1	100%	Fully			
DE.CM-7	Pemantauan personil, koneksi, perangkat, dan perangkat lunak tak berizin dilakukan.	2	5	4	80%	Largely	4	4	0
		3	3	3	100%	Fully			
		4	1	1	100%	Fully			
DE.CM-8	Pemindaian kerentanan dilakukan.	2	3	3	100%	Fully	3	3	0

4.5. Rekomendasi Perbaikan

Untuk aktivitas yang masih belum, diberikan rekomendasi perbaikan agar level kapabilitas keamanan siber pada Dinas Komunikasi dan Informatika Kota Pontianak mencapai level yang diharapkan. Aktivitas rekomendasi perbaikan tersebut kemudian dipetakan ke action priority matrix untuk mengetahui aktivitas mana yang harus dikerjakan terlebih dahulu. Rekomendasi perbaikan tersebut dapat dilihat pada gambar 3.



Gambar 3. Action Priority Matrix Rekomendasi Perbaikan

5. KESIMPULAN

Audit keamanan siber dapat dilakukan dengan menggabungkan dua atau lebih dari *framework* yang tersedia, seperti penggabungan CIS CSC, NIST CSF, dan COBIT 2019. CIS CSC dapat digunakan untuk memetakan proses berdasarkan aset karena setiap kontrol pada CIS CSC terdapat keterangan tipe aset yang termasuk ke dalam kontrol tersebut. NIST CSF digunakan bersamaan dengan COBIT 2019. NIST CSF digunakan untuk membatasi aktivitas yang termasuk ke dalam tata kelola teknologi informasi yang mengatur tentang keamanan siber, dan dilanjutkan dengan melakukan perhitungan di COBIT 2019 menggunakan metode yang sudah disediakan oleh COBIT 2019 yaitu CPM (*COBIT Performance Model).*

Dari hasil perhitungan level kapabilitas berdasarkan metode CPM (*COBIT Performance Model)* pada fungsi-fungsi yang terdapat pada *framework core* NIST CSF , *Identify* (ID) mencapai level 3.9, *Protect* (PR) mencapai level 3.4, *Detect* (DE) mencapai level 2.5, dan *Respond* (RS) mencapai level 4.

Terdapat 19 rekomendasi aktivitas untuk dilakukan oleh DISKOMINFO Kota Pontianak 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*, sementara ada kuadran *Fill Ins* dan *Thankless Task* tidak terdapat aktivitas rekomendasi.

Saran untuk penelitian selanjutnya dapat menggunakan sumber informasi yang berbayar untuk mendapatkan informasi yang lebih lengkap dan akurat, menentukan responden kuesioner dengan tepat, kuesioner ditujukan kepada orang yang mengerti bidang penelitian agar jawaban yang diberikan lebih valid, menggunakan *framework* lain yang kompatibel agar dapat menjadi referensi kelanjutan penelitian.

REFERENSI

[1] A. S. Roy, "*Study of Cyber Security Challenges and It's Emerging Trends on Latest Technologies*", 2021.
[2] Profil Dinas Komunikasi dan Informatika Kota Pontianak. Available: diskominfo.pontianak.go.id/tentang/halaman/profil [Terakhir diakses pada 19 Januari 2023]
[3] B. Oana, "*(Cyber) Security Maturity or No (Cyber) Security*", 2021.
[4] R. A. Ashari, "Rencana penerapan cyber-risk management menggunakan NIST CSF dan COBIT 5", 2018.
[5] NIST, "*Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*", 2018.
[6] CIS, "*CIS Critical Security Controls Version 8",* 2021
[7] ISACA, *COBIT 2019 "Framework: Introduction and Methodology"*, 2018
[8] L. R. S. Dhulipalla, ISACA, *"Using COBIT 2019 Performance Management Model to Assess Governance and Management Objectives"* 2019
[9] ISACA, "Implementing the NIST Cybersecurity Framework Using COBIT 2019", Version 1.0.0, 2019.
[10] E Elue, CISA, and CDPSE, "Effective Capability and Maturity Assessment Using COBIT 2019", 2020