Jurnal Ilmu Siber dan Teknologi Digital (JISTED)
ISSN2986-7312 Vol 2, No 1, 2023, 45-60 https://doi.org/10.35912/jisted.v2i1.2945

Evaluasi Tingkat Capability Keamanan Sistem Informasi PT. CPPI Menggunakan Framework COBIT 2019 *(Evaluation of PT's Information System Security Capability Level. CPPI uses the COBIT 2019 framework)*

Suroto Suroto[1*], John Friadi[2]
Universitas Batam, Batam[1,2]
suroto@univbatam.ac.id[1*], john.friadi@univbatam.ac.id[2]

Riwayat Artikel
Diterima pada 1 Februari 2024
Revisi 1 pada 15 Februari 2024
Revisi 2 pada 21 Februari 2024
Revisi 3 pada 26 Februari 2024
Disetujui pada 27 Februari 2024

Abstract
Purpose: This study aims to determine the capability level of information system security in PT. CPPI. In addition, it provides recommendations for enhancing IS security.
Methodology: This study used a qualitative approach. The objective of this study was PT. The CPPI, a company in Batam, operates in the fields of Forwarding, Transportation, and warehousing. The interviews were directed to personnel in the IT department. Framework for evaluation using the COBIT 2019 framework.
Results: The study results show that the capability level value in the APO12 process reaches level 2 with an average value of 67%, which is the fully achieved level. In addition, in the APO13 process, the capability level reached level 2, with a value of 64%. In the DSS05 process, the capability level is at level 2, with a value of 71%. Finally, in the DSS06 process, the capability level was level 3, with a value of 86%.
Limitations: Some management practices and activities from each process domain were not used as questionnaire material. For example, in the APO12 process, only one management practice is revealed, namely APO12.01, Collect Data. Meanwhile, other practices were not disclosed, such as APO12.02 - Analyze Risk, APO12.03 - Maintain a Risk Profile, etc. The author suggests that other research reveals these management practices.
Contribution: This study can help companies increase their level of capability in IT governance, especially in the area of information technology security. Achievement targets for capability levels can be realized according to COBIT 2019 standards.
Keywords: *COBIT 2019, Capability Level, IT Governance, Audit IS*
How to cite: Suroto, S., Friadi, J. (2023). Evaluasi Tingkat Capability Keamanan Sistem Informasi PT. CPPI Menggunakan Framework COBIT 2019. *Jurnal Ilmu Siber dan Teknologi Digital*, 2(1), 45-60.

1. Pendahuluan

Setiap bisnis harus memiliki sistem untuk mengumpulkan, memproses, menyimpan, dan berbagi data. Di masa lalu, tugas-tugas ini memerlukan banyak waktu dan dokumen. Saat ini, perusahaan menggunakan teknologi modern untuk menyederhanakan dan mengotomatiskan operasi ini. Sistem informasi kini memainkan peran penting dalam pemrosesan data dan pengambilan keputusan. Jika digunakan dengan benar, hal ini dapat memberikan dampak positif terhadap kinerja dan pendapatan organisasi secara keseluruhan (Angelina & Fianty, 2024). PT. Citra Pembina Pengangkutan Industri (PT. CPPI) juga telah menggunakan teknologi dan sistem informasi untuk mendukung proses bisnis. Sebagai perusahaan yang bergerak di sektor *logistic, warehousing & forwarding* memiliki beberapa sistem informasi agar operasi perusahaan berjalan secara efektif & efisien. Perusahaan tentu banyak

memiliki data / informasi *crendential*. Data / informasi adalah aset yang sangat penting bagi perusahaan (Baisholan, Kubayev, & Baisholanov, 2021).

Di sisi lain, fakta menunjukkan bahwa risiko pelanggaran data dan kehilangan informasi sangat tinggi bagi perusahaan. Perusahaan harus melindunginya dari peretas dan pencuri data. Oleh karena itu penerapan keamanan informasi menjadi penting. Menurut (irwin, 2021), keamanan informasi adalah praktik mencegah akses, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, pencatatan atau penghancuran yang tidak sah atas catatan sensitif. Penerapan keamanan informasi dalam suatu organisasi dapat melindungi teknologi dan aset informasi yang digunakannya dengan mencegah, mendeteksi, dan merespons ancaman internal dan eksternal. Menurut (owens, 2023), perusahaan harus menetapkan dan menerapkan prosedur pengendalian untuk meminimalkan risiko, dan melakukan evaluasi / audit untuk mengukur kinerja pengendalian. Hal tersebut berguna untuk mendukung strategi keamanan informasi. Pendapat serupa dari (Kostic, 2021), bahwa audit akan memberikan jaminan bahwa keamanan informasi dan manajemen risiko serta manajemen keamanan informasi secara akurat melaksanakan fungsi manajemen risiko. Manajemen risiko dilakukan dengan cara melakukan analisis risiko hingga mengevaluasi risiko (Suroto & Friadi, 2023).

Panduan dan tool untuk membuat sebuah strategi tersebut telah banyak tersedia saat ini. Salah satunya, kerangka kerja COBIT 2019 yang memiliki prinsip dan panduan bagi kita untuk mengukur tingkat kapabilitas manajemen semua proses TI. Beberapa domain proses yang area fokus pada keamanan TI / SI adalah APO12 - Resiko Terkelola (*Managed Risk*), APO13 – Keamanan Terkelola (*Managed Security*), DSS05 – Layanan Keamanan Terkelola (*Managed Security Services)* dan DSS06 – Kontrol Proses Bisnis Terkelola *(Managed Business Process Controls).* Meskipun telah ada kerangka kerja COBIT atau lainnya, PT. CPPI belum mengadopsi kerangka kerja tersebut. Namun bukan berarti keamanan informasi diabaikan oleh perusahaan. Manajemen keamanan informasi di perusahaan belum mengikuti standar atau kerangka kerja yang ada. Disinilah terjadi kesenjangan (gap). Oleh karena itu, penting untuk melakukan evaluasi atau audit terhadap pengelolaan keamanan informasi perusahaan. *Focus area* penelitian ini adalah *IT Security*, dimana domain proses yang terkait yaitu APO12, APO13, DSS05 dan DSS06. Pada penelitian-penilitian pendahulu, belum ada yang menyertakan domain proses DSS06 sebagai sasaran audit / evaluasi. Penelitian ini bertujuan untuk mengetahui tingkat *capability* dari keamanan sistem informasi di PT. CPPI menggunakan kerangka kerja COBIT 2019. Hasil audit yang berupa rekomendasi perbaikan diharapkan dapat meningkatkan efektifitas dalam pengelola keamanan informasi perusahaan.

2. Tinjauan Pustaka

2.1. Penelitian-Penelitian Sebelumnya

Beberapa penelitian tentang keranngka kerja COBIT telah dilakukan. Mutia & Nur'ainy (2020) melakukan penelitian yang bertujuan untuk mengukur *Capability Level* (tingkat kapabilitas) Tata Kelola TI di Perusahaan Minyak & Gas , PT Energi Mega Persada Tbk. Hasilnya ditemukan bahwa pengukuran terhadap tingkat *Capability* (kapabilitas) Tata Kelola TI dari 37 proses TI untuk semua domain di EMP saat ini berada di level 3,3. Peneliti lainnya, Asro (2023) melakukan penelitian di universitas XYZ untuk mengidentifikasi berapa *Capability* (kapabilitas) universitas XYZ dalam mengelola keamanan informasi. Evaluasi dilakukan menggunakan kerangka kerja COBIT 2019 pada domain APO12, APO13 dan DSS05 Hasil evaluasi menunjukkan pengelolaan keamanan informasi di Universitas XYZ masih di tingkat kapabilitas 2 untuk domain APO12, APO13 dan DSS05. Selain itu, telah dihasilkan 17 rekomendasi perbaikan peningkatan implementasi keamanan informasi.

Handayani, Rusmana, and Warsidi (2023) melakukan penelitian dengan judul *Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector*. Hasil pengukuran menunjukkan bahwa subdomain APO12 – Risiko Terkelola, APO13 –Keamanan Terkelola, dan DSS05 – Layanan Keamanan Terkelola memiliki tingkat *Maturity* pada level 2. Aritonang, Udayanti, and Iksan (2018) melakukan penelitian tata kelola TI dengan fokus pada satu domain, APO13 – *managed security*. Hasil dari penelitian ini menunjukkan tingkat *Capability* (kapabilitas) dari proses APO13 yaitu Level 0 (*Incomplete Process*) dengan status L (*Largely Achieved*) yang artinya sudah mencapai sebagian besar pengelolaan keamanan sistem informasi. Level 1 (*Performed Process*) dengan pencapaian level sebesar

50% dengan status P (*partially achieved*) yang artinya keamanan sistem informasi sudah tercapai sebagian. Selanjutnya juga pada Level 2,3 dan 5 yang memperoleh hasil rata -rata diatas 60% dengan status L. Penelitian yang dilakukan (Gusni, Kraugusteeliana, & Pradnyana, 2021) menunjukkan bahwa tingkat *Capability* (kapabilitas) tata kelola TI di RS Bhayangkara Sespima Polri Jakarta ini berada di tingkat 3 (*Defined*). Penilaian penelitian ini mengacu pada proses EDM03, APO12, APO13, APO14 dan DSS05. Penelitian lain dilakukan oleh (Viamianni, Mulyana, & Dewi, 2023). Penelitian menggunakan kerangka kerja COBIT 2019. Fokus pada tiga domain *Information Technology Governance and Management* (ITGM): APO13, DSS05, dan BAI06. Objek penelitiannya adalah sebuah perusahaan asuransi Indonesia. Hasil penelitian menemukan kesenjangan terhadap tujuh komponen *Capability*. Kesenjangan yang teridentifikasi ini yang kemudian menghasilkan rekomendasi perbaikan. Rekomendasi-rekomendasi ini disusun menjadi peta jalan implementasi TI bagi ReinsurCo.

Penelitian Geovaldo, Suarjaya, and Pratama telah dilakukan dengan objek penelitiannya adalah perusahaan daur ulang sampah, PT. Bumi Lestari Bali. Dalam penelitian, proses TI yang didapat adalah EDM04, APO07 dan DSS05. Hasil penelitian menunjukkan bahwa tingkat *Capability* dari proses TI tersebut yaitu *established process* sedangkan target yang diinginkan instansi adalah *predictable process* . Penelitian (Kesuma, Hermadi, & Nurhadryani, 2023) mengambil objek penelitian di dinas pertanian. Penelitian fokus pada domain proses MEA03 (*Managed Compliance with External Requirements*), BAI04 (*Managed Availability and Capacity*) dan EDM03 (*Ensured Risk Optimization*). Hasil penilaian tingkat kapabilitas pada proses MEA03, BAI04 dan EDM03 baru mencapai tingkat *Capability* (Kapabilitas) level 1.

(Christiadi & Sutomo, 2023) melakukan pengukuran tata kelola TI pada sektor Bisnis Indonesia. Penelitian Hasil pengukuran menunjukkan bahwa subdomain APO12, APO13, dan DSS05 memiliki tingkat *Maturity* (kematangan) pada level 2. Hasil ini menunjukkan adanya kesenjangan dalam kebijakan keamanan *end point,* kebijakan akses, dan pengelolaan log peristiwa dalam insiden TI. Djapandjatay, Tanaamah, and Tanaem (2019) melakukan penelitian untuk mengevaluasi kinerja aplikasi Sistem Cuti Elektronik. Penelitian ini menggunakan COBIT 5 sebagai alat ukur dalam melakukan evaluasi dan hanya berfokus pada satu domain yaitu MEA (*Monitor,Evaluate and Assess*). Hasil yang diperoleh yaitu tingkat kematangan subdomain MEA01 3,84, MEA02 3,82 dan MEA03 4.

2.2. Keamanan Informasi

Meskipun keamanan TI dan keamanan informasi terdengar serupa, keduanya mengacu pada jenis keamanan yang berbeda. Keamanan informasi mengacu pada proses dan alat yang dirancang untuk melindungi informasi bisnis sensitif dari invasi, sedangkan keamanan TI mengacu pada pengamanan data digital, melalui keamanan jaringan komputer (cisco, 2021). Keamanan informasi adalah proses untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Keamanan informasi bahkan merupakan bidang studi yang lebih besar termasuk keamanan komputer dan jaringan komputer (Kizza, Kizza, & Wheeler, 2013). Ini melibatkan penciptaan keadaan di mana informasi dan data aman. Dalam model ini, informasi atau data dipindahkan melalui saluran komunikasi atau disimpan dalam database di server.

Pencegahan akses tidak sah ke sumber daya sistem dicapai melalui sejumlah layanan yang mencakup kontrol akses, otentikasi, kerahasiaan, integritas, dan non-penyangkalan. Pendekatan perlindungan data / informasi meliputi penggunaan enkripsi data, akses yang terkendali, pengelolaan hak akses pengguna yang baik, kebijakan keamanan yang ketat, dan penerapan teknologi keamanan seperti firewall dan sistem deteksi intrusi. Selain itu, backup dan pemulihan data yang teratur juga merupakan bagian penting dari perlindungan data.

2.3. COBIT 2019

COBIT (*Control Objectives for Information and Related Technologies*) adalah kerangka kerja yang memberikan layanan berupa prosedur tata kelola teknologi informasi (TI) kepada perusahaan sebagai support dalam mencapai tujuan perusahaan itu sendiri (ISACA, 2018). COBIT membantu perusahaan dalam menerapkan tata kelola teknologi informasi secara menyeluruh dan menjadi jembatan antara kepentingan pimpinan bisnis dengan permasalahan teknis TI. Sederhananya, COBIT menyampaikan

prosedur tata kelola teknologi informasi secara sederhana dan sistematis kepada pimpinan perusahaan agar lebih mudah dipahami. Penggunaan COBIT 2019 dalam perencanaan strategis untuk mencapai suatu tujuan adalah efektif, dan penggunaan tindakan taktis untuk menerapkan strategi adalah hal terpenting dalam operasi perusahaan (Christopher Anoruo & CGEIT, 2019).

COBIT 2019 adalah generasi ke-6 dari COBIT, yang mulai dikembangkan oleh IT Governance Institute, salah satu bagian dari Information Systems Audit and Control Association (ISACA) pada tahun 1996. Selain menawarkan standar operasional prosedur dalam tata kelola IT, produk ini juga berisikan serangkaian best practice tata kelola IT yang dapat membantu berbagai pemangku kepentingan dalam perusahaan, mulai dari pengguna, auditor, hingga manajemen memecahkan masalah serupa. COBIT menjadi penting karena penerapan teknologi informasi di perusahaan membutuhkan biaya yang besar dan risiko kegagalan yang juga besar. Untuk memaksimalkan implementasinya, dibutuhkan pemahaman konsep dasar teknologi tersebut di tingkat pimpinan perusahaan.

COBIT 2019 mendefinisikan komponen-komponen untuk membangun dan mempertahankan sistem tata kelola dengan tujuh komponen yang sebelumnya disebut "enabler" dalam COBIT 5. Komponen tata kelola dalam COBIT 2019, yaitu: (1) Processes; (2) Organizational Structures; (3) Policies & Procedures; (4) Information Flows; (5) Culture, Ethics & Behaviours; (6) Skills, People & Competencies; (7) Service, Infrastructure and Application

2.4. Mengukur IT Maturity dengan COBIT® 2019

COBIT® 2019 *Framework: Governance and Management Objectives* menggambarkan Capability Level (tingkat kapabilitas) yang diharapkan. Dengan skala 0 hingga 5, skema kapabilitas proses berbasis *Capability Maturity Model Integration*® (CMMI) didukung oleh COBIT® 2019. Dari skor yang diperoleh, dimungkinkan untuk menentukan tingkat kematangan dari 231 praktik dan 40 tujuan yang diselenggarakan di lima domain dalam kerangka COBIT® 2019. Domain pertama, EDM - *Evaluate, Direct and Monitor*. Domain EDM bertanggung jawab atas pembuatan dan pengawasan kebijakan, serta memastikan bahwa tujuan organisasi tercapai melalui penggunaan teknologi informasi yang tepat. Domain ini berfokus pada tugas-tugas seperti pengawasan internal, manajemen risiko, dan pengukuran kinerja.

Domain kedua, APO - *Align, Plan and Organize*. Domain Align berfokus pada keterkaitan strategi bisnis dengan tujuan dan tindakan teknologi informasi. Menjamin keselarasan antara teknologi informasi dengan strategi bisnis. Domain Plan berisi tentang perencanaan dan strategi dalam mengelola sumber daya teknologi informasi. Organisasi harus menentukan tujuan jangka panjang dan jangka pendek, serta merencanakan tindakan yang diperlukan untuk mencapainya. Domain Organize fokus pada tata kelola sumber daya manusia dan struktur organisasi teknologi informasi. Domain ketiga, BAI - *Build, Acquire and Implement*. Domain ini membahas definisi, akuisisi dan implementasi solusi I&T dan integrasinya ke dalam proses bisnis. Domain keempat, DSS - *Deliver, Service and Support*. Menangani penyampaian operasional dan dukungan layanan I&T, termasuk keamanan. Domain kelima, MEA - *Monitor, Evaluate and Assess*. Mengatasi pemantauan kinerja dan kesesuaian I&T dengan target kinerja internal, tujuan pengendalian internal, dan persyaratan eksternal.

2.4.1. Tingkat kapabilitas CMMI

CMMI juga memiliki tingkat kapabilitas yang digunakan untuk menilai kinerja organisasi dan peningkatan proses sebagaimana diterapkan pada bidang praktik individu yang diuraikan dalam model CMMI. Hal ini dapat membantu menghadirkan struktur pada proses dan peningkatan kinerja dan setiap tingkat dibangun berdasarkan tingkat terakhir, serupa dengan tingkat kematangan dalam menilai suatu organisasi.

Aktivitas proses dapat beroperasi pada berbagai tingkat kapabilitas dan kematangan, mulai dari 0 hingga 5. (Elue, 2020). Tingkat kapabilitas adalah ukuran seberapa baik suatu proses diterapkan dan dijalankan (tabel 1), sedangkan tingkat kematangan, yang dikaitkan dengan area fokus, adalah ukuran bagaimana proses-proses yang terdapat dalam area fokus mencapai tingkat kapabilitas tertentu, melalui kumpulan bukti mendasar yang substansial untuk mendukung tujuan perusahaan (tabel 2).

Tabel 1. *Capability Level for Processes* (Tingkat kapabilitas untuk Proses-Proses)

Level	Deskripsi
0	Kurangnya kapabilitas dasar apa pun. Pendekatan yang tidak lengkap untuk mencapai tujuan tata kelola dan pengelolaan. Mungkin tidak memenuhi maksud dari praktik proses apa pun
1	Proses tersebut kurang lebih mencapai tujuannya melalui penerapan serangkaian aktivitas yang tidak lengkap yang dapat dikategorikan sebagai aktivitas awal atau intuitif—tidak terlalu terorganisir.
2	Proses mencapai tujuannya melalui penerapan serangkaian aktivitas dasar namun lengkap yang dapat dicirikan sebagai telah dilakukan.
3	Proses mencapai tujuannya dengan cara yang lebih terorganisir dengan menggunakan aset organisasi. Proses biasanya didefinisikan dengan baik.
4	Proses mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya diukur (secara kuantitatif).
5	Proses mencapai tujuannya, didefinisikan dengan baik, kinerjanya diukur untuk meningkatkan kinerja dan perbaikan berkelanjutan diupayakan.

Sumber: COBIT® 2019 *Framework: Governance And Management Objectives*

Tabel 2. *Maturity Level* for Focus Area (Tingkat Kematangan untuk Area Fokus)

Level	Status	Deskripsi
0	*Incomplete*	Pekerjaan mungkin selesai atau tidak untuk mencapai tujuan tata kelola dan tujuan pengelolaan di area fokus
1	*Initial*	Pekerjaan telah selesai, namun tujuan dan maksud keseluruhan dari area fokus belum tercapai.
2	*Managed*	Perencanaan dan pengukuran kinerja berlangsung, meskipun belum terstandarisasi.
3	*Define*	Standar perusahaan memberikan panduan di seluruh perusahaan.
4	*Quantitative*	Perusahaan ini berbasis data, dengan peningkatan kinerja kuantitatif.
5	*Optimizing*	Perusahaan berfokus pada perbaikan berkelanjutan.

Sumber: COBIT® 2019 *Framework: Governance And Management Objectives*

3. Metodologi penelitian

Objek penelitian ini adalah PT. Citra Pembina Pengangkutan Industries (CPPI). Sebuah perusahaan logistik & forwarding, yang berlokasi di Jl. Mas Suryanegara, Kav A9, Kawasan industri terpadu Kabil, Batam. Lebih khusus lagi, departemen yang menjadi objek adalah departemen TI.

Penelitian ini menggunakan metode kualitatif, dimana riset memberikan penjelasan berupa analisis yang sifatnya subjektif. Metode penelitian ini menggunakan sudut pandang partisipan yang merupakan gambaran prioritas dalam memperoleh hasil penelitian yang sesuai.

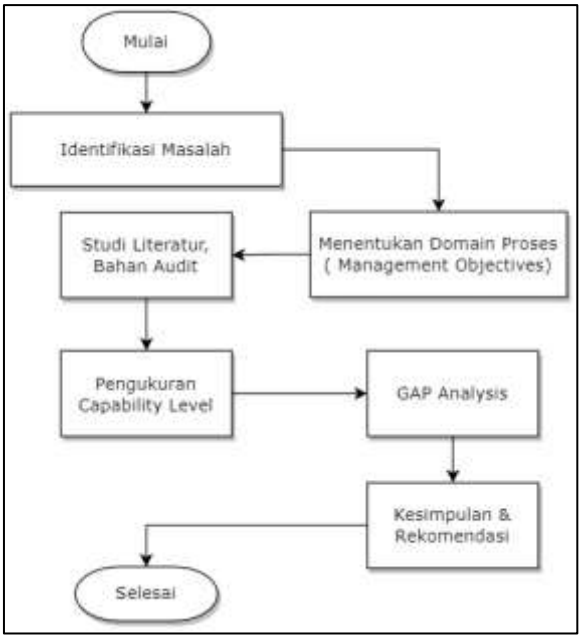
Dalam metode kualitatif ini, penelitian menggunakan teknik pengumpulan data berupa kuisioner. Kuisioner ditujukan ke personal di departemen TI. Daftar partisipan disajikan dalam tabel 3 berikut.

Tabel 3. Daftar Partisipan Kuisioner

No	Nama	Jabatan	Role
1	Heri Samuel	IT Manager	DSS06
2	Aswin	Network Administrator	APO12, APO13, DSS05

Sumber: Data Penelitian

Kerangka kerja penelitian ini mengikuti panduan & prinsip yang ada di COBIT 2019 *Introduction and Methodology*. Adapun kerangka kerja penelitian tersebut dapat dilihat pada gambar 1.



Gambar 1. Kerangka Kerja Penelitian
Sumber: Data Penelitian

Langkah-langkah penelitian, seperti disajikan dalam gambar 1, adalah sebagai berikut;

- Langkah pertama adalah melakukan diskusi yang membahas tentang pemahaman konteks dan strategi perusahaan, serta identifikasi permasalahan (*focus area*) yang ada di perusahaan. Permasalahan yang terjadi adalah pernah terjadi sistem aplikasi down dan proses recovery membutuhkan waktu lama.
- Langkah kedua, adalah untuk menentukan domain proses yang ada di perusahaan. Memilih domain proses atau *management objectives* yang sesuai dengan *focus area*, yaitu *IT Security*. Selain itu, menetapkan / memilih target *Capability Level*, (daftar pilihan tersedia di tabel 1 di atas).
- Langkah ketiga, setelah mengetahui domain proses apa saja yang dibutuhkan di dalam penelitian untuk mengukur tingkat Keamanan IT di perusahaan, maka perlu pengumpulan data-data terkait. Data-data diperoleh dari partisipan / koresponden. Tahap mengumpulkan data dengan cara studi literatur dari buku-buku dan jurnal terkait masalah keamanan TI. Ini digunakan sebagai sumber referensi dan bahan pertanyaan audit / evaluasi.
- Langkah keempat, pengukuran Capability Level oleh partisipan, dalam hal ini personal departemen TI yang mempunyai peran untuk mengevaluasi atau menilai tujuan dalam dokumen audit. Hasil penilaian akan digunakan untuk mengukur tingkat kapabilitas (*Capability Level*). Dalam COBIT 2019 *Framework*, peneliti menggunakan skala rating untuk mengukur tingkat kapabilitas.
- Selanjutnya, langkah kelima adalah menganalisis kesenjangan (GAP *Analysis*) antara tingkat kapabilitas saat ini dengan tingkat kapabilitas target. Menghitung prosentase keberhasilan dengan menggunakan rumus CK sebagai berikut:

$$CK = \frac{S}{ST} \times 100\%$$

CK ; Capaian kapabilitas (dalam prosen)
S ; Banyaknya aktivitas yang dilaksanakan
ST ; Banyaknya aktivitas sesuai persyaratan yang telah ditetapkan

Menurut (Neto, Almeida, & Silva, 2019), pada bagian 7.2.4.1 COBIT 2019 *Design Guide* menjelaskan kaitan skor CK dengan tingkat kapabilitas, seperti disajikan dalam table 4 berikut:

Tabel 4. Hubungan Capaian Kapabilitas dan Tingkat Kapabilitas

Skor Capaian Kapabilitas	Capability Level
>= 75%	4
>= 50% dan < 75%	3
>= 25% dan < 50%	2
<25%	1

Sumber: Data Penelitian

- Langkah terakhir, berdasarkan evaluasi tersebut dan setelah ada temuan (*finding*) audit, maka kesimpulan dapat diambil dan rekomendasi diberikan. Rekomendasi tersebut berguna untuk mengatasi dan memecahkan permasalahan serta meningkatkan tingkat kapabilitas.

4. Hasil dan pembahasan

Penelitian ini berfokus pada area keamanan TI. *Focus Area* (Area Fokus) dalam Kerangka COBIT 2019 adalah topik tata kelola spesifik, domain, atau isu yang dapat diatasi melalui kumpulan tujuan tata kelola dan manajemen serta komponennya. Area-area ini memberikan pendekatan terstruktur untuk mengelola dan meningkatkan infrastruktur informasi dan teknologi dalam suatu organisasi. Penelitian diawali dengan review dokumen kebijakan, prosedur dan instruksi kerja di departemen TI. Ini meliputi prosedur backup data, pengelolaan ruang server, pengembangan perangkat lunak aplikasi atau sistem informasi, kontrol akses pengguna, *password policy*.

Selanjutnya untuk penentuan domain proses atau *Management Objectives*, dimulai dengan review faktor desain (*design factor*) COBIT 2019. Pemilihan domain proses dengan menggunakan perangkat faktor desain menghasilkan 4 domain proses (*Management Objectives*) yaitu APO12 (*Managed Risk*), APO13 (*Managed Security*), DSS05 (*Managed Security Services*) dan DSS06 (*Managed Business Process Controls*). Domain-domain ini terkait keamanan informasi. Ini sesuai panduan pada Toolkit COBIT 2019 *Governance management Objectives Practices*. Kemudian, penetapan target tingkat capability. Disini, perusahaan menetapkan target tingkat *Capability* untuk domain terpilih, seperti disajikan dalam tabel 5 berikut.

Tabel 5. Penetapan Target *Capability Level*

Domain	Target Capability Level
APO12	3
APO13	3
DSS05	3
DSS06	4

Sumber: Data Penelitian

Level 3, artinya bahwa Proses mencapai tujuannya dengan cara yang lebih terorganisir dengan menggunakan aset organisasi. Proses biasanya didefinisikan dengan baik. (lihat tabel 1)
Level 4, artinya bahwa Proses mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya diukur secara kuantitatif. (lihat tabel 1)

Langkah selanjutnya adalah menyiapkan bahan evaluasi, atau kuisioner untuk partisipan yang bertugas & berwenang dalam keamanan informasi perusahaan. Kuisioner menggunakan pernyataan persyaratan yang terdapat di buku COBIT 2019 *Governance and Management Objectives*. Tabel 6 di bawah ini tercantum praktik yang terkait dengan masing-masing tujuan tata kelola dan manajemen di COBIT® 2019.

Domain	Objective ID	Objective Name	Objective Description	Practice Name	Practice Description
Align, Plan and Organize (APO)	APO12	*Managed Risk*	Secara terus-menerus mengidentifikasi, menilai dan mengurangi risiko terkait TI, dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.	Mengumpulkan data	Identifikasi dan kumpulkan data yang relevan untuk memungkinkan identifikasi, analisis, dan pelaporan risiko terkait I&T yang efektif.
	APO13	*Managed Security*	Mendefinisikan, mengoperasikan dan memantau sistem manajemen keamanan informasi (SMKI).	1. Membangun dan memelihara Sistem Manajemen Keamanan Informasi (SMKI).	Membangun dan memelihara Sistem Manajemen Keamanan Informasi (SMKI) yang memberikan pendekatan standar, formal dan berkelanjutan terhadap manajemen keamanan dan privasi informasi. Pastikan sistem mendukung teknologi aman dan proses bisnis yang selaras dengan kebutuhan bisnis, keamanan perusahaan, dan manajemen privasi perusahaan.
				2. Tentukan dan kelola rencana penanganan risiko keamanan informasi dan privasi	Memelihara rencana keamanan informasi yang menjelaskan bagaimana risiko keamanan informasi dikelola dan diselaraskan dengan strategi perusahaan dan arsitektur perusahaan. Memastikan bahwa rekomendasi untuk penerapan peningkatan keamanan didasarkan pada kasus bisnis yang disetujui, diterapkan sebagai bagian integral dari pengembangan

					layanan dan solusi, dan dioperasikan sebagai bagian integral dari operasi bisnis
Deliver, Service and Support (DSS)	DSS05	*Managed Security Services*	Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan dan privasi. Menetapkan dan memelihara peran keamanan informasi dan privasi serta hak akses. Lakukan pemantauan keamanan.	Melindungi dari malicious software (perangkat lunak berbahaya) .	Menerapkan dan memelihara tindakan preventif, detektif, dan korektif (terutama patch keamanan terkini dan pengendalian virus) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak berbahaya (misalnya malware, ransomware, virus, worm, spyware, spam).
	DSS06	*Managed Business Process Controls*	Mendefinisikan dan memelihara pengendalian proses bisnis yang tepat untuk memastikan bahwa informasi yang terkait dan diproses oleh proses bisnis internal atau outsourcing memenuhi semua persyaratan pengendalian informasi yang relevan. Identifikasi persyaratan pengendalian informasi yang relevan. Mengelola dan mengoperasikan kontrol input, throughput dan output yang memadai (kontrol aplikasi) untuk memastikan bahwa informasi dan pemrosesan informasi memenuhi persyaratan ini	Kelola peran, tanggung jawab, hak akses, dan tingkat otoritas otoritas.	Kelola peran bisnis, tanggung jawab, tingkat wewenang dan pemisahan tugas yang diperlukan untuk mendukung tujuan proses bisnis. Otorisasi akses ke semua aset informasi yang terkait dengan proses informasi bisnis, termasuk aset yang berada di bawah pengawasan bisnis, TI, dan pihak ketiga. Hal ini memastikan bahwa bisnis mengetahui lokasi data dan siapa yang menangani data atas nama bisnis tersebut

Sumber: COBIT® 2019 *Framework: Governance And Management Objectives*

Berikutnya hasil evaluasi terhadap domain terkait.

Tabel 7. Hasil Kuisioner Domain Proses APO12

No	Pernyataan	Ya / Tidak
1	Menetapkan dan terus menjalankan metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko TI	Y
2	Rekam data terkait risiko TI yang relevan dan signifikan di lingkungan operasi internal dan eksternal	Y
3	Menginventarisasi proses bisnis dan mencatat ketergantungannya pada proses manajemen layanan TI dan sumber daya infrastruktur TI. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan outsourcing	Y
4	Menentukan dan menyepakati layanan TI dan sumber daya infrastruktur TI mana yang penting untuk mempertahankan pengoperasian proses bisnis. Menganalisis dependensi dan mengidentifikasi link yang lemah.	T
5	Identifikasi skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional	T
6	Menjaga pencatatan aktivitas pengendalian yang ada untuk memitigasi risiko dan yang memungkinkan pengambilan risiko sejalan dengan resiko yang bisa diterima dan ditoleransi risiko. Mengklasifikasikan aktivitas kontrol dan memetakannya ke skenario risiko TI tertentu dan penyatuan skenario risiko TI.	Y

Sumber: Data Penelitian

Dari hasil kuisioner diketahui bahwa dari 6 kegiatan yang dipersyaratkan oleh COBIT 2019, ada 4 kegiatan yang sudah diimplementasikan. Dengan demikian, capaian tingkat *Capability* dapat dihitung dengan rumus seperti yang telah dijelaskan di bagian Metode Penelitian.;

$$CK = \frac{S}{ST} \times 100\%$$

$$CK = \frac{4}{6} \times 100\%$$

$$= 67\%$$

Jadi, prosentase capaian tingkat Capability pada domain APO12 adalah 67% atau setara capability level 3. (lihat tabel 4 di atas). Ini artinya bahwa sebagian besar praktik aktivitas yang terkait manajemen risiko dilaksanakan oleh perusahaan. Di perusahaan ini, upaya pengendalian resiko belum maksimal untuk mengidentifikasi resiko TI apa saja yang mungkin terjadi. Resiko yang disebabkan oleh faktor manusia, alam, perangkat sistem. Identifikasi skenario risiko berdasarkan kategori, lini bisnis, dan area fungsional belum dilaksanakan.

Selanjutnya, perhitungan capaian pada proses APO13. Sesuai persyaratan COBIT 2019, pada proses APO13 ada 14 aktivitas yang semestinya dikerjakan. Hasil kuisioner disajikan pada tabel 8.

Tabel 8. Hasil Kuisioner Domain Proses APO13

No	Pernyataan	Ya / Tidak
1	Menetapkan ruang lingkup dan batasan sistem manajemen keamanan informasi (ISMS) dalam kaitannya dengan karakteristik perusahaan, organisasi, lokasi, aset, dan teknologinya. Sertakan detail, dan justifikasi untuk setiap pengecualian dari cakupan	Y
2	Menetapkan ISMS sesuai dengan kebijakan perusahaan dan konteks dimana perusahaan beroperasi	Y
3	Selaraskan ISMS dengan pendekatan perusahaan secara keseluruhan untuk pengelolaan keamanan	Y

4	Mendapatkan otorisasi manajemen untuk menerapkan dan mengoperasikan atau mengubah SMKI.	Y
5	Menyiapkan dan memelihara pernyataan penerapan yang menggambarkan ruang lingkup SMKI	T
6	Menetapkan dan mengomunikasikan peran dan tanggung jawab manajemen keamanan informasi.	Y
7	Komunikasikan pendekatan ISMS	T
8	Merumuskan dan memelihara rencana penanganan risiko keamanan informasi yang selaras dengan tujuan strategis dan arsitektur perusahaan. Pastikan bahwa rencana tersebut mengidentifikasi praktik manajemen dan solusi keamanan yang tepat dan optimal, dengan sumber daya terkait, tanggung jawab dan prioritas untuk mengelola risiko keamanan informasi yang teridentifikasi	Y
9	Sebagai bagian dari arsitektur perusahaan, pertahankan inventaris komponen solusi yang ada untuk mengelola risiko terkait keamanan	T
10	Mengembangkan proposal untuk menerapkan rencana penanganan risiko keamanan informasi, didukung oleh kasus bisnis yang sesuai yang mencakup pertimbangan pendanaan dan alokasi peran dan tanggung jawab	T
11	Memberikan masukan terhadap desain dan pengembangan praktik manajemen dan solusi yang dipilih dari rencana penanganan risiko keamanan informasi.	T
12	Melaksanakan program pelatihan dan kesadaran keamanan informasi dan privasi.	Y
13	Mengintegrasikan perencanaan, desain, penerapan dan pemantauan prosedur keamanan informasi dan privasi serta pengendalian lainnya yang mampu memungkinkan pencegahan yang cepat, deteksi peristiwa keamanan, dan respons terhadap insiden keamanan.	Y
14	Tentukan bagaimana mengukur efektivitas praktik pengelolaan yang dipilih. Tentukan bagaimana pengukuran ini digunakan untuk menilai efektivitas guna menghasilkan hasil yang sebanding dan dapat direproduksi	Y

Sumber: Data Penelitian

Dari table 8 di atas, diketahui ada 9 aktivitas diantara 14 aktivitas yang dilakukan oleh perusahaan. Sehingga prosentase capaian tingkat Capability adalah :

$$CK = \frac{9}{14} \times 100\%$$

$$= 64\%$$

Jadi, prosentase capaian tingkat Capability pada domain APO13 adalah 64% atau setara *capability level* 3. (lihat tabel 4 di atas). Ini artinya bahwa sebagian besar praktik aktivitas yang terkait manajemen *security* dilaksanakan oleh perusahaan.

Selanjutnya, perhitungan capaian pada proses DSS05. Sesuai persyaratan COBIT 2019, pada proses DSS05 ada 14 aktivitas yang semestinya dikerjakan. Hasil kuisioner disajikan pada tabel 9.

Tabel 9. Hasil Kuisioner Domain Proses DSS05

No	Pernyataan	Ya / Tidak
1	Instal dan aktifkan alat perlindungan perangkat lunak berbahaya di semua fasilitas pemrosesan, dengan file definisi perangkat lunak berbahaya yang diperbarui sesuai kebutuhan (secara otomatis atau	Y

	semi-otomatis).	
2	Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (misalnya, spyware, email phishing).	Y
3	Mengkomunikasikan kesadaran perangkat lunak berbahaya dan menegakkan prosedur dan tanggung jawab pencegahan. Melakukan pelatihan berkala tentang malware dalam penggunaan email dan Internet. Latih pengguna untuk tidak membuka, namun melaporkan, email yang mencurigakan dan tidak menginstal perangkat lunak yang dibagikan atau tidak disetujui.	Y
4	Mendistribusikan semua perangkat lunak perlindungan secara terpusat (versi dan tingkat patch) menggunakan konfigurasi terpusat dan manajemen perubahan TI.	T
5	Secara berkala meninjau dan mengevaluasi informasi mengenai potensi ancaman baru (misalnya, meninjau saran keamanan produk dan layanan vendor	Y
6	Hanya mengizinkan perangkat resmi yang memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasikan perangkat ini untuk memaksa entri kata sandi.	Y
7	Menerapkan mekanisme penyaringan jaringan, seperti firewall dan perangkat lunak pendeteksi intrusi. Menerapkan kebijakan yang tepat untuk mengendalikan lalu lintas masuk dan keluar.	Y
8	Terapkan protokol keamanan yang disetujui untuk konektivitas jaringan.	Y
9	Konfigurasikan peralatan jaringan dengan cara yang aman.	Y
10	Mengenkripsi informasi dalam perjalanan menurut klasifikasinya	Y
11	Berdasarkan penilaian risiko dan kebutuhan bisnis, menetapkan dan memelihara kebijakan keamanan konektivitas	T
12	Membangun mekanisme yang terpercaya untuk mendukung transmisi dan penerimaan informasi yang aman.	Y
13	Melakukan pengujian penetrasi secara berkala untuk mengetahui kecukupan proteksi jaringan.	T
14	Melakukan pengujian keamanan sistem secara berkala untuk mengetahui kecukupan proteksi sistem	T

Sumber: Data Penelitian

Dari table 9 di atas, diketahui ada 10 aktivitas diantara 14 aktivitas yang dilakukan oleh perusahaan. Sehingga prosentase capaian tingkat *Capability* adalah :

$$CK = \frac{10}{14} \times 100\%$$

$$= 71\%$$

Jadi, prosentase capaian tingkat Capability pada domain DSS05 adalah 71% atau setara capability level 3. (lihat tabel 4 di atas). Ini artinya bahwa sebagian besar praktik aktivitas yang terkait manajemen *security services* dilaksanakan oleh perusahaan. Selanjutnya, perhitungan capaian pada proses DSS06. Sesuai persyaratan COBIT 2019, pada proses DSS06 ada 7 aktivitas yang semestinya dikerjakan. Hasil kuisioner disajikan pada tabel 10.

Tabel 10. Hasil Kuisioner Domain Proses DSS06

No	Pernyataan	Ya / Tidak
1	Mengalokasikan peran dan tanggung jawab berdasarkan uraian tugas dan aktivitas proses bisnis yang telah disetujui.	Y
2	Mengalokasikan tingkat wewenang untuk menyetujui transaksi,	Y

	batasan transaksi, dan keputusan lain apa pun yang berkaitan dengan proses bisnis, berdasarkan peran pekerjaan yang disetujui.	
3	Mengalokasikan peran untuk aktivitas sensitif sehingga terdapat pemisahan tugas yang jelas	Y
4	Mengalokasikan hak akses dan hak istimewa berdasarkan jumlah minimum yang diperlukan untuk melakukan aktivitas pekerjaan, berdasarkan peran pekerjaan yang telah ditentukan sebelumnya. Hapus atau revisi hak akses segera jika peran pekerjaan berubah atau anggota staf meninggalkan area proses bisnis.	Y
5	Secara berkala memberikan kesadaran dan pelatihan mengenai peran dan tanggung jawab sehingga setiap orang memahami tanggung jawabnya; pentingnya pengendalian; dan keamanan, integritas, kerahasiaan dan privasi informasi perusahaan dalam segala bentuknya.	T
6	Memastikan hak administratif diamankan, dilacak dan dikendalikan secara memadai dan efektif untuk mencegah penyalahgunaan	Y
7	Tinjau secara berkala definisi kontrol akses, log dan laporan pengecualian. Pastikan semua hak akses valid dan selaras dengan anggota staf saat ini dan peran yang dialokasikan kepada mereka	T

Sumber: Data Penelitian

Dari table 10 di atas, diketahui ada 5 aktivitas diantara 7 aktivitas yang dilakukan oleh perusahaan. Sehingga prosentase capaian tingkat *Capability* adalah :

$$CK = \frac{5}{7} \times 100\%$$

$$= 71\ \%$$

Jadi, prosentase capaian tingkat *Capability* pada domain DSS06 adalah 71% atau setara *capability level* 3. (lihat tabel 4 di atas). Ini artinya bahwa sebagian besar praktik aktifitas yang terkait manajemen *Business Process Controls* dilaksanakan oleh perusahaan. Berdasarkan perhitungan capaian *Capability* untuk empat domain proses tersebut, kita dapat bandingkan dengan level targetnya (lihat tabel 5 di atas). Sehingga dapat diketahui gap. Nilai gap dihitung dari selisih target *capability level* dengan nilai *capability level*. Ringkasan perhitungan disajikan dalam tabel 11.

Tabel 11. Ringkasan Hasil Evaluasi dan Target Level

Domain Process	**Prosentase Capaian Capability**	**Or Capability Level**	**Target Capability Level**	**Gap**
APO12 – *Managed Risk*	67%	3	3	0
APO13 – *Managed Security*	64%	3	3	0
DSS05 - *Managed Security Services*	71 %	3	4	1
DSS06 - *Managed Business Process Controls*	71 %	3	3	0

Sumber: Data Penelitian

Capaian domain proses APO12, APO13 dan DSS06 adalah level 3, dimana ini sesuai target yang telah ditetapkan sebelumnya. Ada satu domain, yaitu DSS05 yang masih belum mencapai target level. Meskipun demikian, kondisi ini lebih baik dari penelitian lain. Misal, (Nisri, 2023), dimana universitas XYZ berada pada level 2, untuk domain APO12 , APO13. Begitu juga, pada objek penelitiannya Riesna, Pujianto, Efendi, Nugroho, and Saputra (2023) di Indonesia Business Sector, berada pada level 2.
Pada tabel 11, terlihat domain DSS05 mengharapkan tingkat kemampuan tertinggi diantara *domain process* lainnya yaitu level 4. Hal ini menunjukkan bahwa DSS05 memerlukan pengukuran lebih lanjut ke level 4 jika kemampuan pada level 3 sudah terpenuhi.

Namun kenyataannya, perusahaan berada pada tingkat Capability 3. Oleh karena itu, rekomendasi perbaikan diperlukan agar perusahaan dapat berada pada tingkat kemampuan yang lebih baik. Selanjutnya, setelah diperoleh temuan dan dampaknya, maka beberapa rekomendasi dapat diberikan kepada perusahaan. Daftar saran / rekomendasi perbaikan disajikan pada tabel 12 berikut.

Tabel 12. Rekomendasi Perbaikan

Objectives / Domain Process	**Rekomendasi Aktivitas**
APO12	1. Siapkan dan pelihara pernyataan penerapan yang menggambarkan ruang lingkup SMKI 2. Komunikasikan pendekatan ISMS
APO13	1. Pertahankan inventaris komponen solusi yang ada untuk mengelola risiko keamanan 2. Kembangkan proposal untuk menerapkan rencana penanganan risiko keamanan informasi. 3. Berikan masukan terhadap desain dan pengembangan praktik manajemen dan solusi yang dipilih dari rencana penanganan risiko keamanan informasi. 4. Tentukan layanan TI dan sumber daya infrastruktur TI mana yang penting untuk mempertahankan pengoperasian proses bisnis. 5. Identifikasi skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional
DSS05	1. Distribusikan semua perangkat lunak perlindungan secara terpusat (versi dan tingkat patch) menggunakan konfigurasi terpusat. 2. Tetapkan dan pelihara kebijakan keamanan Berdasarkan penilaian risiko dan kebutuhan bisnis. 3. Lakukan pengujian penetrasi secara berkala untuk mengetahui kecukupan proteksi jaringan. 4. Lakukan pengujian keamanan sistem secara berkala untuk mengetahui kecukupan proteksi sistem.
DSS06	1. Secara berkala memberikan kesadaran dan pelatihan mengenai peran dan tanggung jawab sehingga setiap orang memahami tanggung jawabnya; pentingnya pengendalian; dan keamanan, integritas, kerahasiaan dan privasi informasi perusahaan dalam segala bentuknya

Sumber: Data Penelitian

5. Kesimpulan

Hasil evaluasi terhadap keamanan TI dengan menggunakan framework COBIT 2019, menunjukkan bahwa nilai tingkat kapabilitas pada proses APO12 mencapai level 3 dengan rata-rata nilai 67% sehingga berada pada level tercapai sepenuhnya. Selain itu, pada proses APO13 tingkat kapabilitas mencapai level 3 dengan nilai sebesar 64%. Kemudian, pada proses DSS05 tingkat kapabilitas berada pada level 3, dengan nilai sebesar 71%. Terakhir, pada proses DSS06 tingkat kapabilitas berada pada level 3, dengan nilai sebesar 71%.

Selain itu, terdapat beberapa temuan pada proses di setiap domain. Bahkan ada gap pada proses DSS05 - *Managed Security Service*. Berdasarkan rata-rata hasil pengukuran subdomain, terdapat rekomendasi perbaikan dan peningkatan level proses yang diukur pada Sektor Bisnis. Rekomendasi diberikan untuk menutup kekurangan tersebut. Perusahaan perlu meninjau (meningkatkan) kebijakan keamanan perangkat endpoint, kebijakan hak akses, dan log peristiwa keamanan diperlukan untuk saran penting dalam rekomendasi peningkatan tingkat sektor bisnis. Studi ini memberikan beberapa implikasi bagi pembuat kebijakan dan manajer perusahaan. Secara keseluruhan, penulis memberikan gambaran komprehensif tentang kumpulan pengetahuan tentang standar, memungkinkan pemahaman yang lebih baik tentang proses manajemen risiko, keamanan TI. Manajer yang tertarik untuk menerapkan standar ini dapat membaca temuan ini untuk lebih memahami implikasi audit keamanan TI serta tingginya

fleksibilitas kerangka kerja COBIT 2019. Secara ringkas, studi ini dapat membantu perusahaan meningkatkan tingkat kapabilitasnya dalam tata kelola TI, khususnya pada area fokus keamanan teknologi informasi

Limitasi dan studi lanjutan

Tidak ada penelitian yang mencakup semua aspek. Begitu juga dengan penelitian ini. Beberapa *management practices* dan *activities* dari setiap domain proses tidak dijadikan bahan kuisioner. Misal pada proses APO12, hanya mengungkap 1 *management practice* saja, yaitu APO12.01 - *Collect Data*. Sedangkan *practices* lainnya tidak diungkap, seperti APO12.02 – *Analyze Risk*, APO12.03 – *Maintain a Risk Profile*, APO12.04 - Articulate Risk, APO12.05 - *Define a risk management action portfolio* dan APO12.06 - *Respond to risk*. Penulis menyarankan ada penelitian lain untuk mengungkapkan *management practices* tersebut.

Ucapan terima kasih

Terima kasih kepada Universitas Batam khususnya Fakultas Teknik untuk membantu dalam perencanaan penelitian. Terima kasih juga kepada pihak perusahaan yang mengizinkan pengukuran menggunakan COBIT 2019.

References

Angelina, A., & Fianty, M. (2024). Capability Level Assessments Of Information Security Controls: An Empirical Analysis Of Practitioners Assessment Capabilities. *G-Tech: Jurnal Teknologi Terapan, 8*(1), 91-103.

Aritonang, I. J., Udayanti, E. D., & Iksan, N. (2018). Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (Apo13). *Itej (Information Technology Engineering Journals), 3*(2), 6-10.

Baisholan, N., Kubayev, K., & Baisholanov, T. (2021). Modern Tools For Information Security Systems. *Известия Нан Рк. Серия Физико-Математическая*(1), 14-18.

Christiadi, R. N., & Sutomo, R. (2023). Measurement Of It Security Governance Capabilities Using Cobit 2019 At Indonesian Business Sector. *G-Tech: Jurnal Teknologi Terapan, 7*(4), 1498-1508.

Christopher Anoruo, C., & Cgeit, C. (2019). Employing Cobit 2019 For Enterprise Governance Strategy.

Cisco. (2021). What Is It Security? Retrieved From Https://Www.Cisco.Com/C/En/Us/Products/Security/What-Is-It-Security.Html

Djapandjatay, J. R., Tanaamah, A. R., & Tanaem, P. F. (2019). Evaluasi Kinerja Sistem Informasi Cuti Elektronik (Sicute) Menggunakan Framework Cobit 5 Pada Badan Kepegawaian, Pendidikan Dan Pelatihan Daerah Kota Salatiga. *Sebatik, 23*(2), 367-373.

Elue, E. (2020). Effective Capability And Maturity Assessment Using Cobit 2019. Retrieved From Https://Www.Isaca.Org/Resources/News-And-Trends/Industry-News/2020/Effective-Capability-And-Maturity-Assessment-Using-Cobit-2019

Geovaldo, I. P. H., Suarjaya, I. M. A. D., & Pratama, I. P. A. E. Evaluasi Keamanan Ti Pada Pt. Bumi Lestari Bali (Ecobali Recycling). *Jurnal Ilmiah Teknologi Dan Komputer, 3*(1), 794-801.

Gusni, R. S. A., Kraugusteeliana, K., & Pradnyana, I. W. W. (2021). *Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan Cobit 2019.* Paper Presented At The Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer Dan Aplikasinya.

Handayani, D., Rusmana, O., & Warsidi, W. (2023). Pengaruh Perkembangan E-Commerce, Modal Usaha, Pengetahuan Kewirausahaan, Dan Penggunaan Sistem Informasi Akuntansi Terhadap Pengambilan Keputusan Berwirausaha. *Jurnal Bisnis Dan Pemasaran Digital, 2*(2), 95-104.

Irwin, L. (2021). 6 Reasons Why Information Security Is Important. Retrieved From Https://Vigilantsoftware.Co.Uk/Blog/The-Importance-Of-Information-Security

Kesuma, I. N. R. W., Hermadi, I., & Nurhadryani, Y. (2023). Evaluasi Tata Kelola Teknologi Informasi Di Dinas Pertanian Gianyar Menggunakan Cobit 2019. *Jurnal Teknologi Informasi Dan Ilmu Komputer, 10*(3), 513-522.

Kizza, J. M., Kizza, W., & Wheeler. (2013). *Guide To Computer Network Security* (Vol. 8): Springer.

Kostic, L. (2021). Cobit Focus Area: Information And Technology Risk—A Model For Internal Audit Analysis. Retrieved From Https://Www.Isaca.Org/Resources/News-And-Trends/Industry-News/2021/Cobit-Focus-Area-Information-And-Technology-Risk-A-Model-For-Internal-Audit-Analysis

Neto, J., Almeida, R., & Silva, M. (2019). Defining Target Capability Levels In Cobit 2019: A Proposal For Refinement. *Universidade Católica De Brasília*.

Nisri, A. (2023). Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019. *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi, 9*(1), 34-41.

Owens, D. (2023). Managing Data Privacy And Information Security With It Audits. Retrieved From Https://Www.Isaca.Org/Resources/News-And-Trends/Industry-News/2023/Managing-Data-Privacy-And-Information-Security-With-It-Audits

Riesna, D. M. R., Pujianto, D. E., Efendi, A. J. I., Nugroho, B. A., & Saputra, D. I. S. (2023). Identifikasi Platform Dan Faktor Sukses Dalam Manajemen Proyek Teknologi Informasi. *Jurnal Teknologi Riset Terapan, 1*(1), 1-9.

Suroto, S., & Friadi, J. (2023). Manajemen Risiko Teknologi Informasi Pada Aplikasi Cms Di Pt. Sarana Citranusa Kabil-Batam Menggunakan Iso31000: 2018. *Jurnal Ilmu Siber Dan Teknologi Digital, 1*(2), 135-148.

Viamianni, A., Mulyana, R., & Dewi, F. (2023). Cobit 2019 Information Security Focus Area Implementation For Reinsurco Digital Transformation. *Jiko (Jurnal Informatika Dan Komputer), 6*(2).