

Audit Tata Kelola Risiko, Keamanan, dan Konfigurasi TI Menggunakan COBIT 2019 pada BUMN infrastruktur di Indonesia

Nur Aeni Hidayah¹, Harli Ramadhoni Wicaksono², Silvia Elga Anggraini³, Devi Dhamayanti⁴, Syarifah Aflia Alkadrie⁵

¹²³⁴⁵Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Tangerang Selatan

E-mail: nur.aeni@uinjkt.ac.id¹, harli.ramadhoni23@mhs.uinjkt.ac.id, silvia.elga23@mhs.uinjkt.ac.id³, devi.dhamayanti23@mhs.uinjkt.ac.id⁴, syarifah.aflialkadrie23@mhs.uinjkt.ac.id⁵

Abstrak. Penelitian ini mengevaluasi capability level tata kelola TI pada sebuah BUMN infrastruktur di Indonesia menggunakan COBIT 2019. Fokus audit diarahkan pada risiko TI, keamanan informasi, dan manajemen konfigurasi melalui Design Factors dan capability assessment pada domain EDM03, APO12, APO13, dan BAI10. Data dikumpulkan melalui observasi, wawancara, kuesioner skala Likert, dan studi dokumen. Hasil menunjukkan nilai aktual EDM03 sebesar 4,06, APO12 sebesar 4,05, APO13 sebesar 4,04, dan BAI10 sebesar 3,96, dengan target Level 5. Capaian tersebut menunjukkan bahwa proses telah dikelola secara kuantitatif, tetapi belum mencapai kondisi optimizing. Gap utama ditemukan pada monitoring risiko, pembaruan Statement of Applicability (SoA), dan konsistensi Configuration Management Database (CMDB). Penelitian ini berkontribusi dengan mengintegrasikan evaluasi risiko, keamanan, dan konfigurasi TI dalam satu asesmen COBIT 2019 berbasis Design Factors pada konteks BUMN infrastruktur. Rekomendasi diarahkan pada penguatan risk review, integrasi risk register dengan ERM, pembaruan SoA, dan penegakan kontrol konfigurasi.

Kata kunci: COBIT 2019, Tata Kelola TI, Risiko TI, Keamanan Informasi, Kapabilitas Proses

Abstract. This study evaluates the IT governance capability level of an Indonesian state-owned infrastructure enterprise using COBIT 2019. The audit focuses on IT risk, information security, and configuration management through Design Factors and capability assessment of EDM03, APO12, APO13, and BAI10. Data were collected through observation, interviews, Likert-scale questionnaires, and document review. The results show actual capability scores of 4.06 for EDM03, 4.05 for APO12, 4.04 for APO13, and 3.96 for BAI10, with Level 5 as the target. These results indicate that the processes are quantitatively managed but not yet optimized. The main gaps concern risk monitoring, Statement of Applicability (SoA) updates, and Configuration Management Database (CMDB) consistency. This study contributes by integrating risk, information security, and configuration analysis in a single COBIT 2019 Design Factors-based assessment for a state-owned

infrastructure context. Recommendations focus on strengthening risk review, integrating IT risk registers with ERM, updating SoA, and enforcing configuration controls.

Keywords: COBIT 2019, IT Governance, IT Risk, Information Security, Process Capability.

1. Pendahuluan

Perkembangan teknologi informasi (TI) dalam beberapa tahun terakhir telah mengubah peran TI secara signifikan, dari sekadar pendukung operasional menjadi instrumen strategis yang berperan dalam meningkatkan daya saing, kualitas layanan, serta efektivitas proses bisnis organisasi [1]. Transformasi digital ini juga terjadi pada sektor konstruksi dan infrastruktur, yang memanfaatkan TI untuk pengelolaan proyek, integrasi data teknik, manajemen keuangan, dan pengambilan keputusan strategis berbasis data [2][3]. Ketergantungan pada sistem digital membuat pengelolaan risiko TI, keamanan informasi, dan konsistensi konfigurasi menjadi aspek yang sangat krusial dalam menjaga keberlangsungan operasional perusahaan.

Kajian literatur menunjukkan bahwa perusahaan telah melakukan penguatan manajemen teknologi melalui tata kelola TI, penggunaan arsitektur sistem modern, dan peningkatan kompetensi SDM TI melalui pelatihan serta sertifikasi [2]. Sementara itu, asesmen kesiapan digital melalui Indonesia Industry 4.0 Readiness Index menekankan perlunya peningkatan pada aspek manajemen, teknologi, dan operasi untuk mencapai kesiapan transformasi digital yang lebih matang [3]. Kondisi tersebut menegaskan bahwa digitalisasi perusahaan infrastruktur tidak hanya bertumpu pada implementasi teknologi, tetapi juga membutuhkan tata kelola TI yang kuat, terutama pada area risiko, keamanan informasi, dan pengendalian konfigurasi.

Sejalan dengan peningkatan intensitas penggunaan TI, risiko terhadap keamanan informasi juga semakin tinggi. Ancaman seperti kebocoran data, serangan siber, gangguan operasional, dan ketidakkonsistenan konfigurasi menjadi hambatan yang sering dialami organisasi yang mengoperasikan layanan berbasis TI [4]. Dalam lingkungan infrastruktur kritis, gangguan pada sistem informasi dapat berdampak pada layanan publik dan kepercayaan pemangku kepentingan, sehingga diperlukan tata kelola keamanan dan pengelolaan risiko yang terstruktur dan terukur [5][6].

COBIT 2019 merupakan salah satu kerangka kerja tata kelola TI yang banyak digunakan untuk memastikan bahwa proses TI selaras dengan tujuan organisasi melalui pengelolaan risiko, keamanan informasi, dan konsistensi proses [7][8]. COBIT 2019 menyediakan struktur evaluasi berbasis governance objectives dan management objectives yang digunakan secara luas di berbagai sektor, termasuk pemerintahan, pendidikan, UMKM, dan layanan publik [9][10][11]. Domain-domain seperti EDM03 (Ensure Risk Optimization), APO12 (Manage Risk), APO13 (Manage Security), dan BAI10 (Manage Configuration) memiliki peran penting dalam menjamin keberlangsungan operasional dan memastikan bahwa sistem TI mendukung tujuan organisasi secara efektif [11][5].

Walaupun penelitian tata kelola TI berbasis COBIT 2019 telah banyak dilakukan pada sektor pendidikan, pemerintahan, kesehatan, dan UMKM [12][10][4], sebagian besar studi masih berfokus pada satu domain tertentu, misalnya keamanan informasi, manajemen risiko, atau evaluasi layanan TI. Studi sebelumnya juga relatif jarang menggabungkan tiga area evaluasi sekaligus, yaitu risiko TI, keamanan informasi, dan manajemen konfigurasi, dalam satu rancangan audit COBIT 2019 pada konteks BUMN infrastruktur. Keterbatasan tersebut penting karena organisasi infrastruktur berskala besar memiliki karakteristik risiko yang berbeda, seperti kompleksitas aset TI, ketergantungan pada layanan kritis, kebutuhan kepatuhan yang tinggi, dan keterlibatan pihak internal maupun eksternal dalam pengelolaan sistem [3][8][13]. Oleh karena itu, penelitian ini mengisi celah tersebut melalui integrasi analisis Design Factors COBIT 2019 dengan capability assessment multi-domain pada EDM03, APO12, APO13, dan BAI10 dalam konteks

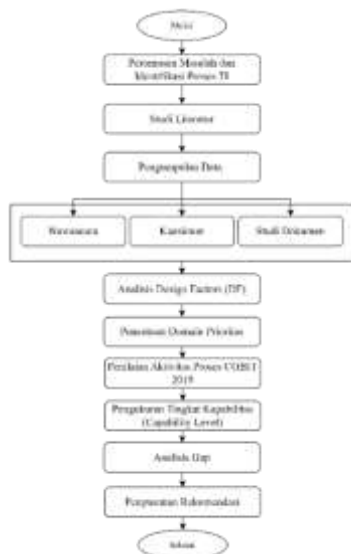
organisasi infrastruktur di Indonesia. Berbeda dengan penelitian sebelumnya yang umumnya mengevaluasi domain secara terpisah, penelitian ini mengintegrasikan analisis risiko, keamanan informasi, dan konfigurasi TI dalam satu evaluasi COBIT 2019 berbasis Design Factors pada konteks BUMN infrastruktur. Penelitian ini memberikan tiga kontribusi utama sebagai berikut.

1. Mengintegrasikan Design Factors COBIT 2019 dengan capability assessment untuk memilih dan menilai domain prioritas secara lebih terarah.
2. Menyajikan evaluasi COBIT 2019 multi-domain yang menghubungkan risiko TI, keamanan informasi, dan manajemen konfigurasi pada organisasi infrastruktur.
3. Merumuskan rekomendasi berbasis gap capability level yang spesifik, aplikatif, dan dapat ditindaklanjuti oleh organisasi sejenis.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk melakukan audit tata kelola TI menggunakan kerangka kerja COBIT 2019 dengan fokus pada domain APO12 (*Manage Risk*), APO13 (*Manage Security*), EDM03 (*Ensure Risk Optimization*), dan BAI10 (*Manage Configuration*). Penelitian ini diharapkan mampu memberikan gambaran *capability level* tata kelola TI organisasi, mengidentifikasi *gap* proses yang masih perlu ditingkatkan, serta menghasilkan rekomendasi strategis yang selaras dengan kebutuhan organisasi dan prinsip tata kelola TI berbasis COBIT 2019

2. Metode

Penelitian ini merupakan penelitian empiris dengan pendekatan deskriptif-evaluatif yang bertujuan untuk mengevaluasi tata kelola Teknologi Informasi (TI) menggunakan framework COBIT 2019. Framework ini digunakan untuk mengidentifikasi karakteristik organisasi melalui analisis *Design Factors* serta mengevaluasi proses tata kelola dan manajemen TI berdasarkan *governance objectives* dan *management objectives* COBIT 2019 [1][7]. Penelitian dilakukan melalui beberapa tahapan, yaitu identifikasi kondisi organisasi, analisis *Design Factors*, penentuan domain prioritas, pengumpulan data, pengukuran *capability level*, analisis gap, dan penyusunan rekomendasi tata kelola TI. Alur penelitian ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian

2.1 Pendekatan Penelitian

Penelitian ini menggunakan pendekatan deskriptif-evaluatif untuk menilai tata kelola Teknologi Informasi (TI) menggunakan kerangka kerja COBIT 2019. Pendekatan ini sejalan dengan metodologi penelitian tata kelola TI yang banyak digunakan pada studi sebelumnya yang menerapkan COBIT 2019

melalui tahapan analisis Design Factors, pemilihan domain prioritas, serta pengukuran tingkat kapabilitas proses TI [13]. Pendekatan ini dipilih karena mampu menggambarkan tingkat kapabilitas TI secara objektif, menilai keselarasan TI dengan tujuan organisasi, dan mengevaluasi risiko, keamanan, dan konfigurasi sistem secara terstruktur [14].

2.2 Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh pihak yang terlibat dalam pengelolaan, pengawasan, dan operasional teknologi informasi pada organisasi. Penentuan domain evaluasi difokuskan pada proses yang berkaitan dengan pengelolaan risiko, keamanan informasi, dan manajemen konfigurasi, yaitu EDM03, APO12, APO13, dan BAI10 [13].

Teknik pengambilan sampel menggunakan purposive sampling, yaitu pemilihan responden berdasarkan keterlibatan, tanggung jawab, dan pemahaman terhadap proses COBIT 2019 yang dievaluasi. Secara keseluruhan, penelitian melibatkan 8 responden yang terdiri atas unsur strategis, manajerial, dan teknis. Namun, penilaian pada setiap domain dilakukan oleh responden yang paling relevan dengan karakter prosesnya. Domain EDM03 dinilai oleh 1 responden strategis, APO12 oleh 3 responden yang berkaitan dengan manajemen risiko, APO13 oleh 3 responden yang berkaitan dengan keamanan informasi, dan BAI10 oleh 6 responden teknis yang berkaitan dengan konfigurasi, aset, sistem, jaringan, dan basis data.

Profil responden mencakup level strategis, pengawasan, keamanan informasi, administrasi sistem, jaringan, basis data, dan konfigurasi. Pemilihan responden didasarkan pada kesesuaian peran, wewenang, tanggung jawab, serta keterlibatan langsung dalam praktik EDM03, APO12, APO13, dan BAI10. Dengan demikian, penelitian ini menekankan kecukupan kompetensi responden dalam audit tata kelola TI, bukan representasi probabilistik seperti pada survei populasi statistik.

2.3 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini meliputi observasi, wawancara, kuesioner, dan studi dokumen. Kombinasi teknik tersebut digunakan untuk memperoleh bukti yang faktual dan memastikan validitas hasil evaluasi tata kelola TI [15].

1. Wawancara digunakan untuk memperoleh informasi mendalam mengenai kebijakan, prosedur, dan aktivitas TI dari pihak yang berwenang.
2. Kuesioner digunakan untuk mengumpulkan data terstruktur terkait penilaian kapabilitas proses sesuai COBIT 2019.
3. Studi dokumen dilakukan untuk menelaah SOP, kebijakan keamanan, laporan insiden, serta dokumen terkait lainnya sebagai bukti pendukung audit TI.

Sebelum digunakan dalam proses pengumpulan data, instrumen kuesioner divalidasi melalui expert judgement oleh pihak yang memahami tata kelola TI dan framework COBIT 2019. Validasi dilakukan untuk memastikan bahwa setiap indikator dan pernyataan sesuai dengan domain COBIT 2019 yang dianalisis serta dapat dipahami oleh responden. Uji reliabilitas statistik, seperti Cronbach Alpha, tidak dilakukan karena jumlah responden terbatas dan kuesioner digunakan sebagai instrumen audit berbasis kompetensi, bukan sebagai instrumen psikometrik berskala besar. Untuk menjaga keandalan hasil, data kuesioner ditriangulasi dengan wawancara, observasi, dan dokumen pendukung.

2.4 Teknik Analisis Data

Analisis data dilakukan melalui beberapa tahapan yang mengacu pada framework COBIT 2019 untuk mengevaluasi tata kelola Teknologi Informasi (TI), khususnya pada aspek risiko, keamanan informasi, dan manajemen konfigurasi. Tahapan analisis dijelaskan sebagai berikut:

1. Analisis *Design Factors* (DF)

Analisis Design Factors dilakukan untuk menilai karakteristik organisasi yang mempengaruhi penentuan prioritas domain COBIT 2019. Sebanyak sebelas faktor desain dianalisis, meliputi Enterprise Strategy, Enterprise Goals, IT Risk Profile, IT-Related Issues, Threat

Landscape, Compliance Requirements, Role of IT, Sourcing Model, IT Implementation Methods, Technology Adoption Strategy, dan Organizational Size.

Setiap faktor memberikan kontribusi terhadap identifikasi area tata kelola TI yang paling relevan dan berpengaruh bagi perusahaan, sehingga menjadi dasar dalam pemilihan domain prioritas COBIT 2019. Penentuan DF ini mengikuti praktik pada penelitian tata kelola TI yang menggunakan *design toolkit* COBIT 2019 melalui studi dokumen dan wawancara untuk menilai kondisi organisasi secara menyeluruh [16].

2. Penentuan Domain Prioritas

Domain prioritas ditentukan berdasarkan hasil integrasi bobot DF yang menghasilkan peta governance/management objective importance. Pemilihan domain ini sesuai praktik penelitian yang menekankan pentingnya risiko, keamanan, dan pengendalian konfigurasi dalam evaluasi tata kelola TI [17].

3. Penilaian Aktivitas Proses COBIT

Setiap proses dianalisis berdasarkan process practices COBIT 2019, meliputi aktivitas, tujuan, dan kontrol yang harus diterapkan. Evaluasi dilakukan dengan membandingkan kondisi aktual perusahaan dengan standar praktik COBIT.

Tahapan penilaian aktivitas proses ini sesuai dengan metodologi yang digunakan pada audit tata kelola TI di lingkungan akademik dan pemerintahan, di mana praktik aktual diverifikasi menggunakan observasi, wawancara, dan dokumentasi [18].

4. Pengukuran Tingkat Kapabilitas (Process Capability Level)

Pengukuran tingkat kapabilitas dilakukan menggunakan skala Level 0–5 sesuai COBIT 2019. Penilaian mempertimbangkan pencapaian aktivitas proses, bukti pendukung, dan konsistensi implementasi. Model kapabilitas ini digunakan secara luas dalam penelitian COBIT, sebagaimana dijelaskan dalam studi tingkat maturitas TI di PT KCI dan perguruan tinggi yang mengukur kesenjangan antara kondisi eksisting dan target kapabilitas [19].

Skala kapabilitas COBIT 2019 mencakup:

- Level 0 (*Incomplete*)
- Level 1 (*Performed*)
- Level 2 (*Managed*)
- Level 3 (*Defined*)
- Level 4 (*Quantitatively Managed*)
- Level 5 (*Optimizing*)

Model ini digunakan untuk menentukan gap dan kebutuhan rekomendasi perbaikan proses TI organisasi, sebagaimana diterapkan dalam berbagai studi evaluasi tata kelola TI berbasis COBIT [17]. Penilaian capability level dilakukan melalui konversi jawaban kuesioner skala Likert ke nilai indeks kuantitatif. Setiap jawaban responden diberi bobot 1-5, dengan nilai 1 menunjukkan penerapan proses yang sangat rendah dan nilai 5 menunjukkan proses telah diterapkan secara menyeluruh, terukur, dan konsisten sesuai praktik COBIT 2019.

Nilai capability level setiap domain dihitung dengan rumus: total skor seluruh jawaban indikator pada domain dibagi jumlah jawaban yang valid pada domain tersebut. Nilai rata-rata ini kemudian dipetakan ke skala capability level COBIT 2019 untuk menggambarkan kondisi aktual proses. Perhitungan dilakukan pada masing-masing domain sehingga diperoleh nilai aktual EDM03, APO12, APO13, dan BAI10.

Dalam penelitian ini, seluruh indikator menggunakan equal weighting karena setiap aktivitas proses dipandang memiliki kontribusi yang setara terhadap pencapaian capability level.

Pembobotan khusus tidak diterapkan agar hasil penilaian tetap sederhana, transparan, dan dapat direplikasi pada organisasi sejenis.

2.5 Analisis Gap Capability Level

Analisis gap dilakukan dengan membandingkan kondisi *capability level* eksisting dengan target *capability level* yang diharapkan organisasi. Selisih antara kondisi aktual dan target digunakan untuk mengidentifikasi area proses yang masih memerlukan peningkatan serta menjadi dasar dalam penyusunan rekomendasi tata kelola TI.

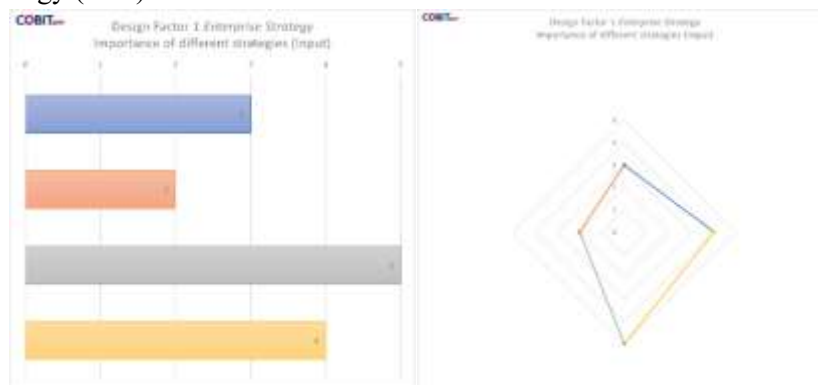
3. Hasil dan Pembahasan

Bagian ini menyajikan hasil analisis tata kelola Teknologi Informasi berdasarkan pengisian Design Factors (DF1–DF11), penentuan domain prioritas COBIT 2019, penilaian aktivitas proses, serta pengukuran tingkat kapabilitas proses.

3.1 Analisis Design Factors (DF1–DF11)

Analisis Design Factors dilakukan untuk mengidentifikasi karakteristik organisasi yang mempengaruhi pemilihan domain tata kelola TI. Setiap DF menghasilkan gambaran prioritas yang menjadi dasar dalam penentuan Governance and Management Objectives (GAMO) COBIT 2019.

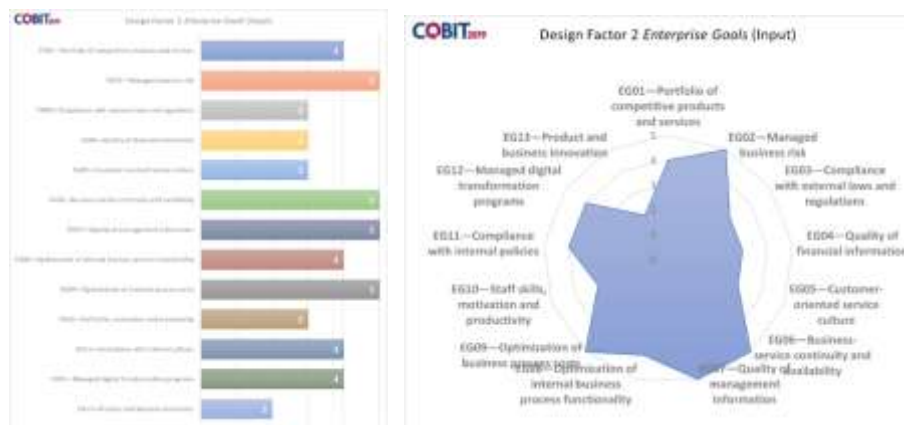
1. Enterprise Strategy (DF1)



Gambar 2. Hasil Design Factor 1

Berdasarkan Gambar 2, DF1 menunjukkan orientasi kuat pada efisiensi operasional dan stabilitas layanan. Skor tertinggi berada pada *cost leadership/operational efficiency* dan *client service/stability* (5 dan 4), sedangkan *pertumbuhan* serta *inovasi* lebih rendah. Pola ini menegaskan bahwa TI diposisikan sebagai pendukung operasi inti dan memperkuat kebutuhan tata kelola risiko serta keamanan TI [12].

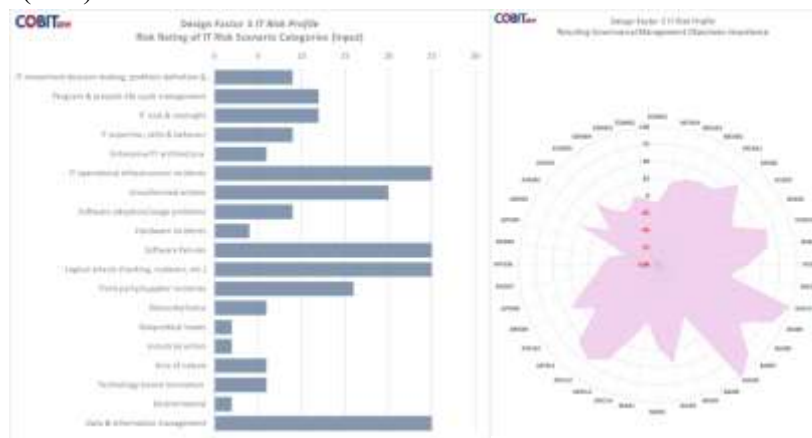
2. Enterprise Goals (DF2)



Gambar 3. Hasil Design Factor 2

Berdasarkan Gambar 3, DF2 menempatkan EG02 (Managed Business Risk), EG06 (Business Service Continuity and Availability), EG07 (Quality of Management Information), dan EG09 (Optimization of Business Process Costs) sebagai prioritas tertinggi. Temuan ini menunjukkan fokus organisasi pada keberlangsungan layanan, efisiensi proses, dan kualitas informasi, sejalan dengan kebutuhan institusi penyedia layanan publik [1].

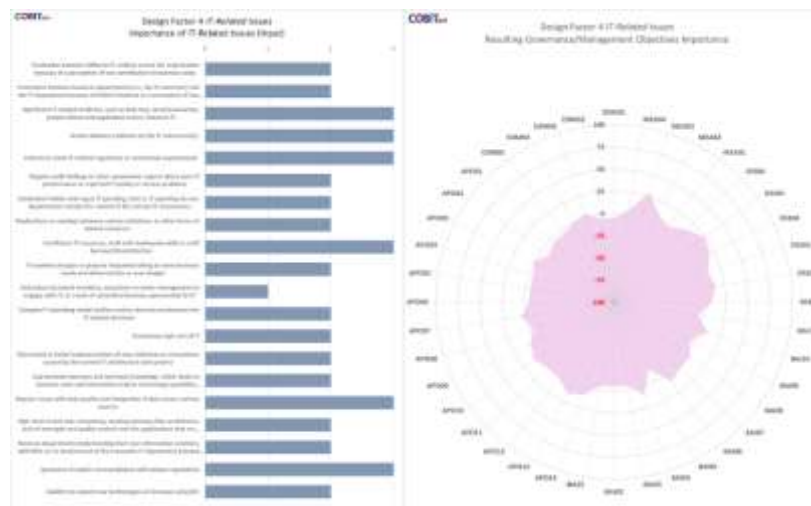
3. IT Risk Profile (DF3)



Gambar 4. Hasil Design Factor 3

Berdasarkan Gambar 4, DF3 menunjukkan paparan tertinggi pada IT operational infrastructure incidents, logical attacks, serta data and information management. Risiko tersebut berdampak pada ketersediaan layanan, integritas sistem, dan kualitas data [4]. Grafik radar memperkuat prioritas EDM03, APO12, dan APO13, serta menunjukkan keterkaitan dengan proses BAI dan DSS dalam rancangan peningkatan tata kelola TI.

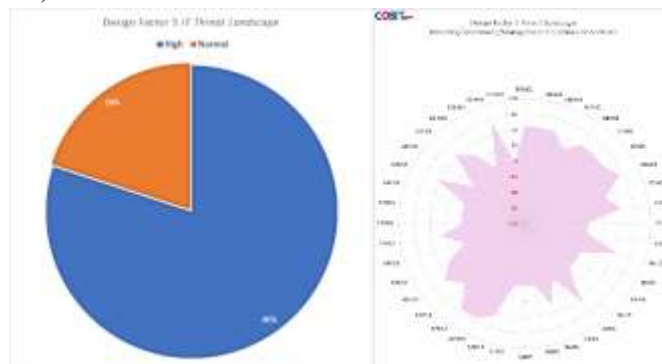
4. IT-Related Issues (DF4)



Gambar 5. Hasil Design Factor 4

Berdasarkan Gambar 5, DF4 menonjolkan temuan audit, biaya pengelolaan data, dan risiko ketidakpatuhan sebagai isu utama. Kondisi ini menunjukkan jarak antara kebijakan formal dan praktik implementasi, terutama pada pengelolaan risiko, keamanan, dan informasi. Profil isu tersebut memperkuat prioritas EDM03, APO12, APO13, dan BAI10 [6].

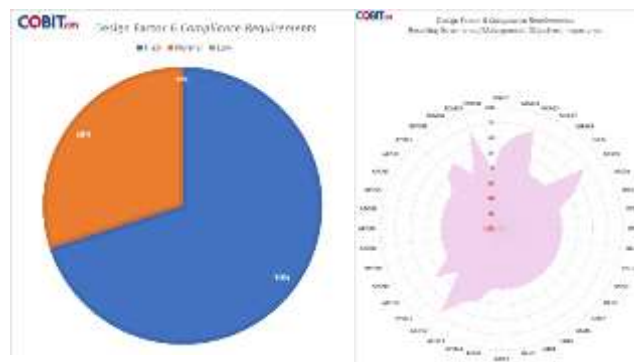
5. Threat Landscape (DF5)



Gambar 6. Hasil Design Factor 5

Berdasarkan Gambar 6, DF5 menunjukkan 80% skenario ancaman berada pada kategori high impact dan 20% normal. Lanskap ancaman ini mempertegas urgensi penguatan APO13, serta proses DSS yang terkait keberlangsungan dan pemulihan layanan. Temuan ini konsisten dengan literatur keamanan TI yang menempatkan cyber threat management sebagai prioritas pada layanan kritikal [4].

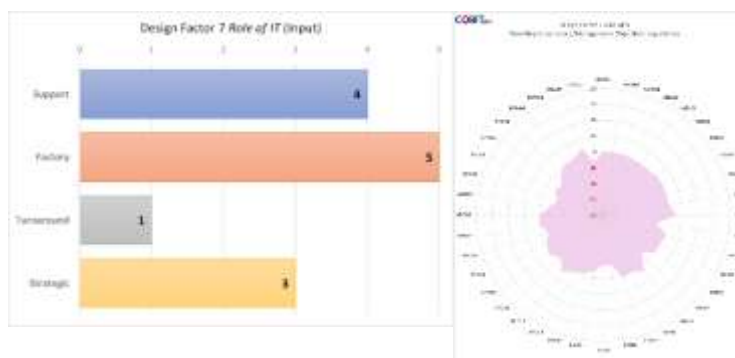
6. Compliance Requirements (DF6)



Gambar 7. Hasil Design Factor 6

Berdasarkan Gambar 7, DF6 menunjukkan 70% kewajiban kepatuhan berada pada kategori high requirement dan 30% normal. Tekanan kepatuhan tersebut memperkuat relevansi MEA03 dan APO12, karena organisasi infrastruktur harus memenuhi standar, regulasi, dan kontrol layanan publik yang lebih ketat dibandingkan sektor komersial biasa [1].

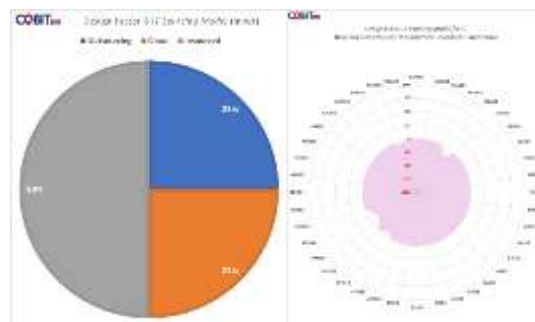
7. Role of IT (DF7)



Gambar 8. Hasil Design Factor 7

Berdasarkan Gambar 8, DF7 menunjukkan peran TI didominasi kategori Factory dan Support. Artinya, TI menjadi fondasi operasi harian sekaligus pendukung proses lintas unit. Prioritas utama berada pada reliability dan availability, sehingga proses DSS04 dan APO11 tetap relevan sebagai area pendukung keberlangsungan serta kualitas layanan.

8. Sourcing Model (DF8)

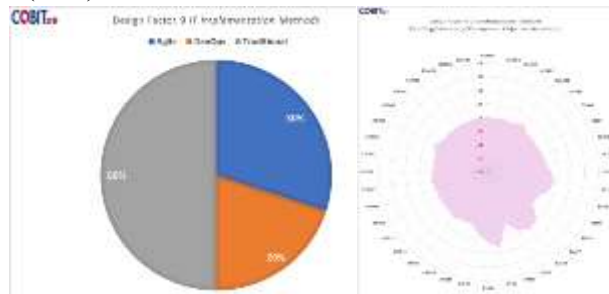


Gambar 9. Hasil Design Factor 8

Berdasarkan Gambar 9, DF8 menunjukkan layanan TI dikelola melalui insourced 50%, outsourcing 25%, dan cloud 25%. Komposisi multi-sourcing ini menuntut kontrol risiko dan

keamanan untuk aset internal maupun pihak ketiga, termasuk SLA, hak akses, dan konfigurasi. Hasilnya memperkuat prioritas APO12, APO13, dan BAI10.

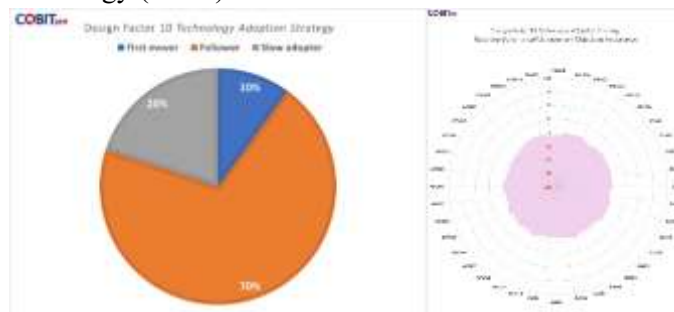
9. Implementation Method (DF9)



Gambar 10. Hasil Design Factor 9

Berdasarkan Gambar 10, DF9 menunjukkan metode implementasi masih didominasi pendekatan tradisional 50%, disertai Agile 30% dan DevOps 20%. Kombinasi ini menandakan fase transisi pengembangan sistem, sehingga change management dan kontrol konfigurasi perlu diperkuat agar lingkungan produksi tetap konsisten. Profil ini menegaskan relevansi BAI10 dan APO12.

10. Technology Adoption Strategy (DF10)



Gambar 11. Hasil Design Factor 10

Berdasarkan Gambar 11, DF10 menunjukkan strategi adopsi teknologi didominasi posisi follower 70%, slow adopter 20%, dan first mover 10%. Organisasi cenderung memilih teknologi yang telah stabil, sehingga fokus tata kelola berada pada keandalan layanan, kompatibilitas sistem, serta konsistensi risiko, keamanan, dan konfigurasi.

11. Enterprise Size (DF11)

Perusahaan yang menjadi objek penelitian dikategorikan sebagai large enterprise dengan jumlah karyawan lebih dari 2.000 orang. Ukuran organisasi yang besar ini menuntut tata kelola TI yang lebih formal, terdokumentasi, dan terintegrasi, khususnya pada pengelolaan risiko, keamanan informasi, dan konfigurasi, sehingga proses-proses TI tidak dapat dikelola secara ad-hoc [20].

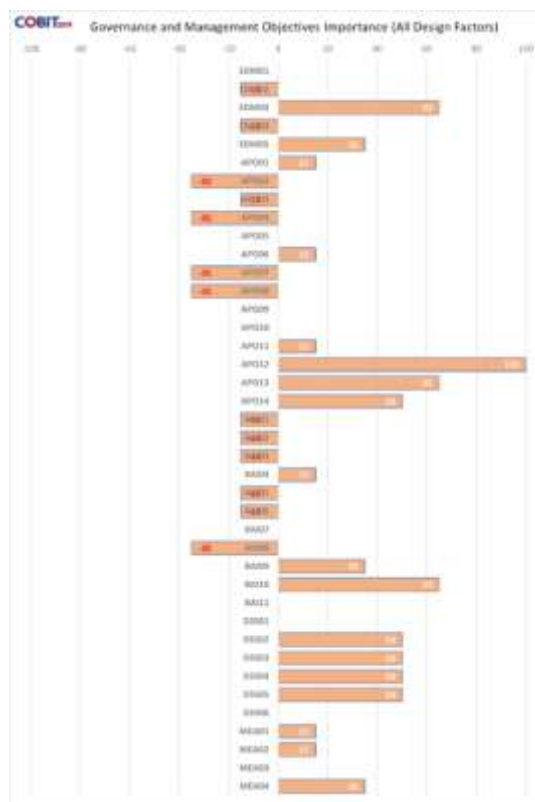
3.2 Prioritas Domain Tata Kelola COBIT 2019

Berdasarkan integrasi seluruh DF melalui GAMO Importance Analysis, diperoleh domain-domain dengan bobot tertinggi, yaitu:

- Ensure Risk Optimization (EDM03)
- Manage Risk (APO12)
- Manage Security (APO13)

- Manage Configuration (BAI10)

Domain tersebut dipilih karena memiliki nilai kepentingan paling tinggi, sejalan dengan konteks risiko, keamanan, dan konsistensi konfigurasi layanan TI. Hasil pemetaan GAMO berdasarkan seluruh Design Factors ditampilkan pada Gambar 12, yang menunjukkan bahwa EDM03, APO12, APO13, dan BAI10 menjadi prioritas utama evaluasi.



Gambar 12. Grafik Governance and Management Objectives Importance (All Design Factors)

3.3 Analisis Tingkat Kapabilitas (Capability Level) dan Kesenjangan

Penilaian capability level dilakukan menggunakan skala Level 0-5 COBIT 2019, berdasarkan bukti kuesioner, wawancara, dan dokumentasi. Hasil evaluasi menunjukkan bahwa EDM03, APO12, dan APO13 berada pada kisaran Level 4, sedangkan BAI10 berada sedikit di bawah ambang Level 4 sehingga menjadi area perbaikan utama menuju target Level 5 (Optimizing). Rangkuman nilai capability level masing-masing domain ditampilkan pada Tabel 3.

Tabel 3. Hasil Tingkat Kapabilitas Setiap Domain

Domain	Nilai Aktual	Target	Gap
Ensure Risk Optimization (EDM03)	4.06	5	0.94
Manage Risk (APO12)	4.05	5	0.95
Manage Security (APO13)	4.04	5	0,96
Manage Configuration (BAI10)	3.96	5	1.04
Rata-rata	4.03	5	0.97

Berdasarkan Tabel 3, nilai capability level aktual seluruh domain berada pada rentang 3.96-4.06. Capaian Level 4 menunjukkan bahwa proses tata kelola TI telah terdefinisi, dijalankan secara konsisten,

dan mulai didukung pengukuran kuantitatif. Namun, capaian ini juga menunjukkan bahwa organisasi baru berada pada tahap siap menuju optimasi, belum sepenuhnya optimal, karena mekanisme perbaikan berkelanjutan, otomatisasi pengendalian, dan pemantauan berbasis indikator belum diterapkan secara merata pada seluruh domain.

- Pada domain EDM03, gap masih muncul karena mekanisme pemantauan risiko TI belum berjalan secara rutin dan pembahasan risiko lebih banyak dilakukan ketika muncul isu tertentu. Akar penyebabnya adalah belum kuatnya siklus risk review periodik dan belum meratanya penerjemahan risk appetite dari level korporat ke level operasional TI. Akibatnya, pemantauan risiko masih cenderung reaktif dan belum sepenuhnya berbasis indikator risiko utama.
- Pada domain APO12, integrasi risk register TI dengan Enterprise Risk Management belum sepenuhnya menyatu karena identifikasi risiko masih dilakukan pada level unit sebelum direkonsiliasi ke tingkat korporat. Kondisi ini membuat konsolidasi risiko TI belum selalu real-time dan audit risiko TI belum memiliki jadwal tahunan yang konsisten. Akar masalahnya terletak pada belum adanya mekanisme integrasi data risiko yang menghubungkan register operasional TI dengan dashboard ERM korporat secara langsung.
- Pada domain APO13, gap terutama disebabkan oleh pembaruan dokumen keamanan, termasuk Statement of Applicability (SoA), yang belum dilakukan secara berkala. SoA belum diperbarui secara rutin karena proses peninjauan kontrol keamanan masih bergantung pada siklus audit atau perubahan besar, bukan pada agenda review tahunan yang terjadwal. Selain itu, pelatihan keamanan informasi belum terlaksana secara konsisten sehingga tingkat kesadaran keamanan pengguna masih perlu diperkuat.
- Domain BAI10 memiliki gap terbesar karena baseline configuration belum diterapkan secara merata pada seluruh sistem dan pembaruan CMDB belum selalu konsisten. Akar penyebab utamanya adalah kompleksitas lingkungan TI yang melibatkan aset internal, layanan pihak ketiga, dan cloud, sebagaimana terlihat pada DF8, serta penggunaan metode implementasi yang beragam sebagaimana terlihat pada DF9. Kombinasi tersebut membuat perubahan konfigurasi lebih sulit ditelusuri apabila prosedur change management, pencatatan aset, dan validasi CMDB tidak dijalankan secara disiplin.

Secara keseluruhan, nilai rata-rata capability level 4.03 menunjukkan bahwa tata kelola TI berada pada tingkat yang baik, namun masih membutuhkan peningkatan signifikan untuk mencapai capability level optimal sesuai target organisasi.

3.4 Perbandingan dengan Studi Sejenis

Dibandingkan dengan studi COBIT 2019 pada sektor kesehatan, pendidikan, dan pemerintahan, penelitian ini memiliki fokus yang lebih terintegrasi. Studi pada rumah sakit cenderung menitikberatkan evaluasi pada keamanan sistem informasi [4], sedangkan studi pada perguruan tinggi lebih banyak mengevaluasi layanan akademik, kualitas sistem, atau tata kelola sistem informasi akademik [10][17]. Pada sektor pemerintahan, penelitian COBIT 2019 umumnya menekankan kepatuhan, dokumentasi, atau penguatan layanan publik berbasis elektronik [6][8][13].

Temuan penelitian ini sejalan dengan studi sektor publik yang menunjukkan bahwa dokumentasi, integrasi kontrol, dan konsistensi pengawasan masih menjadi tantangan utama. Perbedaannya, konteks BUMN infrastruktur menempatkan risiko operasional, keamanan informasi, dan manajemen konfigurasi sebagai satu rangkaian yang saling bergantung. Dengan demikian, gap pada BAI10 tidak hanya berdampak pada pencatatan aset, tetapi juga dapat memengaruhi efektivitas pengendalian risiko pada APO12 dan keamanan informasi pada APO13.

3.5 Rekomendasi Peningkatan Tata Kelola TI

Berdasarkan hasil analisis kesenjangan antara capability level saat ini dan target Level 5 (Optimizing), dirumuskan beberapa rekomendasi peningkatan tata kelola TI sebagai berikut.

Tabel 4. Sintesis gap, dampak, dan rekomendasi per domain

Domain	Gap Utama	Dampak	Rekomendasi
EDM03	Risk review belum rutin dan risk appetite belum diturunkan merata ke level operasional.	Pemantauan risiko cenderung reaktif dan prioritas mitigasi kurang konsisten.	Formalisasi risk appetite/tolerance dan risk review periodik.
APO12	Risk register TI belum terintegrasi penuh dengan ERM dan KRI belum merata.	Konsolidasi risiko terlambat dan kemampuan deteksi dini belum optimal.	Integrasi risk register ke dashboard ERM dan penetapan KRI berbasis data.
APO13	SoA dan kebijakan keamanan belum diperbarui berkala; awareness belum rutin.	Kontrol keamanan berisiko tidak sesuai dengan lanskap ancaman terbaru.	Review tahunan SoA, pelatihan keamanan, simulasi insiden, dan audit keamanan.
BAI10	Baseline configuration dan CMDB belum konsisten; perubahan belum selalu terdokumentasi.	Ketertelusuran aset dan kontrol perubahan konfigurasi melemah.	Verifikasi aset periodik, baseline konfigurasi standar, dan change management formal.

Tabel 4 memperlihatkan bahwa rekomendasi diarahkan pada penguatan siklus pengawasan risiko, pembaruan kontrol keamanan, dan disiplin manajemen konfigurasi agar gap menuju Level 5 dapat dikurangi secara terukur.

3.6 Saran Untuk Penelitian Selanjutnya

Penelitian ini memiliki beberapa keterbatasan. Pertama, penelitian menggunakan studi kasus tunggal pada satu BUMN infrastruktur sehingga hasilnya tidak dapat digeneralisasi secara langsung ke seluruh BUMN atau sektor industri lain. Kedua, sebagian data capability level bersumber dari self-assessment responden sehingga tetap memiliki potensi bias persepsi, meskipun telah ditriangulasi dengan wawancara, observasi, dan dokumen. Ketiga, data kuantitatif yang digunakan masih terbatas pada skor kuesioner capability level dan belum menguji hubungan statistik antara kapabilitas TI dengan indikator kinerja organisasi.

Penelitian selanjutnya dapat memperluas cakupan domain COBIT 2019, misalnya DSS04, MEA03, APO11, atau BAI06, agar evaluasi tata kelola TI menjadi lebih komprehensif. Selain itu, studi longitudinal sebelum dan sesudah implementasi rekomendasi perlu dilakukan untuk mengukur efektivitas perbaikan. Penelitian berikutnya juga dapat menguji korelasi antara capability level TI dan kinerja organisasi, seperti reliabilitas layanan, tingkat insiden, kepatuhan audit, atau efisiensi biaya operasional TI.

4. Kesimpulan

Penelitian ini menyimpulkan bahwa tata kelola Teknologi Informasi pada BUMN infrastruktur di Indonesia telah berada pada capability level yang baik, yaitu pada rentang Level 4 (Quantitatively Managed). Hasil analisis Design Factors mengidentifikasi bahwa risiko operasional, ancaman keamanan, dan tuntutan kepatuhan menjadi faktor dominan yang membentuk prioritas tata kelola TI. Domain EDM03, APO12, APO13, dan BAI10 menunjukkan bahwa pengelolaan risiko, keamanan informasi, dan konsistensi konfigurasi merupakan area utama yang perlu diperkuat secara terpadu.

Meskipun demikian, seluruh domain masih memiliki gap menuju Level 5 (Optimizing). Gap tersebut disebabkan oleh belum optimalnya monitoring risiko, belum terintegrasinya risk register TI dengan ERM korporat, belum rutusnya pembaruan dokumen keamanan seperti SoA, serta belum konsistennya baseline configuration dan pemutakhiran CMDB. Oleh karena itu, perusahaan perlu memperkuat forum risk review, mengintegrasikan data risiko, memperbarui kebijakan keamanan secara berkala, meningkatkan kesadaran keamanan pengguna, dan menegakkan prosedur change management. Temuan ini relevan sebagai

acuan perbaikan pada organisasi sejenis, tetapi generalisasinya perlu dilakukan secara hati-hati karena penelitian bersifat studi kasus tunggal.

Referensi

- [1] N. A. Hidayah, E. Fetrina, and S. Ratnawati, “Analysis of Information Technology Governance Priorities at PTKIN Using The COBIT 2019 Framework,” vol. 8, no. 1, pp. 111–120, 2025, doi: 10.15408/aism.v8i1.45011.
- [2] M. Hutagalung and E. D. Wibawa, “Enhancing Digital Transformation: A Comprehensive Review of PT Utama Karya’s Information Technology Management in 2023,” vol. 07, no. 06, pp. 3898–3902, 2024, doi: 10.47191/ijcsrr/V7-i6-40.
- [3] M. Hutagalung and L. Aldianto, “THE CHALLENGE OF IMPLEMENTATION INDONESIA INFRASTRUCTURE COMPANY CASE STUDY : AT PT . HUTAMA KARYA (PERSERO),” vol. 4, no. 10, pp. 9442–9464, 2024.
- [4] M. A. Algiffary, M. I. Herdiansyah, and Y. N. Kunang, “Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI,” vol. 4, no. 1, pp. 19–26, 2023.
- [5] M. M. Rosady, A. H. Muhammad, and A. Nasiri, “ANALYSIS OF INFORMATION TECHNOLOGY INNOVATION GOVERNANCE USING COBIT: SYSTEMATIC LITERATURE REVIEW,” vol. 10, no. 1, pp. 533–541, 2025.
- [6] B. Delvika, N. Abror, D. S. Rahayu, M. H. Zikri, and H. Dwi, “Jurnal Testing dan Implementasi Sistem Informasi TATA KELOLA AUDIT SISTEM INFORMASI PADA BMKG STASIUN METEOROLOGI SSK II PEKANBARU MENGGUNAKAN COBIT 2019 INFORMATION SYSTEM AUDIT GOVERNANCE AT BMKG SSK II PEKANBARU METEOROLOGY STATION USING COBIT 2019,” vol. 2, no. 1, pp. 28–38, 2024.
- [7] A. C. Puspitaningrum *et al.*, “Systematic Literature Review : Implementasi COBIT sebagai Best Practice Tata Kelola Sistem Pemerintahan berbasis Elektronik (SPBE) Systematic Literature Review : Implementation COBIT as a Best Practice of,” vol. 13, pp. 335–345, 2024.
- [8] A. I. Aprianingsih, D. P. Githa, G. Made, and A. Sasmita, “Audit Tata Kelola TI Pada BMKG Dengan Menggunakan Framework COBIT 2019 (Studi Kasus : BMKG Wilayah III Denpasar),” vol. 11, no. 4, pp. 220–228, 2024.
- [9] H. Z. Rahmat, F. Nurapriani, and B. Huda, “Penerapan Tata Kelola Audit Sistem Informasi Pada Shen Coffee Space Menggunakan Framework COBIT 2019,” 2019.
- [10] N. Putu, M. Kusuma, I. G. Putu, K. Juliharta, A. Agung, and G. Adi, “Evaluasi Tata Kelola Sistem Informasi Akademik Menggunakan Kerangka Kerja COBIT 2019 (Studi Kasus : Universitas Primakara),” vol. 18, no. 02, 2024.
- [11] N. A. Hidayah, M. A. Arfani, and Y. A. Kusumastuti, “Identifikasi Tujuan Tata Kelola Teknologi Informasi PLT FST UIN Jakarta Menggunakan Framework COBIT 2019,” vol. 5, no. 1, pp. 90–97, 2024.
- [12] D. Nurjanah and B. A. Akbar, “AUDIT SISTEM INFORMASI KEUANGAN DESA (SISKEUDES) MENGGUNAKAN FRAMEWORK COBIT 2019 (STUDI KASUS DESA KARANGHEGAR) Pendahuluan Tujuan Penelitian Kajian Teori Definisi Audit Sistem Informasi,” vol. 10, no. 02, pp. 45–52, 2023.
- [13] R. Afdhani and B. Soewito, “Perancangan Tata Kelola TI Menggunakan Framework COBIT 2019

- pada Pusat Data dan Informasi Kementerian,” vol. 10, pp. 22–33, 2024.
- [14] A. Y. Nugroho, “Audit Tata Kelola Teknologi Informasi Adaptif Di Era Transformasi Digital Menggunakan COBIT 2019,” vol. 2, no. 1, pp. 1–10, 2025.
- [15] P. D. Driya, I. G. Lanang, A. Raditra, and I. M. Ardwi, “TEKNIK PENGUMPULAN DATA PADA AUDIT SISTEM INFORMASI DENGAN FRAMEWORK COBIT,” vol. 2, no. 2, pp. 70–83, 2021.
- [16] M. G. Ginanjar, L. Ramadani, and R. A. Nugraha, “Perancangan Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 di DISKOMINFOSAN Kabupaten Sukabumi,” vol. 10, no. 3, 2021.
- [17] A. F. K. Parinduri and J. Hartono, “Evaluasi Penerapan Tata Kelola Teknologi Informasi (TI) Menggunakan Framework Cobit 2019 (Studi Kasus pada Perguruan Tinggi Harapan Maju),” vol. 11, no. 3, 2023.
- [18] I. P. Windasari, M. Yonanta, R. Y. Himawati, and A. F. Rochim, “Audit Tata Kelola Teknologi Informasi Pada Perusahaan Menggunakan Domain DSS dan MEA Kerangka Kerja COBIT 2019 (Studi Kasus : Fakultas Teknik UNDIP),” vol. 43, no. 1, pp. 67–77, 2022, doi: 10.14710/teknik.v43i1.34121.
- [19] H. Santoso and U. Pradita, “Strategi Peningkatan Tata Kelola TI di PT Kereta Commuter Indonesia untuk Memenuhi Standar COBIT 2019 Universitas Pradita , Indonesia IT Governance Improvement Strategy at PT Kereta Commuter Indonesia to Meet COBIT 2019 Standards,” vol. 5, no. 6, pp. 1519–1525, 2025.
- [20] R. A. Fandi, M. Jazman, M. Fronita, and E. Saputra, “Audit Tata Kelola Teknologi Informasi pada BKKBN Provinsi Riau menggunakan Cobit 2019 Audit of Information Tecnology Governance at BKKBN Riau Province using the 2019 Cobit Framework,” vol. 13, pp. 2672–2686, 2024.