

# Jurnal JTik (Jurnal Teknologi Informasi dan Komunikasi)

DOI: <https://doi.org/10.35870/jtik.v10i4.6691>

## Manajemen Risiko Keamanan Aset Teknologi Informasi dengan Metode COBIT 2019 (Studi Kasus: Diskominfo Kabupaten Tangerang)

Nida Fadhillah<sup>1</sup>, Yulhendri<sup>2\*</sup><sup>1,2\*</sup> Program Studi Sistem Informasi, Universitas Esa Unggul, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta, Indonesia.

### article info

#### Article history:

Received 25 February 2026

Received in revised form

18 March 2026

Accepted 1 April 2026

Available online October 2026.

#### Keywords:

Risk Management; IT Asset

Security; COBIT 2019.

#### Kata Kunci:

Manajemen Risiko; Keamanan

Aset TI; COBIT 2019.

### abstract

Information Technology (IT) asset security is a fundamental aspect in sustaining the operational continuity of an organization, particularly within the government sector. The Tangerang Regency Communication and Information Agency (Diskominfo), as the entity responsible for managing regional information systems, is required to apply sound risk management practices to protect IT assets from various threats. This study aims to identify, assess, and manage IT asset security risks by applying the COBIT 2019 framework, which provides a structured approach to IT governance and management. The research methods employed include literature review, interviews, and analysis of IT security policies and procedures in place at Diskominfo Tangerang Regency. IT asset security was examined based on relevant domains within COBIT 2019, with emphasis on risk management processes and information security controls. The findings of this study are expected to yield strategic recommendations for Diskominfo Tangerang Regency in strengthening the effectiveness of IT asset security risk management and ensuring adherence to applicable IT governance standards.

### abstrak

Keamanan aset Teknologi Informasi (TI) merupakan aspek mendasar dalam menjaga keberlangsungan operasional suatu organisasi, terutama di sektor pemerintahan. Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Tangerang, selaku entitas yang bertanggung jawab atas pengelolaan sistem informasi daerah, dituntut untuk menerapkan praktik manajemen risiko yang baik guna melindungi aset TI dari berbagai ancaman. Penelitian ini bertujuan untuk mengidentifikasi, menilai, dan mengelola risiko keamanan aset TI dengan menerapkan framework COBIT 2019, yang menyediakan pendekatan terstruktur dalam tata kelola dan manajemen TI. Metode penelitian yang digunakan meliputi studi literatur, wawancara, serta analisis terhadap kebijakan dan prosedur keamanan TI yang berlaku di Diskominfo Kabupaten Tangerang. Keamanan aset TI dikaji berdasarkan domain yang relevan dalam COBIT 2019, dengan penekanan pada proses manajemen risiko dan pengendalian keamanan informasi. Temuan penelitian ini diharapkan dapat menghasilkan rekomendasi strategis bagi Diskominfo Kabupaten Tangerang dalam memperkuat efektivitas manajemen risiko keamanan aset TI, serta memastikan kepatuhan terhadap standar tata kelola TI yang berlaku.

\*Corresponding Author. Email: [nidafadhillah07ag@gmail.com](mailto:nidafadhillah07ag@gmail.com) <sup>1\*</sup>.

Copyright 2026 by the authors of this article. Published by Lembaga Otonom Lembaga Informasi dan Riset Indonesia (KITA INFO dan Riset). This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

## 1. Pendahuluan

Teknologi Informasi (TI) telah menjadi bagian yang tidak terpisahkan dari kehidupan manusia. Hampir seluruh aspek kehidupan, mulai dari individu, organisasi, hingga pemerintahan, bergantung pada TI untuk menjalankan operasinya sehari-hari. Oleh sebab itu, aset TI memiliki nilai yang tinggi dan harus dilindungi dari berbagai ancaman keamanan (Saputra, 2023). Serangan siber yang semakin terorganisir dan canggih menjadikan aset TI yang menyimpan data sensitif sebagai sasaran utama. Kebocoran data dan serangan siber dapat menyebabkan kerugian finansial yang besar, serta berdampak pada reputasi organisasi dan kepercayaan publik (Simanjuntak *et al.*, 2023). Keamanan data merupakan salah satu aset terpenting bagi industri TI. Salah satu cara untuk melindungi data dari ancaman pencurian adalah melalui penerapan manajemen risiko, yang berfungsi untuk mendeteksi celah keamanan dalam sistem organisasi yang berpotensi menimbulkan pelanggaran. Diperlukan prosedur dan kebijakan yang tepat untuk mencegah pelanggaran keamanan tersebut masuk ke dalam instansi maupun organisasi (Jauhary *et al.*, 2022).

Manajemen risiko merupakan suatu sistem yang digunakan untuk memimpin, mengarahkan, dan mengendalikan organisasi guna meningkatkan kinerjanya demi kepentingan pemangku kepentingan dan pertumbuhan ekonomi nasional, dengan berpedoman pada hukum dan standar etika yang berlaku (Miftakhatun, 2020). Manajemen risiko dapat pula didefinisikan sebagai metode yang terstruktur dan sistematis untuk mengidentifikasi, memantau, merancang solusi, melaporkan risiko, dan mengelola organisasi dalam menghadapi berbagai risiko. Tujuannya adalah memaksimalkan kemungkinan dan dampak dari peristiwa yang bersifat positif, sekaligus meminimalkan kemungkinan dan dampak dari peristiwa yang bersifat negatif (Ariesta & Perdanakusuma, 2022). Salah satu instansi pemerintahan yang menjadikan TI sebagai kebutuhan dalam menunjang pelayanan publik adalah Dinas Komunikasi dan Informatika (Diskominfo). Diskominfo Kabupaten Tangerang merupakan salah satu dinas di lingkungan Pemerintah Kabupaten Tangerang yang bertanggung jawab dalam pengelolaan informasi dan teknologi di

wilayahnya. Aset TI seperti data, perangkat lunak, perangkat keras, dan infrastruktur jaringan merupakan elemen penting yang harus dijaga keamanannya guna mendukung pelayanan publik yang efektif dan efisien (Afdhani & Soewito, 2024).

Seiring dengan meningkatnya ancaman keamanan siber, seperti serangan *malware*, *phishing*, serta kebocoran data, risiko terhadap aset teknologi informasi pun semakin bertambah. Berdasarkan hasil wawancara dengan Ketua Tim Perencanaan Diskominfo Kabupaten Tangerang, pengelolaan TI pada instansi tersebut belum berjalan secara maksimal. Keterbatasan sumber daya manusia (SDM) menjadi salah satu faktor utama yang menyebabkan instansi belum sepenuhnya mampu menghadapi risiko yang dapat terjadi sewaktu-waktu. Selain itu, masih terdapat pegawai yang kurang memahami pentingnya praktik keamanan, seperti penggunaan kata sandi yang kuat atau kewaspadaan terhadap *email phishing*. Kondisi ini turut meningkatkan risiko pelanggaran keamanan, di samping risiko bencana alam, kegagalan perangkat keras, atau insiden lainnya yang dapat mengancam ketersediaan layanan TI (Rohman *et al.*, 2020). Ketidaksiapan dalam menghadapi risiko-risiko tersebut dapat berdampak serius, seperti gangguan layanan, pencurian data sensitif, hingga kerugian finansial dan reputasi (Ridwan *et al.*, 2021). Berdasarkan kondisi tersebut, diperlukan suatu pendekatan yang terstruktur dalam mengelola risiko keamanan aset TI di lingkungan Diskominfo Kabupaten Tangerang melalui penerapan manajemen risiko TI yang efektif berbasis praktik terbaik. Salah satu acuan yang relevan adalah COBIT 2019 (*Control Objectives for Information and Related Technologies*), yang memberikan panduan lengkap untuk tata kelola dan manajemen risiko TI pada tingkat *enterprise* (Putra & Wijaya, 2022).

COBIT 2019 merupakan pembaruan dari versi sebelumnya, di mana ISACA menyelaraskan COBIT agar tetap relevan dalam membantu organisasi mencapai tujuan bisnisnya (ISACA, 2019). Tingkat kegunaan TI yang memadai dapat dicapai dengan menerapkan manajemen TI yang mempertimbangkan seluruh aspek yang berkaitan dengan penggunaan dan ketersediaan layanan, termasuk layanan dan sumber daya. Hal ini dapat diwujudkan melalui penerapan sistem tata kelola yang baik, disertai sumber daya yang

memadai serta dampak risiko yang seminimal mungkin. Untuk memenuhi tujuan tata kelola dan manajemen, setiap organisasi perlu menetapkan, menyesuaikan, dan mempertahankan tata kelola sistem yang telah dibangun (ISACA, 2019). Secara umum, COBIT 2019 bertujuan untuk meningkatkan pemahaman serta pengelolaan risiko agar manfaat teknologi informasi dapat tercapai secara optimal, sekaligus membantu penyatuan praktik manajemen teknologi informasi dalam satu acuan yang terstandar.

Berdasarkan latar belakang tersebut, penelitian ini mengangkat judul "*Manajemen Risiko Keamanan Aset Teknologi Informasi dengan Metode COBIT 2019 (Studi Kasus: Diskominfo Kabupaten Tangerang)*." Penelitian ini bertujuan untuk menganalisis penerapan manajemen risiko keamanan aset TI menggunakan COBIT 2019 di Diskominfo Kabupaten Tangerang. Melalui penelitian ini, diharapkan dapat ditemukan solusi yang tepat untuk meningkatkan efektivitas manajemen risiko serta menghasilkan rekomendasi kebijakan berbasis data guna meningkatkan keamanan TI di instansi tersebut.

## 2. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dan kuantitatif yang dilaksanakan pada September 2024 hingga Februari 2025 di Diskominfo Kabupaten Tangerang. Data primer diperoleh melalui wawancara, observasi lapangan, dan penyebaran kuesioner, sedangkan data sekunder bersumber dari dokumen instansi terkait penerapan SPBE. Permasalahan yang diidentifikasi berfokus pada keterbatasan SDM dan belum optimalnya pengelolaan risiko TI, terutama pada aset SPBE yang meliputi infrastruktur, data/informasi, perangkat keras, layanan, serta keamanan informasi. Penelitian ini menggunakan COBIT 2019 dengan fokus pada domain EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*) untuk menganalisis tata kelola dan manajemen risiko TI. Tahapan penelitian meliputi identifikasi penerapan komponen COBIT 2019, penentuan *governance and management objectives*, serta pemetaan peran dan tanggung jawab menggunakan *RACI Chart* terhadap enam responden sesuai struktur organisasi.

Instrumen penelitian berupa kuesioner berbasis *capability level* COBIT 2019 dengan skala penilaian 0–5 yang disusun berdasarkan subproses EDM03 dan APO12. Selain itu, dilakukan validasi dokumen (*work product*) seperti dokumen anggaran, audit keamanan informasi, laporan insiden, dan panduan penanganan serangan siber. Data yang terkumpul kemudian diolah untuk menghitung tingkat *capability level* setiap proses melalui perhitungan persentase aktivitas, *output*, *outcome*, dan atribut proses. Selanjutnya dilakukan analisis kesenjangan (*gap analysis*) dengan membandingkan tingkat kapabilitas saat ini (*as-is*) dengan target yang diharapkan (*to-be*). Hasil analisis tersebut menjadi dasar dalam penyusunan rekomendasi mitigasi risiko guna meningkatkan efektivitas tata kelola dan manajemen risiko TI di Diskominfo Kabupaten Tangerang sesuai standar COBIT 2019.

## 3. Hasil dan Pembahasan

### Hasil

Penelitian ini mengumpulkan data primer melalui penyebaran kuesioner kepada responden yang telah dipetakan menggunakan *RACI Chart* COBIT 2019, yaitu unsur pimpinan dan kepala bidang di Dinas Komunikasi dan Informatika Kabupaten Tangerang, meliputi Kepala Dinas, Sekretaris Dinas, Bidang Aplikasi Informatika, Bidang Statistik Sektoral, Bidang Informasi & Komunikasi Publik, serta Bidang Persandian dan Keamanan Informasi. Pengumpulan data difokuskan pada dua *Governance and Management Objectives* COBIT 2019, yaitu EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*). Instrumen kuesioner disusun berdasarkan aktivitas dan *work product* COBIT 2019 dengan skala penilaian *Process Capability Model* mulai dari *Not Achieved* (N) hingga *Fully Achieved* (F). Data yang diperoleh kemudian dianalisis untuk menentukan tingkat kapabilitas (*capability level*) sebagai gambaran kondisi aktual (*as-is*) manajemen risiko keamanan aset TI di instansi tersebut.

### Memahami Konteks dan Strategi Instansi

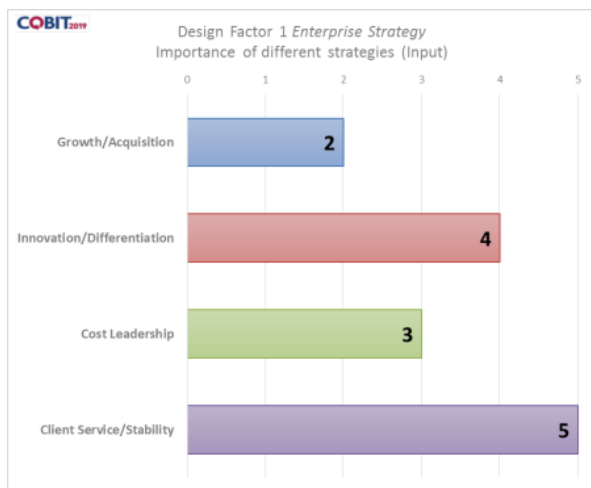
Tahapan perancangan tata kelola TI berdasarkan COBIT 2019 pada Dinas Komunikasi dan Informatika Kabupaten Tangerang meliputi empat poin utama. Pertama, *Understand Enterprise Strategy*:

strategi difokuskan pada peningkatan kinerja penyelenggaraan pemerintahan daerah melalui penguatan tata kelola, pemanfaatan teknologi informasi, dan pengembangan SDM, dengan sasaran meningkatkan kualitas layanan komunikasi dan informasi publik berbasis elektronik serta mendukung penerapan *digital governance* dalam program Tangerang Gemilang. Kedua, *Understand Enterprise Goals*: tujuan utama adalah mewujudkan pemerintahan digital melalui pemanfaatan *platform* elektronik agar layanan publik lebih efektif dan efisien, disertai peningkatan transparansi, aksesibilitas informasi, dan akuntabilitas kinerja. Ketiga, *Understand the Risk Profile*: instansi menghadapi berbagai risiko TI, terutama keterbatasan infrastruktur yang dapat berdampak pada gangguan operasional, kerugian material, penurunan kinerja layanan, dan risiko reputasi. Keempat, *Understand Current ICT-Related Issues*: permasalahan TI yang dihadapi meliputi keterbatasan infrastruktur, belum optimalnya penyatuan sistem dan proses kerja, keterbatasan sumber data serta sistem pelaporan, serta jumlah dan kompetensi SDM yang belum sepenuhnya sesuai kebutuhan organisasi.

## Menentukan Lingkup Awal Sistem Tata Kelola

### 1) *Design Factor 1 – Enterprise Strategy*

Tahap awal penentuan lingkup tata kelola dilakukan dengan menganalisis Faktor Desain 1 (Strategi Organisasi) berdasarkan COBIT 2019.



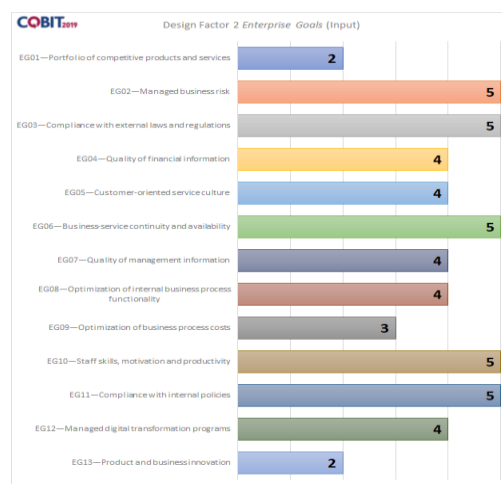
Gambar 1. Grafik Enterprise Strategy Diskominfo Kabupaten Tangerang

Hasil analisis menunjukkan bahwa instansi

memberikan prioritas tertinggi pada strategi Pelayanan Pelanggan dan Stabilitas (skor 5) serta Inovasi (skor 4), yang diarahkan pada pembangunan *digital government* untuk menyediakan layanan informasi publik yang andal dan berorientasi pada kebutuhan masyarakat. Strategi Pengendalian Biaya (skor 3) diterapkan melalui digitalisasi sistem *paperless* guna menekan pemborosan anggaran operasional, sementara aspek Pertumbuhan (skor 2) diperhatikan melalui peningkatan kapasitas kinerja secara bertahap. Seluruh efektivitas strategi ini diukur melalui evaluasi tahunan Indeks SPBE oleh Kementerian PANRB sebagai tolok ukur kematangan tata kelola TI di Kabupaten Tangerang.

### 2) *Design Factor 2 – Enterprise Goals*

Tahap kedua adalah identifikasi *Enterprise Goals* yang mengacu pada 13 tujuan standar COBIT 2019.



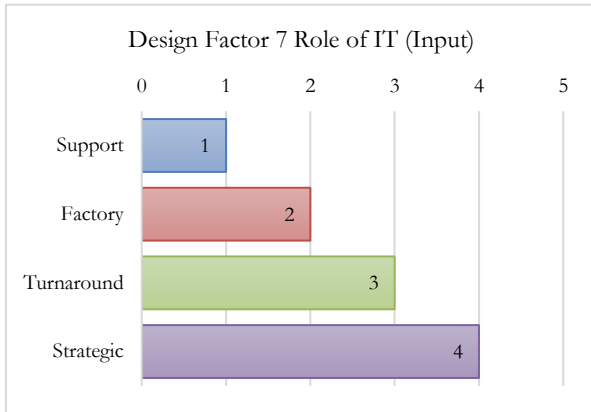
Gambar 2. Grafik Enterprise Goals Diskominfo Kabupaten Tangerang

Sebagai organisasi sektor publik, Diskominfo memberikan nilai kepentingan tertinggi (skor 5) pada aspek pengelolaan risiko (EG02), kepatuhan regulasi eksternal (EG03), keberlangsungan layanan (EG06), kualitas layanan TI (EG10), serta kepatuhan kebijakan internal (EG11). Aspek pendukung seperti kualitas informasi, budaya layanan, dan peningkatan efisiensi proses internal dinilai sangat penting (skor 4), sedangkan tujuan komersial seperti portofolio produk kompetitif (EG01) dan inovasi bisnis (EG13)

mendapat skor rendah karena tidak relevan dengan karakteristik instansi pemerintah.

3) *Design Factor 3 – Risk Profile*

Tahap ketiga adalah pemetaan Profil Risiko TI untuk mengidentifikasi potensi ancaman berdasarkan tingkat dampak dan kemungkinan terjadinya (*likelihood*).

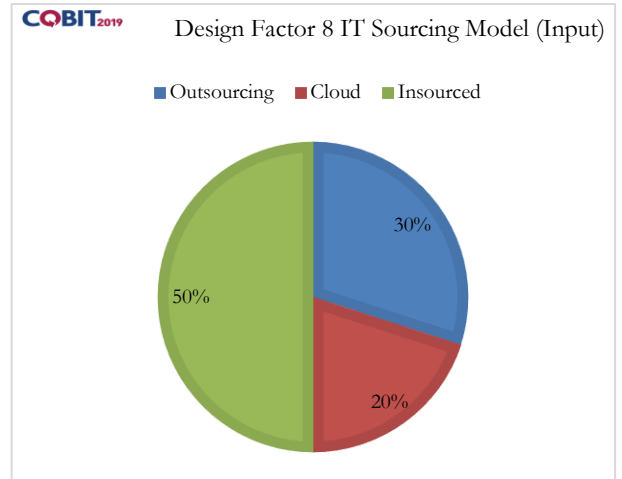


Gambar 3. Grafik Risk Profile Diskominfo Kabupaten Tangerang

Risiko dengan tingkat tertinggi ditemukan pada kategori Insiden Infrastruktur Operasional, Tindakan Tidak Sah (*Unauthorized Actions*), serta Manajemen Data dan Keamanan Informasi, mengingat tingginya ketergantungan instansi terhadap infrastruktur digital. Kategori risiko seperti kompetensi SDM, kegagalan perangkat lunak, dan kepatuhan regulasi berada pada tingkat menengah hingga tinggi, sedangkan risiko terkait investasi TI dan faktor eksternal seperti risiko politik dinilai rendah karena adanya mekanisme perencanaan yang terstruktur.

4) *Design Factor 4 – I&T Related Issues*

Tahap keempat adalah identifikasi *I&T-Related Issues* untuk memetakan permasalahan teknologi informasi yang sedang atau pernah terjadi di Diskominfo Kabupaten Tangerang.



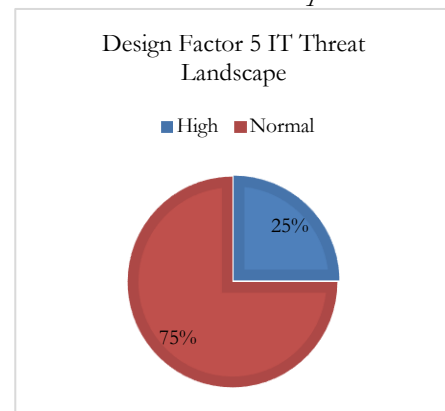
Gambar 4. Grafik I&T Related Issues Diskominfo Kabupaten Tangerang

Isu dengan tingkat kepentingan tertinggi (skor 3) meliputi insiden TI seperti kehilangan data, pelanggaran keamanan, serta gangguan layanan oleh pihak ketiga. Temuan audit yang berulang dan ketidakpatuhan terhadap regulasi juga menjadi perhatian serius karena mengindikasikan kelemahan pada pengendalian internal. Permasalahan lain yang dinilai penting mencakup keterbatasan kompetensi SDM, pengelolaan risiko yang belum optimal, serta rendahnya kualitas integrasi data, sementara isu koordinasi antarunit kerja berada pada level sedang (skor 2).

**Memperbaiki Lingkup Sistem Tata Kelola**

Tahap ini merupakan proses untuk menetapkan ruang lingkup *governance system* melalui penilaian terhadap faktor desain lanjutan.

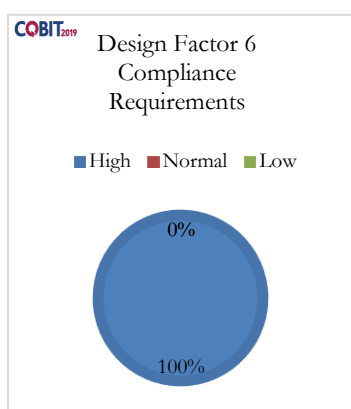
5) *Design Factor 5 – Threat Landscape*



Gambar 5. Grafik Threat Landscape Diskominfo Kabupaten Tangerang

Hasil analisis menunjukkan bahwa organisasi berada dalam lingkungan ancaman yang didominasi kategori Normal (75%), mencakup risiko operasional umum seperti kesalahan konfigurasi, kendala SDM, dan *human error*. Terdapat pula porsi Ancaman Tinggi (25%) yang berkaitan dengan keamanan aset informasi dan keberlangsungan layanan publik, mencakup potensi serangan siber, kebocoran data, serta kegagalan infrastruktur fisik. Mengingat masih adanya keterbatasan kompetensi keamanan informasi di kalangan pegawai, Diskominfo perlu memperkuat sistem pertahanan siber dan kesiapsiagaan insiden agar risiko tersebut dapat dimitigasi secara efektif.

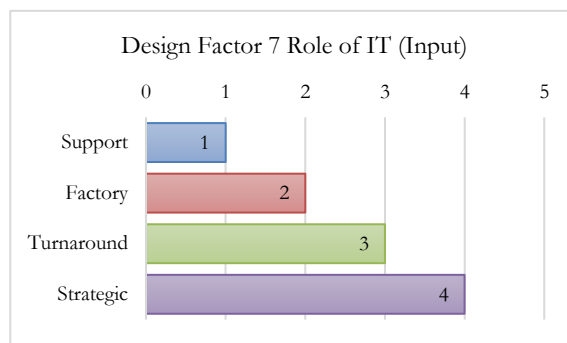
#### 6) Design Factor 6 – Compliance Requirements



Gambar 6. Grafik Compliance Requirements Diskominfo Kabupaten Tangerang

Diskominfo Kabupaten Tangerang menetapkan tingkat Kepatuhan Tinggi (100%), yang menunjukkan bahwa seluruh operasional instansi terikat pada ketentuan hukum yang berlaku tanpa pengecualian. Instansi berkomitmen penuh mematuhi hierarki regulasi mulai dari Peraturan Presiden, Peraturan Menteri, hingga Peraturan Daerah dan Peraturan Wali Kota. Komitmen ini bukan sekadar kewajiban administratif, melainkan dasar utama dalam menegakkan prinsip *good governance* serta menjaga etika operasional penyelenggaraan pemerintahan berbasis elektronik.

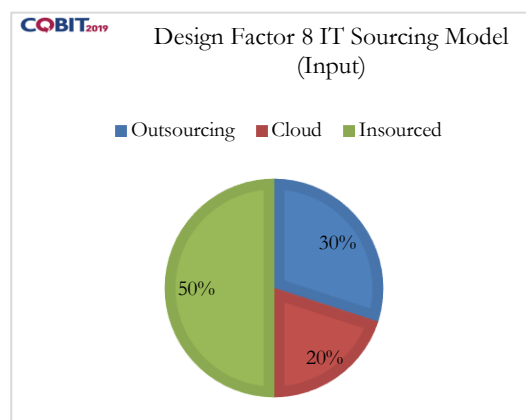
#### 7) Design Factor 7 – Role of IT



Gambar 7. Grafik Role of IT Diskominfo Kabupaten Tangerang

Diskominfo menetapkan peran TI pada tingkat *Strategic* (skor 4), yang menegaskan bahwa teknologi informasi bukan sekadar alat pendukung administratif, melainkan bagian utama dalam penyelenggaraan layanan publik dan pengelolaan SPBE yang transparan dan akuntabel. Peran TI belum mencapai tingkat *transformational* sepenuhnya karena masih adanya kendala keterbatasan SDM dan fokus yang dominan pada aspek keberlangsungan serta pengendalian risiko.

#### 8) Design Factor 8 – Sourcing Model for IT

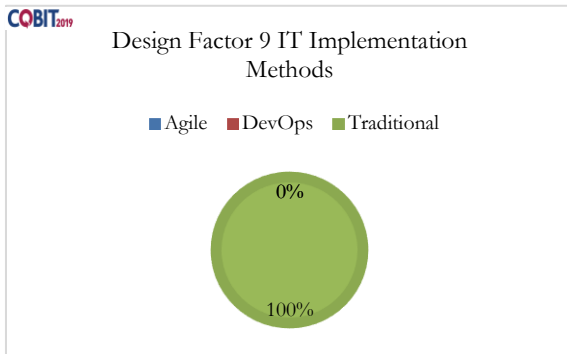


Gambar 8. Grafik Sourcing Model for IT Diskominfo Kabupaten Tangerang

Strategi penyediaan TI didominasi model *Insourced* (50%), yang mencerminkan prioritas pada kendali penuh terhadap aset TI dan keamanan data pemerintahan. Diskominfo juga melibatkan pihak ketiga melalui model *Outsourcing*

(30%) untuk mendukung pengembangan aplikasi dan kebutuhan teknis spesifik, sementara penggunaan *Cloud* (20%) masih terbatas pada fungsi pendukung karena pertimbangan regulasi keamanan data nasional.

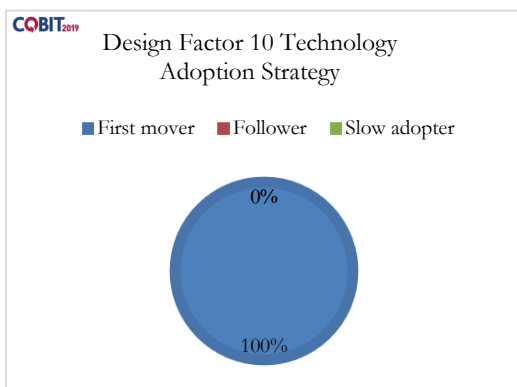
9) *Design Factor 9 – IT Implementation Method*



Gambar 9. Grafik IT Implementation Method Diskominfo Kabupaten Tangerang

Diskominfo menerapkan metode *Traditional* sepenuhnya (100%), yang menunjukkan bahwa instansi masih menggunakan pendekatan konvensional seperti *waterfall* dengan tahapan pengembangan yang terstruktur. Organisasi belum mengadopsi pola kerja yang bersifat adaptif dan iteratif seperti *Agile* maupun *DevOps*. Penyesuaian ke arah metode yang lebih fleksibel di masa depan dapat menjadi pertimbangan strategis untuk meningkatkan kinerja pengembangan sistem TI di Kabupaten Tangerang.

10) *Design Factor 10 – Technology Adoption Strategy*

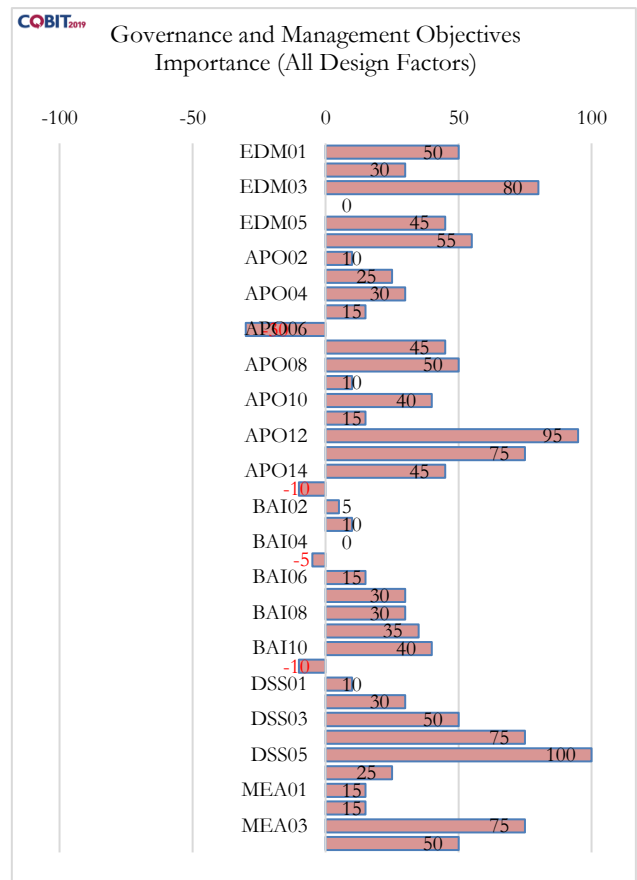


Gambar 10. Grafik Technology Adoption Strategy Diskominfo Kabupaten Tangerang

Diskominfo Kabupaten Tangerang secara penuh menerapkan strategi *First Mover* (100%), yang menunjukkan komitmen instansi untuk berada di garda terdepan dalam pemanfaatan teknologi informasi terbaru dibandingkan perangkat daerah lainnya. Dengan menjadi pengadopsi awal, instansi dapat memastikan bahwa infrastruktur dan layanan digital yang digunakan selalu terkini dan selaras dengan kebutuhan organisasi, sekaligus memperkuat posisi Diskominfo sebagai pemimpin dalam penerapan *digital government* di tingkat daerah.

**Menyimpulkan Desain Sistem Tata Kelola**

Setelah analisis *design factor* (DF1–DF10) dilakukan, seluruh hasil dipadukan untuk merumuskan objektif proses yang menjadi prioritas dalam rancangan sistem tata kelola TI di Dinas Komunikasi dan Informatika Kabupaten Tangerang.



Gambar 11. Kesimpulan Design Factor Diskominfo Kabupaten Tangerang

Hasil pemetaan menunjukkan bahwa proses dengan

tingkat kepentingan tertinggi adalah APO12 (*Manage Risk*), diikuti oleh DSS05 (*Managed Security Services*), EDM03 (*Ensure Risk Optimization*), APO13 (*Managed Security*), serta DSS04 (*Managed Continuity*). Dominasi proses pada domain EDM, APO, dan DSS menegaskan bahwa organisasi memprioritaskan manajemen risiko, keamanan informasi, serta keberlangsungan layanan TI. Proses pada domain BAI dan sebagian APO memiliki tingkat kepentingan yang relatif lebih rendah, menunjukkan bahwa inovasi dan pengembangan sistem belum menjadi fokus utama dibandingkan stabilitas dan kontinuitas layanan. Hasil analisis *design factor* ini memberikan justifikasi yang kuat terhadap pemilihan EDM03 dan APO12 sebagai fokus utama penelitian.

### Analisis Aktivitas *Capability Level*

Analisis tingkat kapabilitas merupakan langkah penting untuk mengukur sejauh mana Diskominfo Kabupaten Tangerang telah menerapkan tata kelola TI berdasarkan standar COBIT 2019. Penilaian menggunakan skala level 0 hingga 5, di mana pencapaian setiap level diukur menggunakan rumus Skala Guttman. Sebuah level dinyatakan tercapai secara penuh (*Fully Achieved*) apabila mencapai skor minimal 85%; apabila skor berada di bawah angka tersebut, penilaian dinyatakan berhenti di level sebelumnya. Proses EDM03 (*Ensure Risk Optimisation*) berhasil mencapai Level 1 dengan skor 91,67% (*Fully Achieved*), yang menunjukkan bahwa instansi telah memiliki struktur tata kelola yang jelas dalam penetapan arahan risiko. Saat pengujian dinaikkan ke Level 2, skor yang diperoleh adalah 83,33% (*Largey Achieved*), sehingga kapabilitas EDM03 secara resmi ditetapkan berada di Level 1. Temuan ini diperkuat oleh analisis bukti dokumen (*work product*), di mana Diskominfo telah memiliki kebijakan manajemen risiko, *risk register*, dan laporan insiden, namun belum memiliki dokumen *Risk Appetite Statement* yang menjadi syarat untuk mencapai level kematangan yang lebih tinggi.

Proses APO12 (*Manage Risk*) yang berfokus pada pelaksanaan manajemen risiko di tingkat operasional melibatkan lima responden dari berbagai bidang strategis. Hasil perhitungan menunjukkan variasi skor antara 66,67% hingga 83,33%, yang mengindikasikan bahwa manajemen risiko sudah dipahami secara konsep dan dijalankan secara parsial,

namun belum mencapai tingkat kepatuhan penuh yang seragam di seluruh unit kerja. Perbaikan selanjutnya perlu diarahkan pada standardisasi pelaporan risiko dan penyusunan dokumen strategis seperti *Risk Appetite Statement* agar instansi dapat naik ke level kematangan yang lebih terorganisir dan terukur.

### Gap Analysis

Analisis kesenjangan (*gap analysis*) membandingkan kondisi aktual pengelolaan TI saat ini (*as-is*) dengan target ideal yang ingin dicapai (*to-be*) di Diskominfo Kabupaten Tangerang.

Tabel 1. Gap Capability Level Objective Process

<i>Government and Management Objectives</i>	<i>As-is</i>	<i>To-be</i>	<i>Gap</i>
EDM03	2	3	1
APO12	2	3	1

Kedua proses, yaitu EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*), saat ini berada pada Level 2 (*as-is*), sementara target yang diharapkan adalah Level 3 (*to-be*), sehingga terdapat kesenjangan sebesar 1 level pada kedua area tersebut. Kesenjangan ini mengindikasikan bahwa meskipun instansi telah menerapkan praktik manajemen risiko secara konsisten, proses tersebut masih perlu ditingkatkan agar lebih terorganisir. Untuk menutup celah tersebut, Diskominfo perlu menstandarisasi kebijakan risiko, memperkuat keterlibatan pimpinan, serta memastikan seluruh prosedur pengelolaan risiko terdokumentasi secara formal sebagai bagian dari budaya kerja organisasi.

### Pembahasan

Berdasarkan analisis kualitatif dan kuantitatif menggunakan COBIT 2019, ditemukan bahwa proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*) memegang peran penting dalam menyelaraskan TI dengan tujuan bisnis Diskominfo Kabupaten Tangerang. Untuk meningkatkan tingkat kemampuan dari kondisi saat ini (*as-is*) menuju target yang diharapkan (*to-be*), diperlukan langkah-langkah strategis yang berfokus pada standarisasi dan formalisasi dokumen.

Tabel 2. Rekomendasi untuk EDM03 – *Ensure Risk Optimisation*

Aspek	Kondisi Saat Ini	Rekomendasi
Tata Kelola Risiko	Belum ada kebijakan risiko TI terintegrasi	Menyusun Kebijakan Manajemen Risiko TI yang disetujui pimpinan
<i>Risk Appetite &amp; Tolerance</i>	Tidak terdokumentasi	Menetapkan <i>risk appetite &amp; risk tolerance</i> secara formal
<i>Monitoring</i> Risiko	Bersifat insidental	Membentuk mekanisme pemantauan risiko berkala
Pelaporan Risiko	Tidak standar	Membuat laporan risiko TI periodik kepada pimpinan

Tabel 3. Rekomendasi untuk APO12 – *Manage Risk*

Aktivitas APO12	Temuan	Rekomendasi
Identifikasi Risiko	Belum terdokumentasi	Menyusun <i>risk register</i> aset TI
Analisis Risiko	Tidak konsisten	Menggunakan skala <i>likelihood &amp; impact</i>
Evaluasi Risiko	Tidak ada prioritas	Menetapkan tingkat risiko (tinggi, sedang, rendah)
Penanganan Risiko	Reaktif	Menyusun rencana mitigasi formal
<i>Review</i> Risiko	Tidak berkala	Melakukan <i>review</i> risiko minimal satu tahun sekali

Rekomendasi utama mencakup perubahan tata kelola risiko dari yang bersifat insidental menjadi terstruktur melalui penyusunan kebijakan manajemen risiko yang disetujui pimpinan, penetapan *risk appetite*, serta pembentukan mekanisme pelaporan periodik. Pada sisi operasional, instansi disarankan untuk menyusun *risk register* aset TI, menggunakan skala analisis risiko yang konsisten, dan melakukan mitigasi secara proaktif. Melalui perbaikan pada aspek SDM dan keamanan ini, diharapkan tata kelola TI Diskominfo semakin baik dalam mendorong efisiensi organisasi dan meningkatkan mutu pelayanan publik bagi masyarakat.

#### 4. Kesimpulan dan Saran

Berdasarkan hasil penelitian manajemen risiko keamanan aset TI di Diskominfo Kabupaten Tangerang, dapat disimpulkan bahwa meskipun kesadaran terhadap pengelolaan risiko sudah terbentuk, penerapannya belum berjalan secara optimal. Hasil evaluasi pada domain EDM03 dan APO12 menunjukkan bahwa pelaksanaan manajemen risiko masih bersifat parsial dan belum didukung dokumentasi formal yang memadai. Kondisi ini menyebabkan adanya kesenjangan (*gap*) kapabilitas, di mana proses saat ini belum sepenuhnya terdefinisi dan terstandarisasi sesuai target COBIT

2019. Faktor utama yang menjadi kendala adalah keterbatasan kompetensi SDM dan rendahnya pemahaman pegawai terhadap praktik keamanan informasi. Sebagai langkah perbaikan, disarankan agar Diskominfo Kabupaten Tangerang meningkatkan kapabilitas manajemen risiko secara bertahap melalui penyusunan kebijakan dan prosedur baku yang terdokumentasi. Peningkatan kompetensi SDM melalui pelatihan dan sosialisasi berkala menjadi hal yang mendesak untuk meminimalkan risiko akibat faktor manusia. Selain itu, diperlukan mekanisme evaluasi dan pemantauan risiko secara periodik untuk memastikan langkah mitigasi berjalan efektif dan tetap selaras dengan tujuan strategis organisasi serta tata kelola TI yang berlaku.

#### 5. Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada Fakultas Ilmu Komputer, Universitas Esa Unggul, atas dukungan yang diberikan dalam penyelesaian penelitian ini. Penghargaan setinggi-tingginya juga disampaikan kepada instansi terkait dan rekan-rekan sejawat yang telah membantu proses pengumpulan serta pengolahan data sehingga penelitian ini dapat terselesaikan dengan baik

## 6. Daftar Pustaka

- Afdhani, R., & Soewito, B. (2024). Perancangan tata kelola TI menggunakan framework COBIT 2019 pada Pusat Data dan Informasi Kementerian XYZ. *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi*, 10(1), 22–33. <https://doi.org/10.34010/jtk3ti.v10i1.12365>
- Ariesta, A. D., & Perdanakusuma, A. R. (2022). Evaluasi tata kelola dan manajemen risiko teknologi informasi pada PT. MyECO Teknologi Nusantara menggunakan framework COBIT 2019 proses EDM03 dan APO12. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 6(12), 5736–5745.
- ISACA. (2019). *COBIT 2019 framework: Introduction and methodology*. ISACA.
- Jauhary, H., Pratiwi, G. E., Salim, A. Z., & Fitroh, F. (2022). Penerapan ISO27001 dalam menjaga dan meminimalisir risiko keamanan informasi: Literatur review. *Media Jurnal Informatika*, 14(1), 43. <https://doi.org/10.35194/mji.v14i1.1581>
- Miftakhatun, M. (2020). Analisis manajemen risiko teknologi informasi pada website Ecofo menggunakan ISO 31000. *Journal of Computer Science and Engineering*, 1(2), 128–146. <https://doi.org/10.36596/jcse.v1i2.76>
- Putra, S. C., & Wijaya, A. F. (2022). Analysis of information technology governance using COBIT 2019 framework (Case study: PT. Bangkit Anugerah Bersama). *Journal of Information Systems and Informatics*, 4(4), 1135–1151. <https://doi.org/10.51519/journalisi.v4i4.401>
- Ridwan, M., AM, S., Ulum, B., & Muhammad, F. (2021). Pentingnya penerapan literature review pada penelitian ilmiah. *Jurnal Masobi*, 2(1), 42. <https://doi.org/10.36339/jmas.v2i1.427>
- Rohman, A. F., Ambarwati, A., & Setiawan, E. (2020). Analisis manajemen risiko IT dan keamanan aset menggunakan metode Octave-S. *INTECOMS: Journal of Information Technology and Computer Science*, 3(2), 298–310. <https://doi.org/10.31539/intecom.v3i2.1854>
- Saputra, D. (2023). Evaluasi tata kelola teknologi informasi pada Inspektorat Kabupaten Pringsewu menggunakan framework COBIT 2019 dan balanced scorecard. *Jurnal Sistem Informasi*, 2(2), 11–18.
- Simanjuntak, C. R., Pratama, S. A., & Barovich, G. (2023). Remanajemen jaringan menggunakan framework NIST pada Perpustakaan Daerah Provinsi Sumatera Selatan. *Jurnal Teknologi Sistem Informasi*, 4(1), 152–163. <https://doi.org/10.35957/jtsi.v4i1.4796>