BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Identifikasi *Enterprise Goals*

Peneliti melakukan analisis dan pemetaan untuk menentukan *enterprise goals* yang relevan dengan permasalahan yang dihadapi, dengan mengacu pada pedoman COBIT 2019. Proses ini bertujuan untuk memastikan bahwa tujuan perusahaan yang ditetapkan selaras dengan tantangan yang ada, sehingga dapat memberikan solusi yang efektif dalam pengelolaan teknologi informasi.

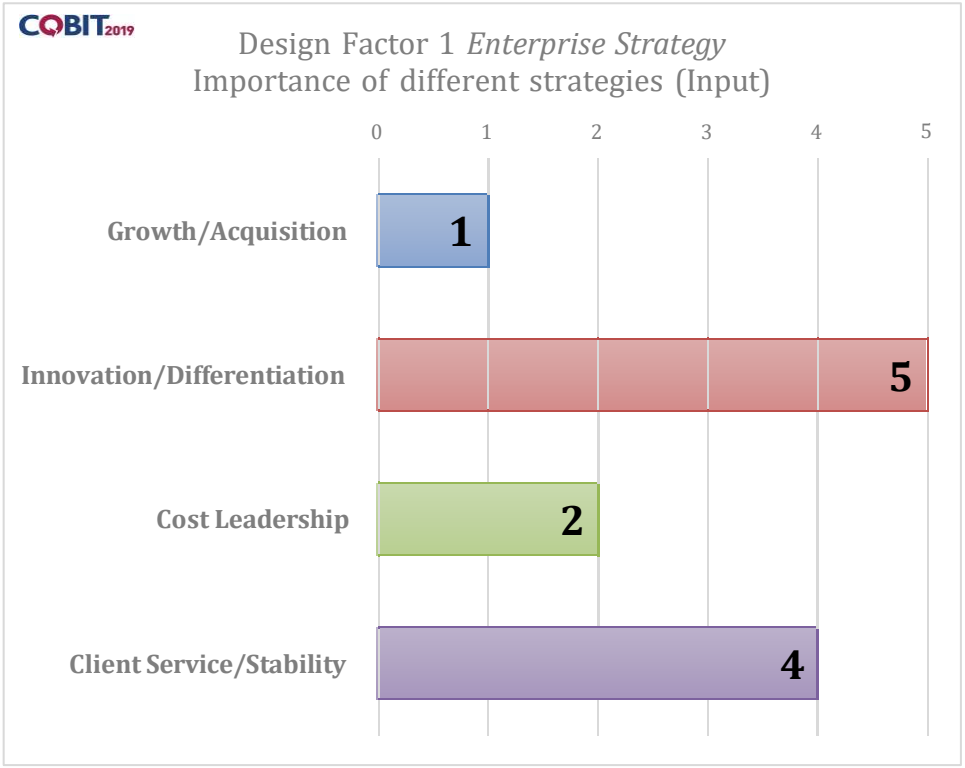
Latar belakang permasalahan yang telah diidentifikasi dirangkum dalam Tabel 4.1, yang berisi pemetaan antara permasalahan utama dengan tujuan strategis perusahaan. Dengan pendekatan ini, diharapkan solusi yang diterapkan dapat meningkatkan efisiensi serta efektivitas dalam pencapaian target organisasi sesuai dengan prinsip tata kelola yang baik.

Tabel 4 1 Latar Belakang Penelitian

No	Latar Belakang Penelitian
1	Bagaimana melakukan audit yang memastikan bahwa Simassadawan disampaikan dengan cara yang andal dan efisien, serta mendukung kebutuhan bisnis.
2	Bagaimana memastikan Simassadawan yang dibangun atau diakuisisi memenuhi kebutuhan bisnis dan diimplementasikan secara efektif.
3	Bagaimana memastikan bahwa Simassadawan berjalan sesuai dengan rencana dan mencapai tujuan yang diinginkan

1. Strategi Kelembagaan (*Enterprise Strategy*)

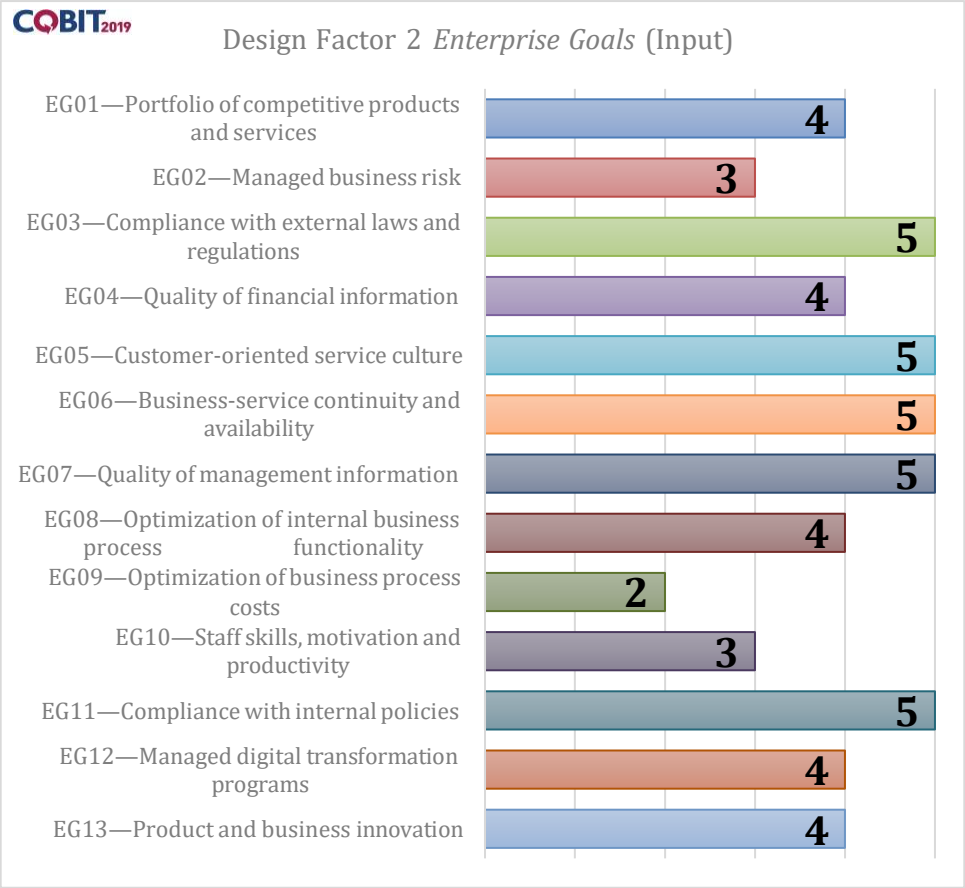
Berdasarkan analisis faktor desain pertama (*enterprise strategy*), strategi yang diterapkan oleh SIMASSADAWAN dalam pemanfaatan teknologi informasi difokuskan pada upaya peningkatan kualitas layanan *(client service/stability*).



Gambar 4 1 Enterprise Strategy

2. Tujuan Organisasi/Perusahaan (*Enterprise Goals*)

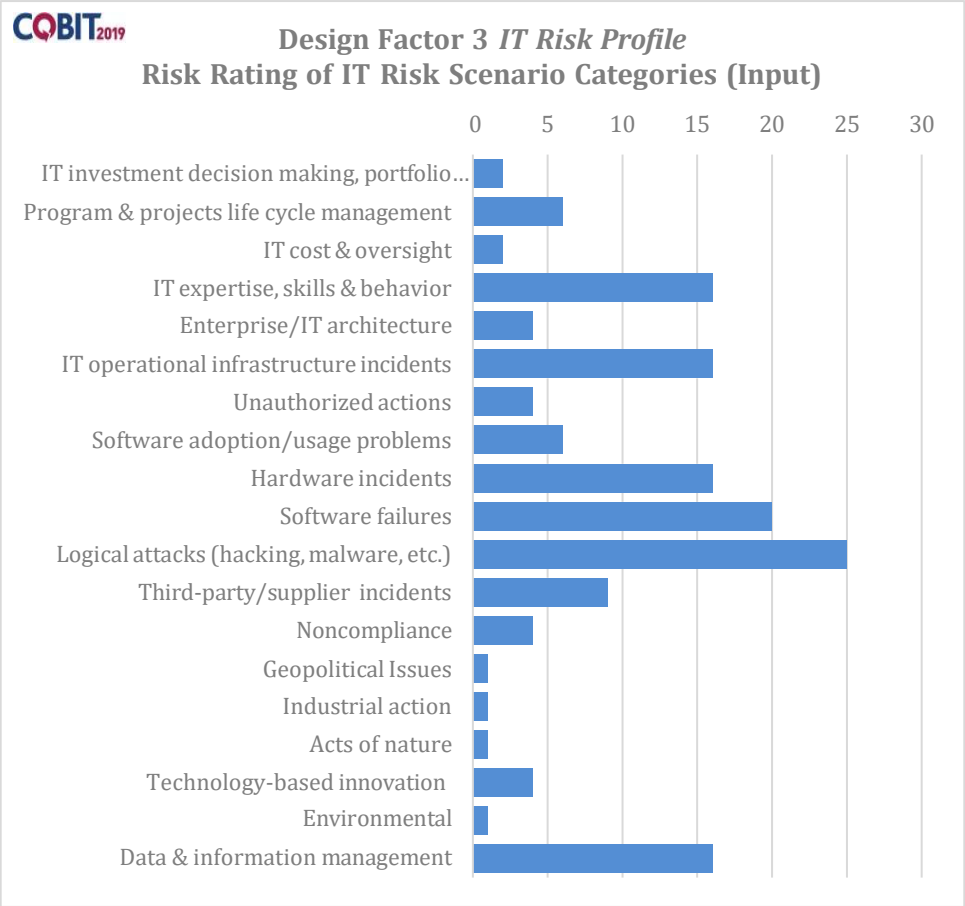
Dengan mempertimbangkan pemetaan faktor desain kedua (*enterprise goals*), tujuan utama yang ingin dicapai oleh perusahaan atau instansi adalah mengoptimalkan kinerja organisasi, meningkatkan efisiensi operasional, serta memastikan keberlanjutan dan pertumbuhan yang selaras dengan visi dan misi yang telah ditetapkan.



Gambar 4 2 Enterprise Goals

3. Profil Risiko Teknologi Informasi (*IT Risk Profile*)

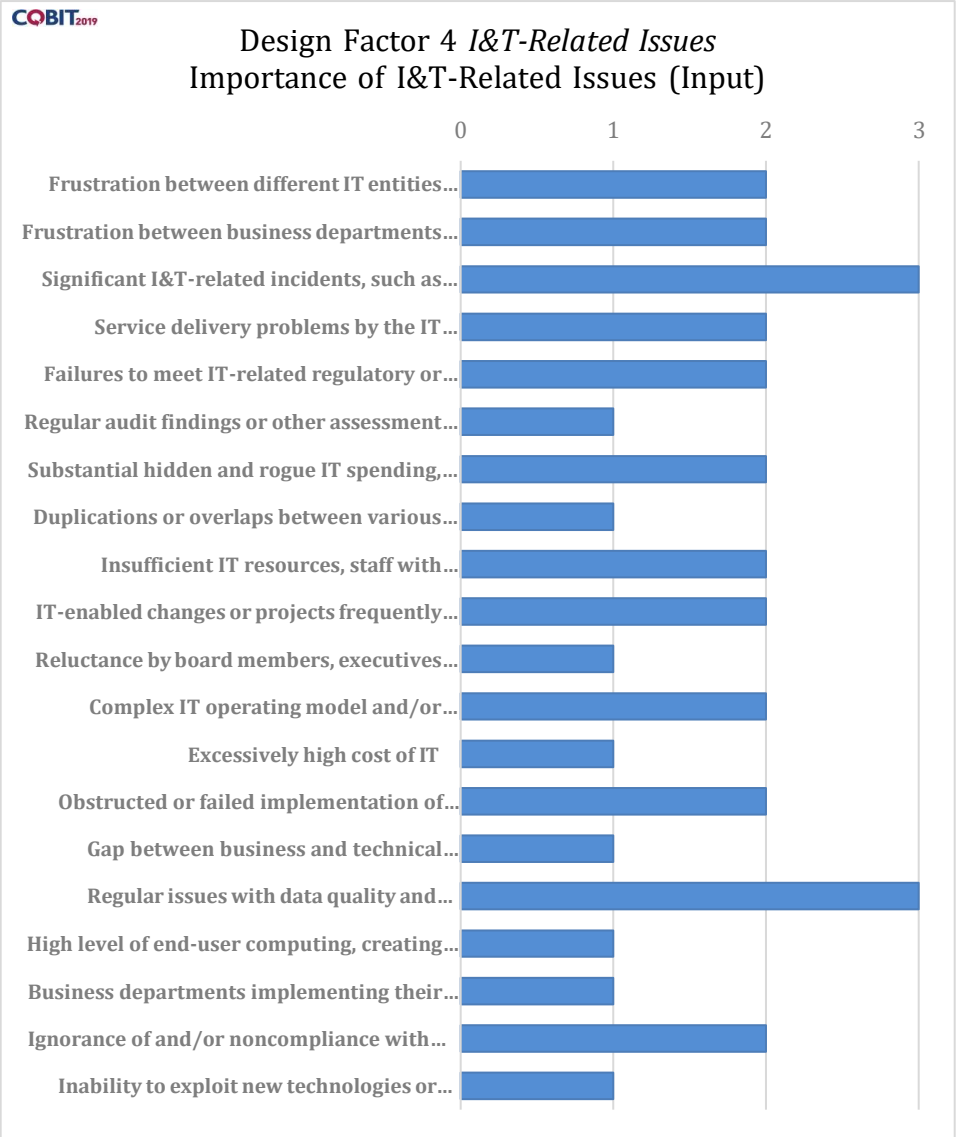
Berdasarkan pemetaan faktor desain ketiga (*IT risk profile*), identifikasi dan analisis risiko dalam pemanfaatan teknologi informasi menjadi aspek krusial bagi keberlangsungan operasional instansi. Risiko yang dapat timbul mencakup ancaman keamanan data, gangguan sistem, ketidaksesuaian infrastruktur dengan kebutuhan organisasi, serta potensi kesalahan manusia dalam pengelolaan teknologi. Oleh karena itu, diperlukan strategi mitigasi yang tepat, seperti penerapan kebijakan keamanan yang ketat, peningkatan kapasitas sumber daya manusia dalam bidang TI, serta penggunaan teknologi yang andal dan sesuai dengan standar keamanan informasi.



Gambar 4 3 *IT Risk Profile*

4. Isu Terkait Teknologi Informasi (*IT Related Issues*)

Berdasarkan pemetaan faktor desain keempat *I&T-Releate Issues* (Isu-isu terkait IT), menampilkan tingkat kepentingan berbagai isu terkait TI. Website Simassadawan memiliki dua isu serius yang menjadi perhatian khusus. Isu pertama merupakan insiden yang signifikan seperti kehilangan data, pelanggaran keamanan, dan aplikasi eror dan isu serius yang kedua menunjukan bahwa masalah terkait kualitas data dan integrasi data yang buruk dari berbagai sumber.



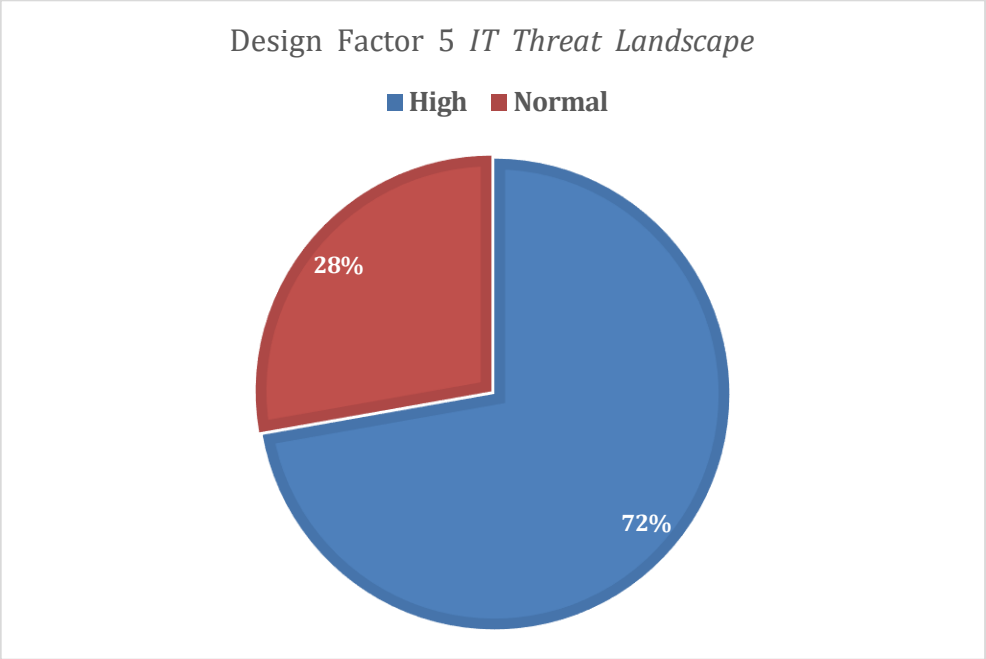
Gambar 4 4 *IT Related Issue*

5. Lanskap Ancaman Teknologi Informasi (*IT Threat Landscape*)

Berdasarkan pemetaan faktor desain kelima (*IT threat landscape*), berbagai ancaman terhadap teknologi informasi perlu diidentifikasi dan diantisipasi guna menjaga keamanan serta kelangsungan operasional organisasi. Ancaman yang dihadapi meliputi serangan siber seperti *malware*, *phishing*, *ransomware*, dan peretasan data yang dapat mengakibatkan kebocoran informasi sensitif. Selain itu,

risiko kegagalan sistem akibat kesalahan konfigurasi, kurangnya pemeliharaan perangkat lunak dan keras, serta ancaman bencana alam yang dapat merusak infrastruktur TI juga menjadi perhatian utama.

Untuk menghadapi tantangan ini, diperlukan langkah-langkah strategis seperti penerapan sistem keamanan berlapis, enkripsi data, pemantauan aktivitas jaringan secara *real-time*, serta edukasi kepada pengguna terkait praktik keamanan siber. Selain itu, organisasi perlu memiliki rencana pemulihan bencana (*disaster recovery plan*) yang efektif untuk memastikan operasional dapat tetap berjalan meskipun terjadi gangguan atau serangan terhadap sistem TI.



Gambar 4 5 *IT Thread Landscape*

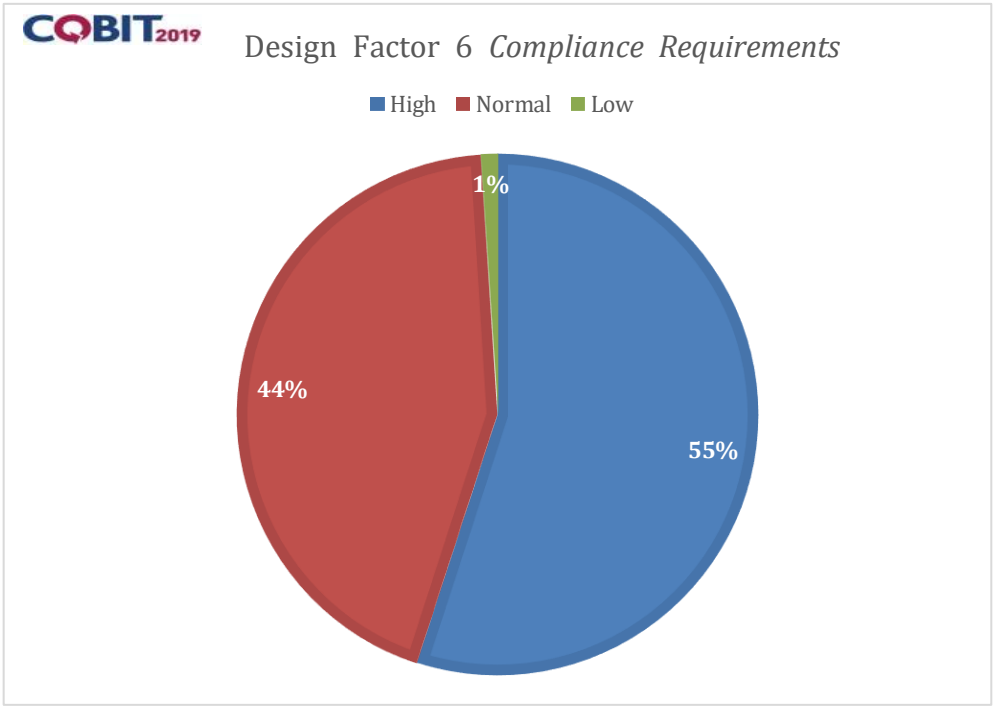
6. Persyaratan Kepatuhan (*Compliance Requirements*)

Berdasarkan pemetaan faktor desain keenam (*compliance requirements*), organisasi harus mematuhi berbagai regulasi dan standar yang berkaitan dengan pemanfaatan teknologi informasi. Kepatuhan ini mencakup aspek hukum, kebijakan internal,

serta standar industri yang bertujuan untuk memastikan keamanan, integritas, dan efisiensi dalam pengelolaan data serta sistem informasi.

Beberapa regulasi yang relevan dapat mencakup perlindungan data pribadi, keamanan siber, audit teknologi informasi, serta tata kelola TI yang sesuai dengan standar nasional maupun internasional seperti ISO 27001 atau regulasi pemerintah setempat. Kegagalan dalam memenuhi persyaratan ini dapat mengakibatkan sanksi hukum, denda, atau hilangnya kepercayaan dari pemangku kepentingan.

Oleh karena itu, organisasi perlu menerapkan kebijakan kepatuhan yang ketat, melakukan audit secara berkala, serta meningkatkan kesadaran dan pemahaman pegawai terhadap regulasi yang berlaku. Selain itu, kerja sama dengan regulator dan pihak eksternal yang berwenang juga penting untuk memastikan bahwa sistem TI yang digunakan tetap sesuai dengan peraturan dan standar yang berlaku.



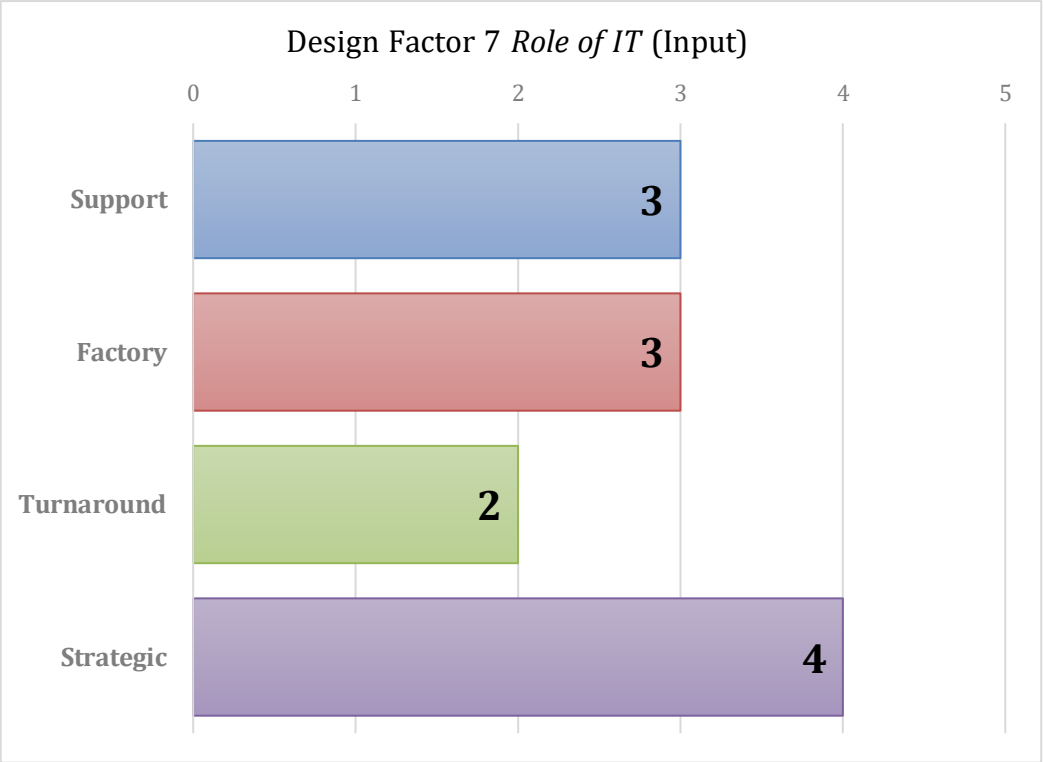
Gambar 4 6 *Compliance Requirements*

7. Peran Teknologi Informasi (*Role of IT*)

Berdasarkan pemetaan faktor desain ketujuh (*role of IT*), teknologi informasi memiliki peran strategis dalam mendukung operasional, efisiensi, dan inovasi di dalam organisasi. TI tidak hanya berfungsi sebagai alat bantu dalam pengolahan data dan komunikasi, tetapi juga menjadi faktor kunci dalam meningkatkan produktivitas, mempercepat proses bisnis, serta memungkinkan pengambilan keputusan yang lebih akurat berbasis data.

Di era transformasi digital, peran TI semakin berkembang dalam berbagai aspek, termasuk otomatisasi proses kerja, integrasi sistem antar unit, peningkatan pengalaman pengguna melalui layanan berbasis digital, serta penguatan keamanan data dan informasi. Dengan pemanfaatan teknologi seperti *cloud computing*, *big data analytics*, kecerdasan buatan (AI), dan *Internet of Things* (IoT), organisasi dapat lebih adaptif terhadap perubahan dan meningkatkan daya saingnya.

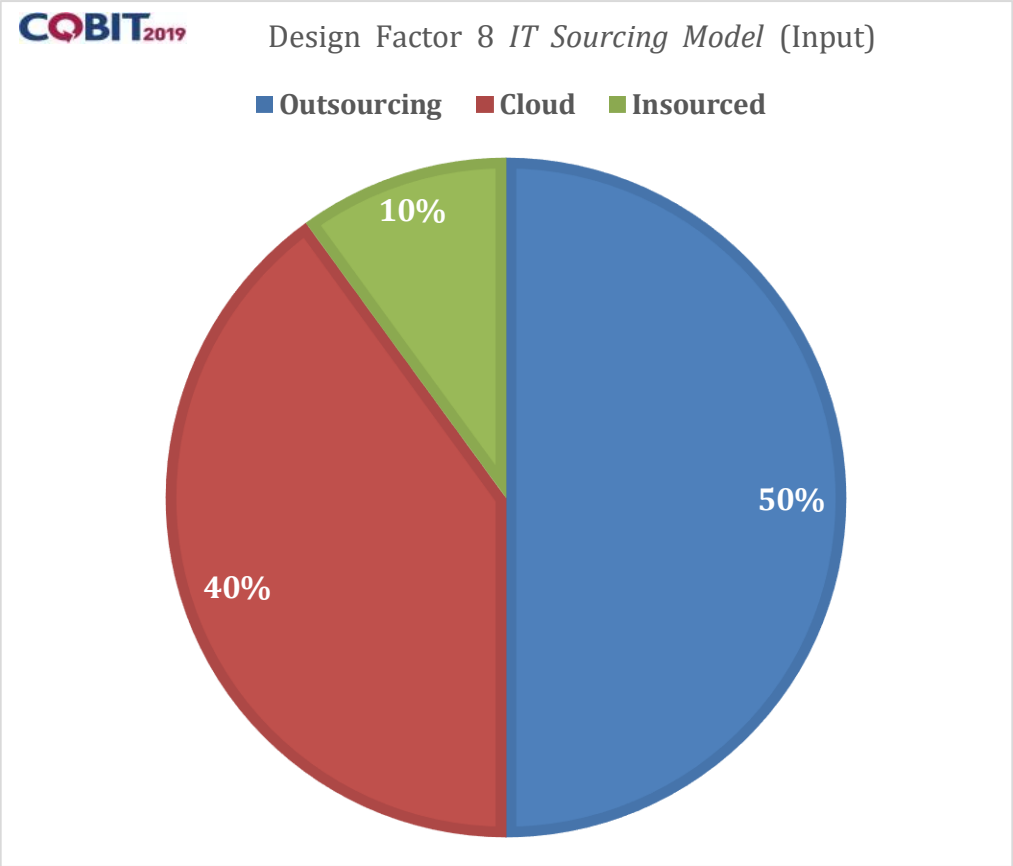
Untuk mengoptimalkan peran TI, diperlukan strategi yang selaras dengan tujuan organisasi, investasi yang tepat dalam infrastruktur dan sumber daya manusia, serta pengelolaan yang efektif guna memastikan teknologi dapat memberikan nilai tambah yang signifikan bagi keberlanjutan dan pertumbuhan organisasi.



Gambar 4 7 *Role of IT*

8. Model Sumber Teknologi Informasi (*Sourcing Model IT*)

Berdasarkan pemetaan faktor desain kedelapan (*sourcing model IT*), pemilihan model pengadaan dan pengelolaan sumber daya teknologi informasi menjadi aspek krusial dalam mendukung operasional serta strategi organisasi. Model sourcing TI mencakup berbagai pendekatan, mulai dari pengembangan internal, penggunaan layanan pihak ketiga, hingga kombinasi keduanya yang disesuaikan dengan kebutuhan organisasi.

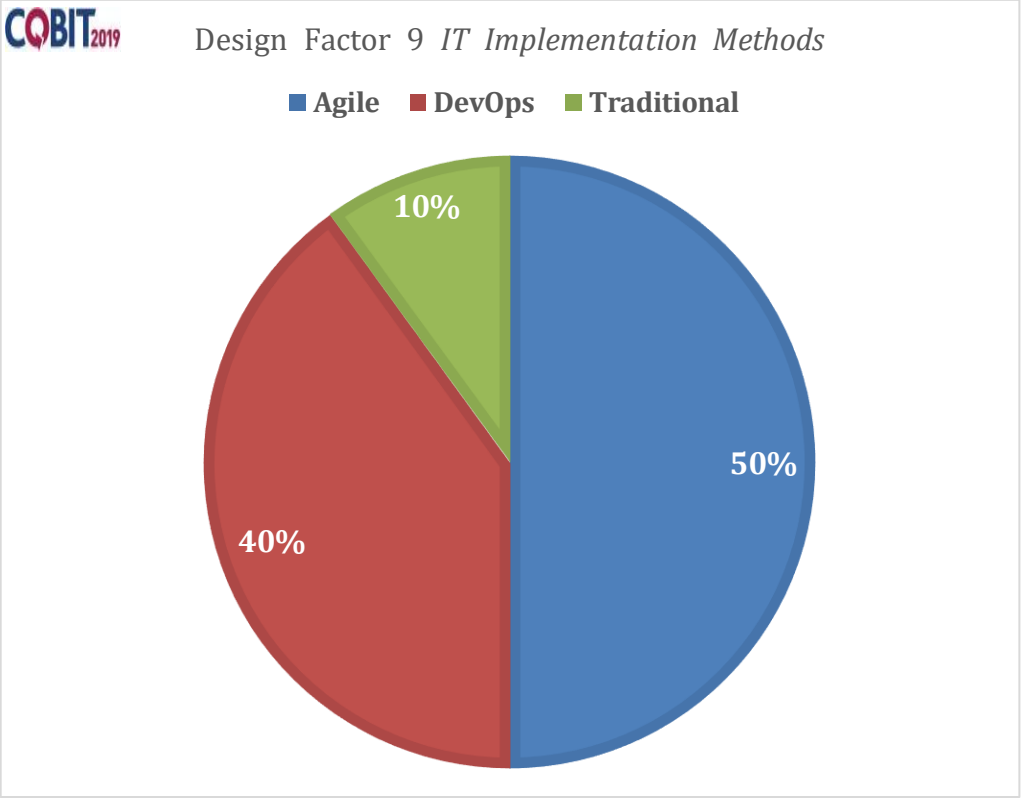


Gambar 4 8 *Sourcing Model IT*

9. Metode Implementasi Teknologi Informasi (*IT Implementation Methods*)

Berdasarkan pemetaan faktor desain kesembilan (*IT implementation methods*), penerapan teknologi informasi dalam organisasi dapat dilakukan melalui berbagai pendekatan yang disesuaikan dengan kebutuhan dan tujuan strategis. Metode yang umum digunakan meliputi *waterfall*, yang menekankan pendekatan berurutan dan sistematis; *agile*, yang lebih fleksibel dengan iterasi cepat untuk meningkatkan responsivitas terhadap perubahan; serta devOps, yang mengintegrasikan pengembangan dan operasional untuk meningkatkan efisiensi dan keandalan sistem. Pemilihan metode implementasi harus mempertimbangkan kompleksitas

proyek, ketersediaan sumber daya, serta kecepatan adopsi teknologi guna memastikan bahwa penerapan TI berjalan efektif,

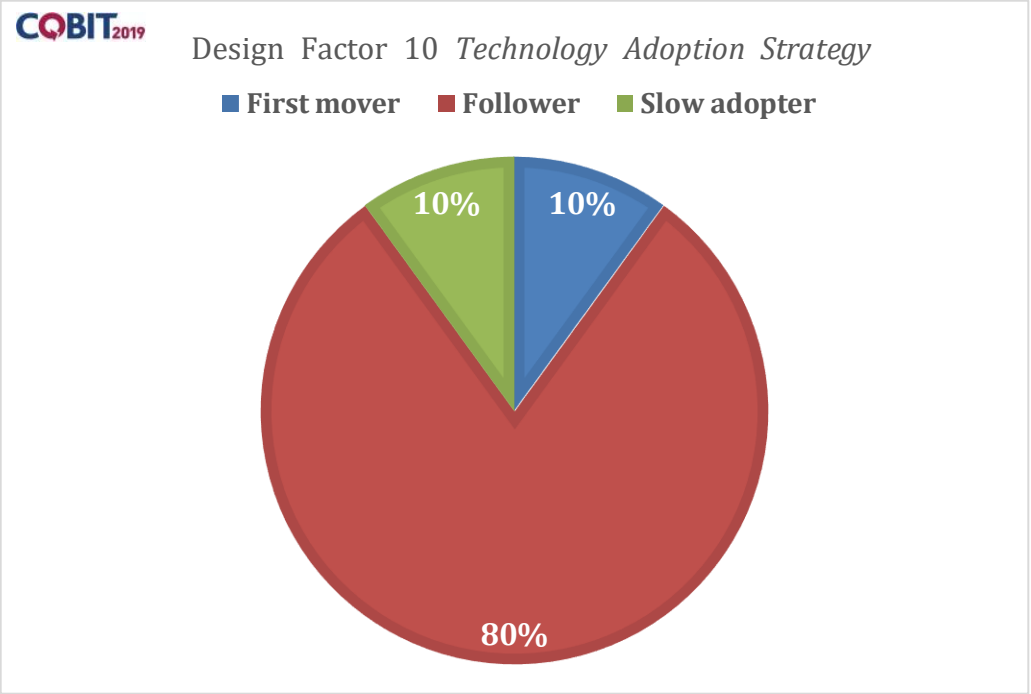


Gambar 4 9 *IT Implementation Methods*

10. Strategi Adopsi Teknologi (*Technology Adoption Strategy*)

Berdasarkan pemetaan faktor desain kesepuluh (*technology adoption strategy*), terdapat tiga pendekatan utama dalam pengadopsian teknologi, yaitu *first mover*, *follower*, dan *slow adopter*. Organisasi yang memilih strategi *first mover* akan menjadi pelopor dalam penerapan teknologi baru, yang dapat memberikan keunggulan kompetitif tetapi juga menghadapi risiko tinggi terkait biaya dan ketidakpastian. Sementara itu, strategi *follower* memungkinkan organisasi untuk mengadopsi teknologi setelah melihat keberhasilan dan kegagalan dari para pelopor, sehingga mengurangi risiko namun tetap dapat bersaing di pasar. Di sisi

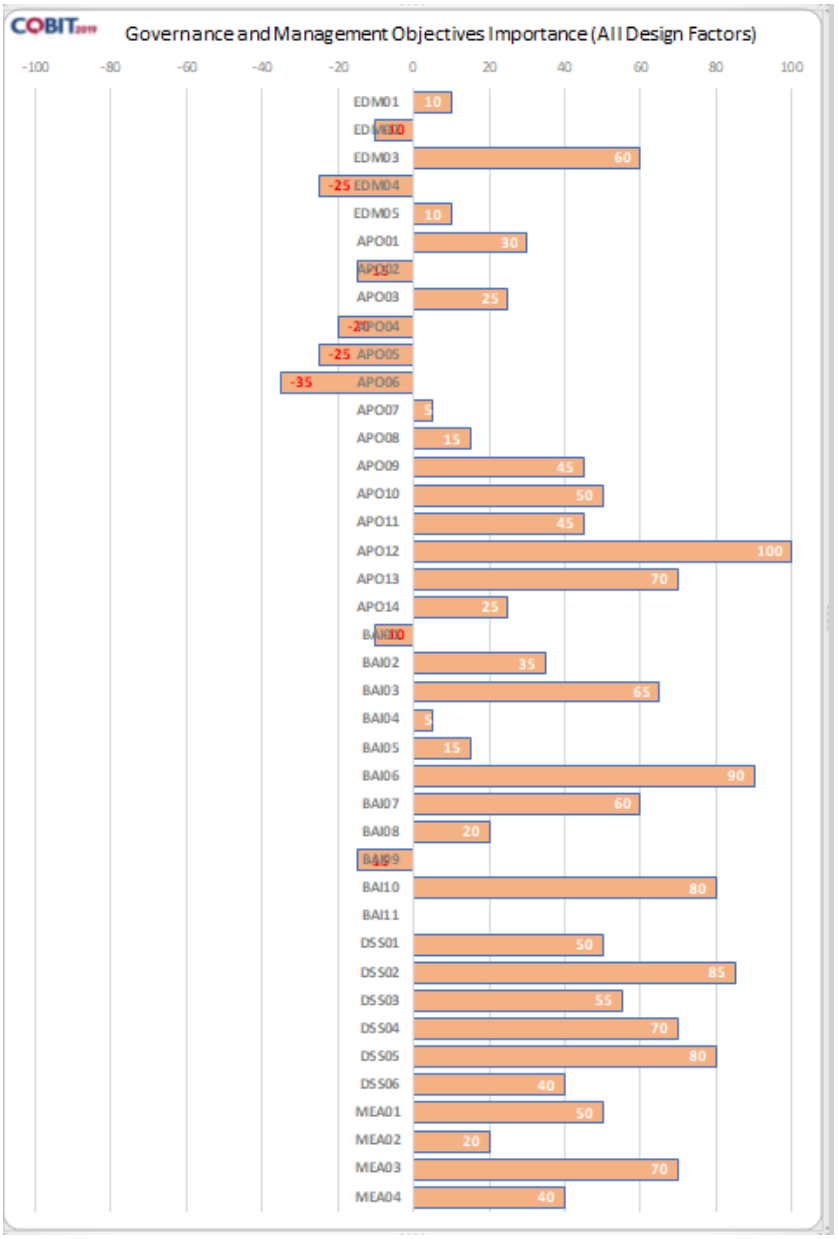
lain, strategi *slow adopter* lebih konservatif, di mana organisasi menunda adopsi teknologi hingga benar-benar matang dan terbukti stabil, yang biasanya lebih mengutamakan efisiensi biaya serta minimnya gangguan operasional. Pemilihan strategi ini harus disesuaikan dengan kebutuhan, sumber daya, serta tujuan jangka panjang organisasi agar teknologi yang diadopsi benar-benar memberikan nilai tambah.



Gambar 4 10 *Technology Adoption Strategy*

4.1.1 Design Factor for Objectives Domain

Berikut hasil *mapping* dari semua design factor pada SIMASSADAWAN.



Gambar 4 11 Governance and Management Objectives Importance (All Design Factors)

Gambar diatas merupakan diagram batang yang menunjukkan tingkat kepentingan tujuan Tata Kelola dan Manajemen COBIT 2019 berdasarkan semua faktor desain.

Dari hasil pemetaan design factor dapat disimpulkan domain objectif terpilih dalam melakukan asesmen tata kelola TI pada Simassadawan adalah APO12, BAI06, BAI10, DSS02 dan DSS05 (dengan kriteria nilai kepentingan >75)
Dari gambar ini, beberapa proses dengan kepentingan tertinggi meliputi:

- APO12 (100) – Manajemen Risiko TI dianggap sebagai prioritas utama.
- BAI06 (90) – Pengelolaan perubahan teknologi memiliki tingkat kepentingan yang tinggi.
- DSS02 (85) – Pengelolaan permintaan layanan dan insiden menjadi aspek penting.
- BAI10 (80) & DSS05 (80) – Menunjukkan kebutuhan kuat dalam implementasi layanan dan keamanan operasional.

Sementara itu, beberapa proses memiliki nilai negatif, seperti EDM04 (-25), APO04 (-20), APO05 (-25), dan APO06 (-35), yang menunjukkan bahwa aspek- aspek ini memiliki tingkat kepentingan yang lebih rendah dibandingkan faktor lainnya dalam konteks desain tata kelola organisasi ini.
Secara keseluruhan, diagram ini membantu dalam memahami area mana yang perlu mendapatkan perhatian lebih dalam perencanaan tata kelola dan manajemen TI, dengan fokus utama pada keamanan, manajemen risiko, dan operasional layanan.

4.2 Hasil Identifikasi *Related Goals*

Berdasarkan hasil pemetaan latar belakang penelitian dengan *enterprise goals*, langkah berikutnya adalah memetakan serta menetapkan IT *related goals* yang disesuaikan dengan *enterprise goals* yang telah dipilih sebelumnya, dengan merujuk pada pedoman COBIT 2019.

Setelah IT related goals dipetakan dan diselaraskan dengan *enterprise goals*, hasil pemetaan tersebut kemudian didokumentasikan.

Tabel 4 2 *IT Related Goals (Customer, Intern, Learning & Growth)*

Information And Related Technology Goal	***Customer***	***Internal***	***Learning & Growth***
Risiko bisnis terkelola, yaitu kejadian dalam bisnis seperti kegagalan proses dalam sistem dapat teratasi atau dikelola dengan baik. (DSS05, APO12)		✓	
Keterampilan, motivasi, dan produktivitas staf, yaitu dibutuhkan sumber daya yang kompeten untuk mengelola TI dengan baik. (BAI06, APO12)		✓	
Inovasi produk dan bisnis, yaitu dibutuhkan ide baru untuk menyesuaikan diri terhadap perkembangan teknologi. (BAI10)			✓
Mengelola sumber daya manusia serta memantau alokasi dan optimalisasi sumber daya sesuai dengan prioritas. (BAI06, APO12)		✓	
Memantau strategi penyediaan TI, strategi arsitektur, sumber daya TI, dan kemampuan untuk memenuhi kebutuhan saat ini dan masa depan. (BAI10, APO12)		✓	
Memantau kinerja sumber daya terhadap target, menganalisis penyebab penyimpangan, dan melakukan tindakan perbaikan. (BAI06, APO12)		✓	
Melaksanakan perbaikan berkesinambungan dari proses dan kematangannya untuk mendukung tujuan bisnis. (BAI10, APO12)			✓

Kesadaran, komunikasi, dan pemahaman tujuan TI kepada pemangku kepentingan yang tepat dan pengguna. (DSS02, APO12)			✓
Meningkatkan efisiensi dan efektivitas, misalnya melalui pelatihan, dokumentasi standar, dan otomatisasi proses. (BAI06, APO12)			✓
Mendefinisikan, memelihara, dan menyediakan alat serta pedoman untuk keamanan serta kontrol informasi. (DSS05, APO12)		✓	
Menentukan penempatan fungsi TI dan memperoleh kesepakatan. (DSS02, APO12)		✓	

Setelah melakukan pemetaan dan penetapan Tujuan Terkait TI yang disesuaikan dengan tujuan perusahaan, hasil pemetaan tujuan perusahaan dan tujuan terkait TI selanjutnya disajikan dalam Tabel 4.3

Tabel 4 3 Pemetaan *Enterprise Goals* terhadap *IT Related*

Enterprise Goals	***IT-Related Goals***	***DSS02 (Manage Service Requests and Incidents)***	***DSS05 (Manage Security Services)***	***BAI06 (Manage Changes)***	***BAI10 (Manage Configuration)***	***APO12 (Manage Risk)***
1. Pemenuhan kebutuhan *stakeholder* (*Stakeholder Value of Business Investments*)	Layanan TI yang cepat dan efektif dalam menangani permintaan serta insiden.	✓	✓	✓	✓	✓
2. Kepatuhan terhadap peraturan dan hukum (*Compliance with External Laws and Regulations*)	Sistem TI yang selaras dengan standar kepatuhan dan keamanan data.	✓	✓		✓	✓
3. Pengelolaan risiko bisnis yang optimal (*Managed Business Risk*)	Implementasi kebijakan dan prosedur keamanan TI yang kuat untuk meminimalkan risiko.		✓	✓	✓	✓
4. Optimalisasi biaya layanan TI (*Optimized IT Costs*)	Pengelolaan insiden dan permintaan layanan TI secara efisien untuk menekan biaya operasional.	✓			✓	✓

5. Kualitas layanan TI yang andal dan efisien (*Reliable and Efficient IT Service Delivery*)	Kemampuan sistem dalam merespons insiden serta pengelolaan konfigurasi yang optimal.	✓		✓	✓	✓
6. Inovasi teknologi untuk mendukung pertumbuhan bisnis *(Business Service Continuity and Availability*)	Peningkatan proses pemantauan layanan serta keamanan dalam infrastruktur TI.		✓	✓	✓	✓
7. Manajemen SDM yang efektif dalam TI (*Skilled and Motivated Personnel*)	Peningkatan kompetensi tim dalam menangani insiden, perubahan, dan konfigurasi TI.	✓	✓	✓	✓	✓
8. Keamanan informasi dan perlindungan data (*Security of Information and Processing Infrastructure*)	Penguatan strategi keamanan TI dan pengelolaan perubahan yang adaptif.		✓	✓	✓	✓

Penjelasan Tabel *Enterprise Goals* dan IT *Related Goals*

Tabel 4 4 Tabel *Enterprise Goals* dan *IT Related Goals*

Enterprise Goals	***IT Related Goals***	***DSS02 (Manage Service Requests and Incidents)***	***DSS05 (Manage Security Services)***	***BAI06 (Manage Changes)***	***BAI10 (Manage Configuration)***	***APO12 (Manage Risk)***
1. Pemenuhan kebutuhan stakeholder (Stakeholder Value of Business Investments)	Keamanan informasi dan pengelolaan risiko bisnis yang baik.	✓	✓	✓	✓	✓
2. Kepatuhan terhadap peraturan dan hukum (Compliance with External Laws and Regulations)	Sistem TI yang mendukung kepatuhan regulasi dan keamanan data.	✓	✓		✓	✓
3. Pengelolaan risiko bisnis yang optimal (Managed Business Risk)	Implementasi kebijakan keamanan TI untuk mengurangi risiko.		✓	✓	✓	✓
4. Optimalisasi biaya layanan TI (Optimized IT Costs)	Efisiensi dalam penyelesaian insiden dan permintaan layanan TI.	✓		✓	✓	✓
5. Kualitas layanan TI yang andal dan efisien (Reliable and Efficient IT Service Delivery)	Respons cepat terhadap insiden dan permasalahan TI.	✓	✓	✓	✓	✓
6. Inovasi teknologi untuk mendukung pertumbuhan bisnis (Business Service Continuity and Availability)	Peningkatan proses pemantauan performa sistem dan keamanan TI.	✓	✓	✓	✓	✓

7. Manajemen SDM yang efektif dalam TI (Skilled and Motivated Personnel)	Peningkatan kompetensi karyawan dalam menangani keamanan dan insiden TI.	✓	✓	✓	✓	✓
8. Keamanan informasi dan perlindungan data (Security of Information and Processing Infrastructure)	Implementasi kebijakan keamanan yang kuat dan responsif terhadap ancaman.	✓	✓	✓	✓	

Penjelasan Tabel Pemetaan *Enterprise Goals* dengan *IT-Related Goals*

Tabel ini memetakan tujuan perusahaan (*Enterprise Goals*) terhadap tujuan TI (*IT-Related Goals*) yang dikelola melalui beberapa domain pengelolaan TI, yaitu:

- DSS02 (*Manage Service Requests and Incidents*) → Mengelola permintaan layanan dan insiden TI.
- DSS05 (*Manage Security Services*) → Mengelola keamanan TI dan perlindungan data.
- BAI06 (*Manage Changes*) → Mengelola perubahan sistem untuk meminimalkan risiko.
- BAI10 (*Manage Configuration*) → Mengelola konfigurasi TI guna menjaga keandalan layanan.
- APO12 (*Manage Risk*) → Mengelola risiko TI dan memastikan keberlanjutan bisnis.

Berikut adalah penjelasan hubungan masing-masing *Enterprise Goals dengan IT-Related Goals*:

1. Pemenuhan kebutuhan *stakeholder* (*Stakeholder Value of Business Investments*)
    - Perusahaan perlu memastikan bahwa investasi di bidang TI memberikan nilai tambah bagi *stakeholder*.

- DSS02: Layanan TI yang cepat dan responsif memastikan kepuasan pengguna.
- DSS05: Pengelolaan keamanan yang baik melindungi sistem dari ancaman yang dapat mengganggu nilai bisnis.
- BAI06: Manajemen perubahan yang baik mencegah gangguan operasional saat melakukan perubahan sistem.
- BAI10: Pengelolaan konfigurasi yang tepat memastikan stabilitas sistem TI yang mendukung kebutuhan bisnis.
- APO12: Risiko terkait investasi TI harus dikelola dengan baik agar tidak merugikan bisnis.

2. Kepatuhan terhadap peraturan dan hukum (*Compliance with External Laws and Regulations*)

- Sistem TI harus mendukung kepatuhan terhadap regulasi eksternal serta menjaga keamanan data.
- DSS02: Mengelola permintaan layanan yang terkait dengan kepatuhan regulasi.
- DSS05: Memastikan sistem TI memiliki kontrol keamanan yang mematuhi regulasi.
- BAI10: Pengelolaan konfigurasi yang baik membantu memastikan sistem tetap sesuai dengan standar regulasi.
- APO12: Manajemen risiko memastikan bahwa kepatuhan terhadap regulasi diperhitungkan dan dipantau secara aktif.

3. Pengelolaan risiko bisnis yang optimal (*Managed Business Risk*)

- Tujuan ini bertujuan untuk mengurangi risiko bisnis yang terkait dengan layanan TI.
- DSS05: Pengelolaan keamanan TI membantu meminimalkan risiko serangan siber dan kebocoran data.
- BAI06: Manajemen perubahan yang terkontrol mengurangi risiko kegagalan sistem saat perubahan diterapkan.
- BAI10: Konfigurasi yang tepat memastikan bahwa sistem berjalan sesuai standar yang telah ditetapkan.

- APO12: Manajemen risiko menjadi aspek utama dalam memastikan bahwa ancaman terhadap bisnis dapat diminimalkan.

4. Optimalisasi biaya layanan TI (*Optimized IT Costs*)
    - Efisiensi biaya dalam layanan TI sangat penting untuk mengurangi pengeluaran yang tidak perlu.
    - DSS02: Pengelolaan insiden yang baik mengurangi biaya akibat gangguan layanan yang berulang.
    - BAI06: Mengelola perubahan dengan baik menghindari pengeluaran yang tidak efisien akibat implementasi perubahan yang buruk.
    - BAI10: Konfigurasi yang optimal memastikan bahwa sumber daya TI digunakan dengan efisien.
    - APO12: Manajemen risiko membantu mengidentifikasi dan mengurangi biaya yang tidak perlu akibat ancaman atau kegagalan layanan TI.
5. Kualitas layanan TI yang andal dan efisien (*Reliable and Efficient IT Service Delivery*)
    - Perusahaan perlu memastikan bahwa layanan TI dapat diandalkan dan efisien.
    - DSS02: Layanan responsif terhadap insiden membantu menjaga ketersediaan layanan TI.
    - DSS05: Keamanan layanan TI membantu melindungi data dan sistem dari ancaman.
    - BAI06: Pengelolaan perubahan yang baik menghindari gangguan layanan akibat implementasi yang buruk.
    - BAI10: Pengelolaan konfigurasi memastikan bahwa sistem tetap stabil dan berjalan dengan optimal.
    - APO12: Manajemen risiko membantu dalam menjaga keberlanjutan layanan TI dengan mengidentifikasi dan memitigasi potensi gangguan.
6. Inovasi teknologi untuk mendukung pertumbuhan bisnis (*Business Service Continuity and Availability*)
    - Perusahaan harus terus berinovasi untuk meningkatkan keberlanjutan bisnis.

- DSS02: Layanan TI harus mampu menangani permintaan terkait pengembangan dan inovasi teknologi.
- DSS05: Keamanan sistem harus tetap menjadi prioritas dalam penerapan teknologi baru.
- BAI06: Pengelolaan perubahan membantu memastikan bahwa inovasi teknologi diimplementasikan tanpa risiko besar.
- BAI10: Konfigurasi yang baik mendukung kelangsungan operasional sistem yang baru diimplementasikan.
- APO12: Manajemen risiko membantu menilai dampak inovasi teknologi sebelum diterapkan ke dalam sistem produksi.

7. Manajemen SDM yang efektif dalam TI (*Skilled and Motivated Personnel*)
    - Pengelolaan SDM yang baik dalam bidang TI penting untuk memastikan layanan berjalan optimal.
    - DSS02: Tim TI harus terampil dalam menangani permintaan layanan dan insiden.
    - DSS05: Karyawan harus memiliki pemahaman mendalam mengenai keamanan sistem.
    - BAI06: SDM harus mampu mengelola perubahan dengan efektif dan meminimalkan risiko.
    - BAI10: Pengelolaan konfigurasi yang baik memerlukan tim dengan keahlian teknis yang kuat.
    - APO12: Manajemen risiko mencakup peningkatan kompetensi SDM dalam mengidentifikasi dan menangani ancaman TI.
8. Keamanan informasi dan perlindungan data (*Security of Information and Processing Infrastructure*)
    - Perusahaan harus memastikan bahwa informasi dan data mereka terlindungi dari ancaman.
    - DSS02: Tim TI harus mampu menangani insiden yang berkaitan dengan pelanggaran keamanan.
    - DSS05: Sistem keamanan harus terus diperbarui untuk menghadapi ancaman siber yang berkembang.

- BAI06: Perubahan sistem harus dilakukan dengan memperhatikan aspek keamanan informasi.
- BAI10: Konfigurasi sistem harus mengikuti standar keamanan untuk menghindari potensi eksploitasi.
- APO12: Manajemen risiko memastikan bahwa ancaman keamanan dapat diidentifikasi dan diminimalkan sebelum berdampak besar pada bisnis.

4.3 Identifikasi Domain COBIT 2019

Berdasarkan hasil pemetaan *IT related goals* terhadap proses COBIT 2019, domain yang akan digunakan dalam penelitian ini yaitu padatabel 4.5

Tabel 4 5 Pemetaan *IT Related Goals* terhadap proses COBIT 2019

No	**Domain COBIT 2019**	**Deskripsi**	***Enterprise Goals & IT Related Goals***	**Implementasi dalam Organisasi**
1	DSS02 - *Manage Service Requests and Incidents*	Mengelola permintaan layanan dan menangani insiden TI untuk meningkatkan efisiensi dan keandalan layanan.	Optimasi biaya TI	Menggunakan *IT Service Management* (ITSM) untuk meningkatkan efisiensi.
			Keandalan layanan TI	Menyediakan sistem respons cepat terhadap insiden untuk meminimalkan dampak pada bisnis.

2	DSS05 - *Manage Security Services*	Mengelola keamanan layanan TI untuk melindungi sistem dari ancaman dan memastikan kepatuhan regulasi.	Keamanan informasi	Menyusun kebijakan keamanan informasi sesuai standar dan regulasi.
			Kepatuhan hukum	Melakukan audit berkala dan pemantauan keamanan secara proaktif.
3	BAI06 - *Manage Changes*	Mengelola perubahan sistem TI untuk memastikan transisi yang aman dan mengurangi risiko operasional.	Keandalan layanan TI	Menerapkan *Change Management* untuk memastikan perubahan tidak mengganggu operasional.
			Inovasi teknologi	Mengoptimalkan proses perubahan untuk mendukung perkembangan bisnis yang lebih cepat.

4	BAI10 - *Manage Configuration*	Mengelola konfigurasi sistem TI untuk memastikan bahwa seluruh komponen terdokumentasi dan dapat diandalkan.	Efektivitas SDM TI	Menggunakan alat *Configuration Management Database* (CMDB) untuk mengelola aset TI.
			Peningkatan keamanan informasi	Memastikan konfigurasi sistem selalu sesuai dengan standar keamanan dan praktik terbaik.
5	APO12 - *Manage Risk*	Mengelola risiko TI untuk memastikan keberlanjutan bisnis dan meminimalkan dampak negatif dari ancaman potensial.	Manajemen risiko bisnis	Mengembangkan strategi mitigasi risiko untuk mengurangi kemungkinan gangguan operasional.
			Kepatuhan terhadap regulasi	Melakukan identifikasi dan evaluasi risiko secara berkala guna memastikan kepatuhan terhadap peraturan yang berlaku.

			Keamanan dan ketahanan TI	Menerapkan pendekatan berbasis risiko untuk memastikan perlindungan terhadap ancaman siber dan kegagalan sistem.

Tabel ini memberikan gambaran jelas tentang bagaimana domain Cobit 2019 dapat digunakan untuk mendukung tujuan bisnis dan bagaimana implementasinya dalam organisasi.

Ringkasan proses Cobit 2019 yang diperoleh dari pemetaan latar belakang masalah terhadap *IT Related Goals* dan Proses COBIT 2019 dapat ditemukan pada Tabel 4.6

Tabel 4 6 Domain COBIT 2019 pada Penelitian

Domain	**Proses Cobit 2019**
APO	APO12
DSS	DSS02,DSS05
BAI	BAI06, BAI10

4.4 RACI *Chart*: Identifikasi Responden

Dalam penelitian ini, responden yang dilibatkan terdiri dari beberapa pihak yang memiliki peran penting dalam pengelolaan dan penggunaan SIMASSADAWAN

Tabel 4 7 *RACI Chart*

Fungsi / Proses	Bupati	Diskominfo	SKPD	BPS	Masyarakat
Penetapan Kebijakan Satu Data	A	R	C	C	I
Pengelolaan Portal Simassadawan	I	R	C	C	I
Pengumpulan dan Validasi Data	I	R	R	C	I
Publikasi dan Diseminasi Data	I	R	C	C	I
Penggunaan Data untuk Perencanaan	I	C	R	C	I

Keterangan RACI:

R (Responsible) : Bertanggungjawab dalam menyelesaikan tugas

A (Accountable) : Bertanggungjawab penuh terhadap hasil akhir

C (Consulted) : Memberikan konsultasi, saran, dan pendapat

I (Informed) : Mendapatkan informasi dan perkembangan terkait

RACI Chart terpilih adalah SKPD yang terdiri dari 33 OPD dan 15 Kecamatan yang ada pada Kabupaten Way Kanan sehingga total jumlah responden dalam kuisioner adalah 48 responden.

Kuesioner dalam penelitian ini menggunakan framework COBIT 2019 dan disusun berdasarkan domain berikut:

Tabel 4 8 Tabel Kuisioner

Domain	Pertanyaan	1	2	3	4	5
APO12 – *Manage Risk*	Organisasi memiliki kebijakan formal dalam mengelola risiko TI.	☐	☐	☐	☐	☐
APO12 – *Manage Risk*	Risiko TI dievaluasi secara berkala untuk mengantisipasi potensi ancaman.	☐	☐	☐	☐	☐
APO12 – *Manage Risk*	Ada sistem pemantauan yang dapat mendeteksi risiko sebelum menyebabkan gangguan.	☐	☐	☐	☐	☐
APO12 – *Manage Risk*	Mitigasi risiko terdokumentasi dengan baik dan mudah diakses oleh tim terkait.	☐	☐	☐	☐	☐
DSS02 – *Manage Service Requests and Incidents*	Tim TI merespons permintaan layanan dalam waktu yang telah ditetapkan.	☐	☐	☐	☐	☐
DSS02 – *Manage Service Requests and Incidents*	Ada sistem tiket otomatis yang membantu dalam menangani insiden dengan cepat.	☐	☐	☐	☐	☐
DSS02 – *Manage Service Requests and Incidents*	Organisasi memiliki prosedur yang jelas dalam menangani insiden kritis.	☐	☐	☐	☐	☐
DSS02 – *Manage Service Requests and Incidents*	Insiden dianalisis dan terdokumentasi untuk menghindari kejadian berulang.	☐	☐	☐	☐	☐
DSS05 – *Manage Security Services*	Organisasi memiliki kebijakan keamanan yang diterapkan dalam semua sistem TI.	☐	☐	☐	☐	☐
DSS05 – *Manage Security Services*	Audit keamanan dilakukan secara berkala untuk mengidentifikasi kelemahan sistem.	☐	☐	☐	☐	☐
DSS05 – *Manage Security Services*	Ada sistem deteksi dan respons terhadap ancaman keamanan yang efektif.	☐	☐	☐	☐	☐
DSS05 – *Manage Security Services*	Pengguna mendapatkan pelatihan rutin mengenai praktik keamanan informasi.	☐	☐	☐	☐	☐
BAI06 – *Manage Changes*	Setiap perubahan sistem TI melewati proses persetujuan yang ketat.	☐	☐	☐	☐	☐
BAI06 – *Manage Changes*	Setiap perubahan sistem TI melewati proses persetujuan yang ketat.	☐	☐	☐	☐	☐
BAI06 – *Manage Changes*	Dampak perubahan terhadap layanan TI selalu dianalisis sebelum implementasi.	☐	☐	☐	☐	☐
BAI06 – *Manage Changes*	Organisasi memiliki prosedur rollback jika terjadi kegagalan dalam penerapan perubahan.	☐	☐	☐	☐	☐
BAI10 – *Manage Configuration*	Organisasi memiliki sistem terpusat untuk mencatat semua konfigurasi TI.	☐	☐	☐	☐	☐

BAI10 – *Manage Configuration*	Setiap perubahan konfigurasi terdokumentasi dan dikontrol dengan ketat.	☐	☐	☐	☐	☐
BAI10 – *Manage Configuration*	Ada mekanisme otomatis untuk mendeteksi perubahan tidak sah pada konfigurasi sistem.	☐	☐	☐	☐	☐
BAI10 – *Manage Configuration*	Pengelolaan konfigurasi membantu organisasi dalam menjaga keandalan dan keamanan sistem.	☐	☐	☐	☐	☐

4.5 Teknik Pembuatan Skala

Dalam penelitian ini, kuisioner menggunakan model pengukuran dengan skala ordinal Likert. Pengukuran dalam model ini melibatkan skala ordinal dan nominal. Skala ordinal mengacu pada pemberian angka yang memiliki arti dalam bentuk tingkatan. Sementara itu, skala nominal digunakan untuk mengurutkan objek berdasarkan tingkatannya, mulai dari yang terendah hingga yang tertinggi. Skala nominal ini tidak memberikan nilai absolut terhadap objek, melainkan hanya menyusun objek menurut urutan tingkatan, dari yang paling rendah hingga yang paling tinggi. Tingkatan nilai yang digunakan dapat dilihat pada Tabel 4.9

Tabel 4 9 Nilai Tingkatan (ISACA Governance and Management, 2019)

Nilai	Keterangan
1	Sangat tidak setuju
2	Tidak Setuju
3	Ragu
4	Setuju
5	Sangat Setuju

Sedangkan nilai absolut merupakan nilai model *maturity* dapat dilihat dari nilai padatabel 4.10 dibawah ini.

Tabel 4 10 Nilai Absolut Model *Maturity* (ISACA *Governance and Management*, 2019)

Nilai	Keterangan
0	Tidak ada
1	Inisiasi
2	Dapat diulang
3	Ditetapkan
4	Diatur
5	Dioptimalisasi

Selanjutnya, hubungan antara nilai tingkat dan nilai absolut dijalin dengan menggunakan perhitungan indeks, yang dihitung melalui metode matematika untuk menentukan nilai indeks tersebut.

Tabel 4 11 Skala Pembulatan Indeks (ISACA Governance and Manajement, 2019)

Skala Pembulatan	Tingkat Model Maturity	Tingkat Model Kapabilitas
4,51 – 5,00	5 – Optimalisasi	5 – *Optimising Proses*
3,51 – 4,50	4 – Diatur	4 – *Predictable Process*
2,51 – 3,50	3 – Ditetapkan	3 – *Establised Process*
1,51 – 2,50	2 - Dapat Diulang	2 – *Managed Process*
0,51 – 1,50	1 – Inisialisasi	1 – *Performed Process*
0,00 – 0,50	0 – Tidak Ada	0 – *Incomplate Process*

4.6 Komputasi *Capability* Level

Model kapabilitas adalah alat untuk menilai kondisi kinerja. Proses pengukuran ini akan memberikan evaluasi terhadap kondisi saat ini berdasarkan domain proses APO12, BAI06, BAI10, DSS02, DSS05. Pengukuran tingkat kapabilitas dilakukan dengan menggunakan rumus berikut:

$$x = \frac{\sum Xi}{n}$$

Keterangan:

X = *Mean* atau rata-rata hitung

∑ = Penjumlahan keseluruhan

Xi = Skor berapa jumlah *X*, *I* = 1, 2, 3, , n (skor sampel ke-*i*)*N* = Jumlah sampel

4.7 Capability Level Proses

Setelah proses pengukuran dilakukan menggunakan kuesioner, diperoleh tingkat kapabilitas domain yang mencerminkan seberapa baik kemampuan atau kesiapan dalam menghadapi tantangan yang ada, serta memberikan gambaran yang lebih jelas mengenai potensi pengembangan di masa depan.

1. Domain DSS05

Pada tahapan proses ang disajikan dalam Tabel, diperoleh data yang menunjukkan hasil pengukuran yang lebih terperinci dan memberikan wawasan yang lebih mendalam mengenai perkembangan kapabilitas domain, yang menjadi dasar untuk langkah-langkah strategis selanjutnya.

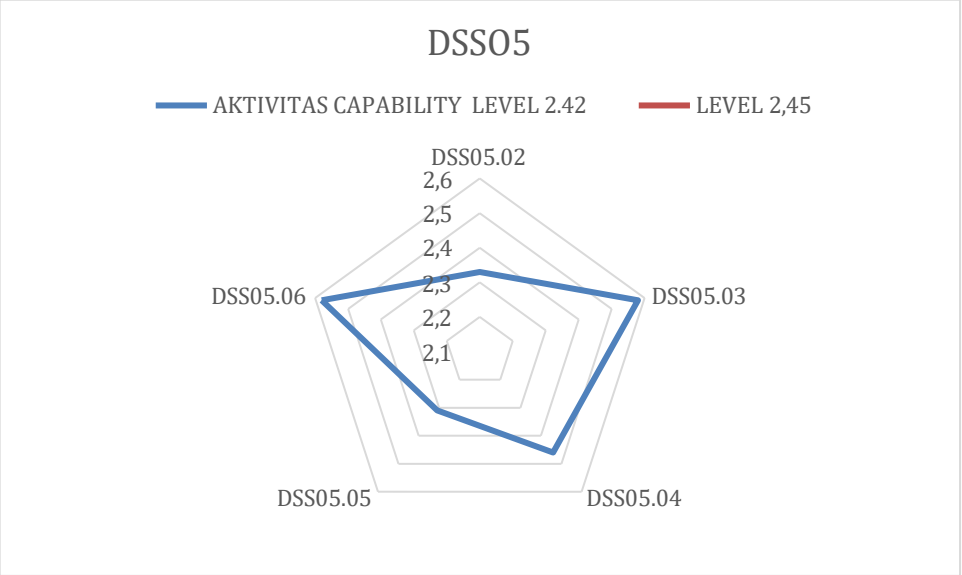
Tabel 4 12 *Capability Level* Proses DSS05

Proses	Aktivitas	Aktivitas *Capability Level*	Level
DSS05	DSS05.01	2.42	2,46
	DSS05.02	2.33	
	DSS05.03	2.58	
	DSS05.04	2.46	
	DSS05.05	2.31	
	DSS05.06	2.54	
	DSS05.07	2.58	

Tabel diatas menunjukkan evaluasi proses DSS05 (*Manage Security Services*) dalam COBIT 2019, dengan *Capability Level* rata-rata 2.46 (*Managed*). Ini berarti aktivitas dalam DSS05 telah terkelola tetapi belum sepenuhnya distandarisasi.

Untuk meningkatkan ke Level 3 (*Defined*), organisasi perlu memperkuat dokumentasi standar, meningkatkan automasi keamanan, dan menerapkan pemantauan lebih ketat agar layanan keamanan TI lebih efektif.

Skor *capability* level untuk responden pada tahap DSS05 dapat dilihat pada Grafik 4.12, yang menggambarkan tingkat kapabilitas yang dicapai oleh masing-masing responden dalam melaksanakan aktivitas-aktivitas pada tahap tersebut



Gambar 4 12 Grafik Domain DSS05

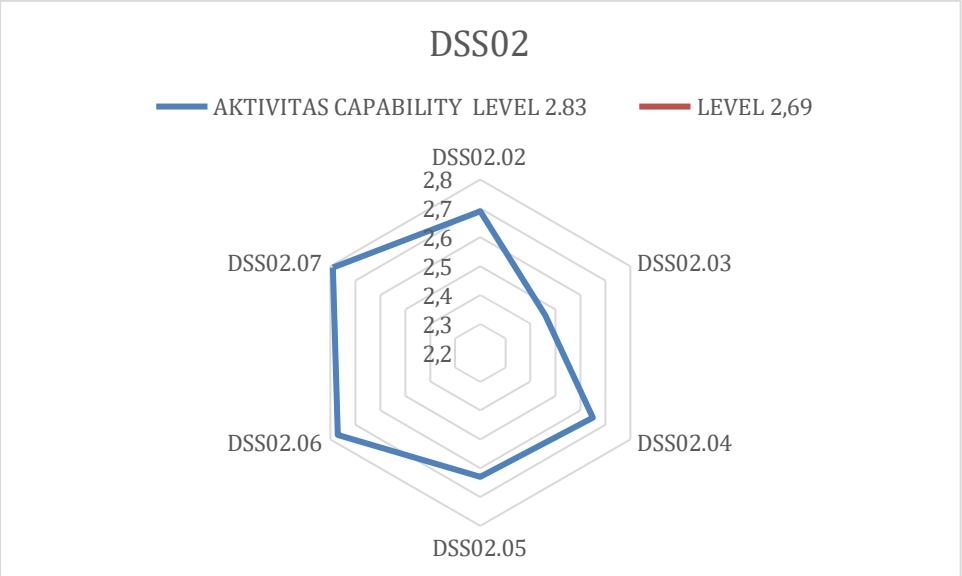
2. Domain DSS02

Tabel 4 13 *Capability* Level Proses DSS02

Proses	Aktivitas	Aktivitas *Capability Level*	Level
DSS02	DSS02.01	2.83	2,69
	DSS02.02	2.69	
	DSS02.03	2.46	
	DSS02.04	2.65	
	DSS02.05	2.63	
	DSS02.06	2.77	
	DSS02.07	2.79	

Tabel ini menunjukkan evaluasi *Capability Level* untuk proses dalam domain DSS02 (*Manage Service Requests and Incidents*) berdasarkan aktivitas spesifik (DSS02.01 hingga DSS02.07). Skor kapabilitas pada tiap aktivitas berkisar antara 2.46 hingga 2.83, dengan rata-rata di kisaran Level 2 (*Managed Process*). Hal ini menunjukkan bahwa proses permintaan layanan dan manajemen insiden telah terdefinisi dengan baik dan diterapkan secara konsisten dalam organisasi. Namun, untuk mencapai tingkat kematangan yang lebih tinggi (Level 3 atau lebih), organisasi perlu meningkatkan standar, pengukuran kinerja, serta otomatisasi dalam pengelolaan layanan dan respons terhadap insiden.

Skor *capability* level untuk responden pada tahap DSS02 dapat dilihat pada Grafik 4.13, yang menggambarkan tingkat kapabilitas yang dicapai oleh masing-masing responden dalam melaksanakan aktivitas-aktivitas pada tahap tersebut.



Gambar 4 13 Grafik Domain DSS02

3. Domain APO12

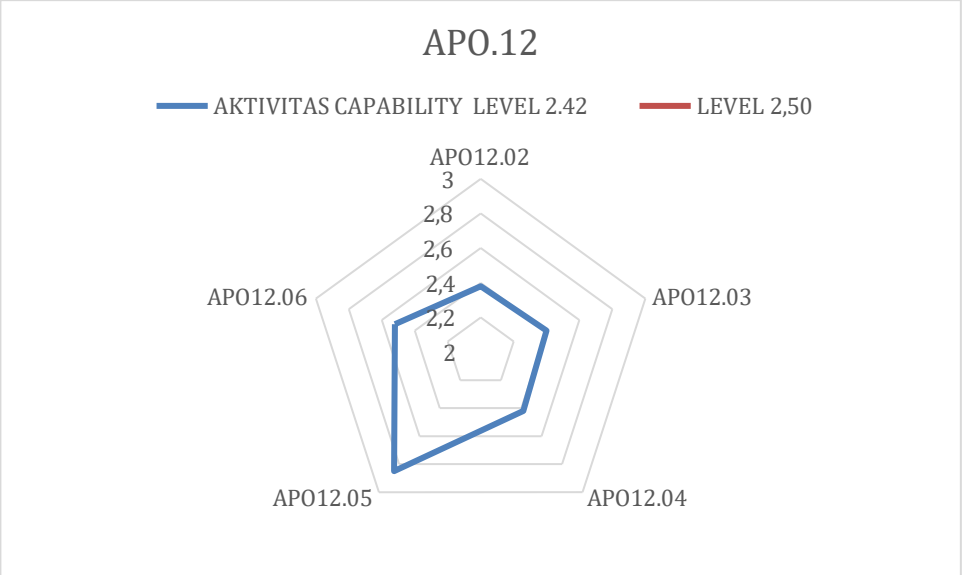
Tabel 4 14 *Capability* Level Proses APO12

Proses	**Aktivitas**	**Aktivitas *Capability Level***	**Level**
APO.12	APO12.01	2.42	2,50
	APO12.02	2.38	
	APO12.03	2.4	
	APO12.04	2.42	
	APO12.05	2.85	
	APO12.06	2.52	

Tabel diatas menunjukkan evaluasi *Capability Level* untuk proses APO12 (*Manage Risk*) berdasarkan enam aktivitas (APO12.01 hingga APO12.06). Nilai kapabilitas aktivitas berkisar antara 2.38 hingga 2.85, dengan rata-rata Level 2.50, yang menunjukkan bahwa proses ini berada pada Level 2 (*Managed Process*). Ini berarti bahwa manajemen risiko telah diterapkan secara terstruktur dalam organisasi,

namun masih memerlukan peningkatan dalam standarisasi, otomatisasi, dan pengukuran efektivitas agar dapat mencapai tingkat kematangan yang lebih tinggi (Level 3 atau lebih).

Skor *capability* level untuk responden pada tahap APO12 dapat dilihat pada Grafik 4.14, yang menggambarkan tingkat kapabilitas yang dicapai oleh masing-masing responden dalam melaksanakan aktivitas-aktivitas pada tahap tersebut.



Gambar 4 14 Grafik Domain APO12

4. Domain BAI.06

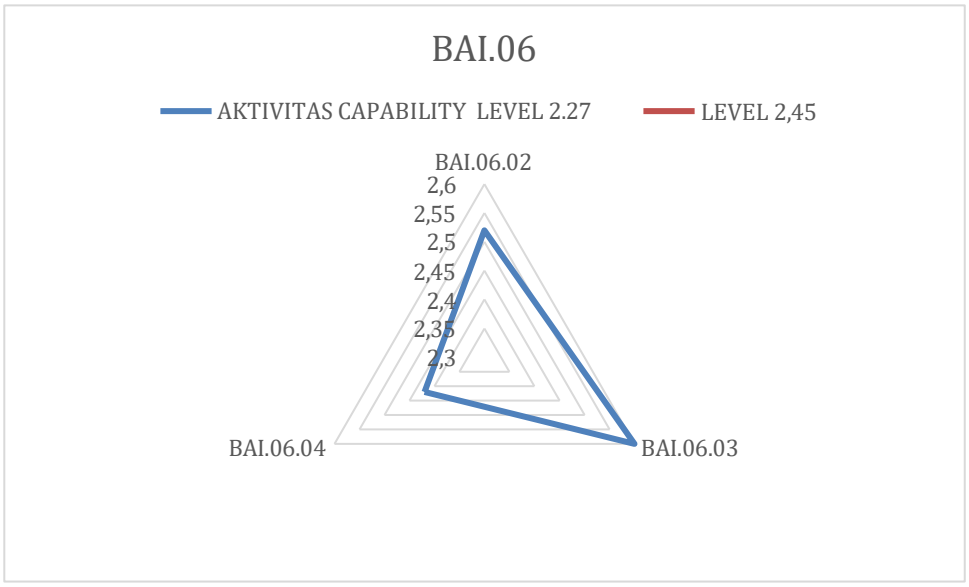
Tabel 4 15 *Capability* Level Proses BAI06

Proses	Aktivitas	Aktivitas *Capability* Level	Level
BAI.06	BAI.06.01	2.27	2,45
	BAI.06.02	2.52	
	BAI.06.03	2.6	
	BAI.06.04	2.42	

Tabel diatas menunjukkan evaluasi *Capability Level* untuk proses BAI06 (*Manage IT Change*) berdasarkan empat aktivitas (BAI06.01 hingga BAI06.04). Nilai

kapabilitas aktivitas berkisar antara 2.27 hingga 2.6, dengan rata-rata Level 2.45, yang menunjukkan bahwa proses ini berada pada Level 2 (*Managed Process*). Ini berarti bahwa manajemen risiko telah diterapkan secara terstruktur dalam organisasi, namun masih memerlukan peningkatan dalam standarisasi, otomatisasi, dan pengukuran efektivitas agar dapat mencapai tingkat kematangan yang lebih tinggi (Level 3 atau lebih).

Skor *capability* level untuk responden pada tahap BAI.06 dapat dilihat pada Grafik 4.15, yang menggambarkan tingkat kapabilitas yang dicapai oleh masing-masing responden dalam melaksanakan aktivitas-aktivitas pada tahap tersebut.



Gambar 4 15 Grafik Domain BAI06

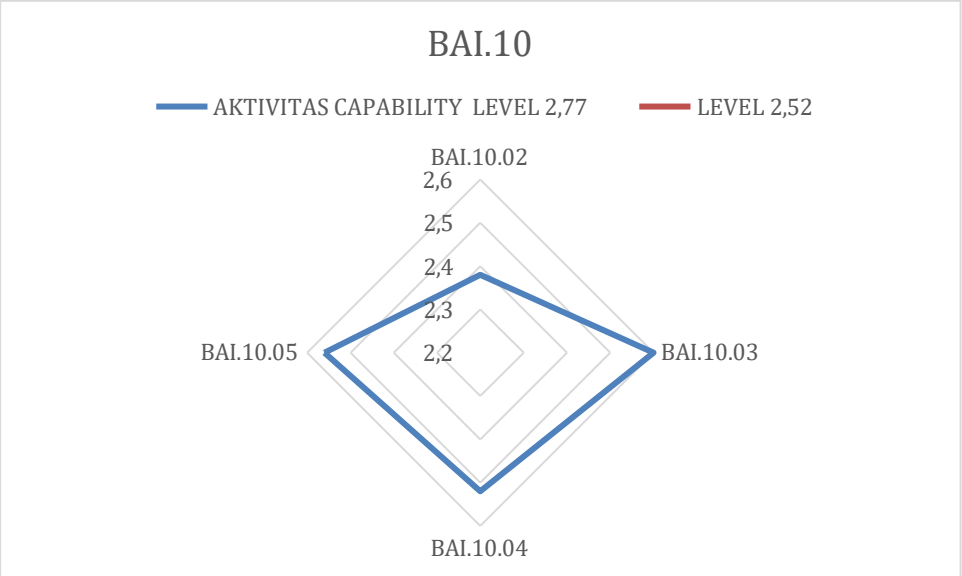
5. Domain BAI.10

Tabel 4 16 *Capability* Level Proses BAI10

Proses	Aktivitas	Aktivitas *Capability* Level	Level
BAI.10	BAI.10.01	2,77	2,52
	BAI.10.02	2.38	
	BAI.10.03	2.6	
	BAI.10.04	2.52	
	BAI.10.05	2.56	

Tabel diatas menunjukkan evaluasi *Capability Level* untuk proses BAI10 (*Manage Configuration*) berdasarkan lima aktivitas utama (BAI10.01 hingga BAI10.05). Nilai kapabilitas aktivitas berkisar antara 2.38 hingga 2.77, dengan rata-rata Level 2.52, yang menunjukkan bahwa proses ini berada pada Level 2 (*Managed Process*). Ini mengindikasikan bahwa organisasi telah memiliki prosedur terdokumentasi dalam mengelola konfigurasi sistem TI, namun masih memerlukan peningkatan dalam aspek pemantauan, kontrol perubahan, serta otomatisasi untuk mencapai Level 3 (*Established Process*), di mana proses lebih matang, terdokumentasi dengan baik, dan dioptimalkan untuk mendukung efisiensi serta keandalan layanan TI.

Skor *capability* level untuk responden pada tahap BAI10 dapat dilihat pada Grafik 4.16, yang menggambarkan tingkat kapabilitas yang dicapai oleh masing-masing responden dalam melaksanakan aktivitas-aktivitas pada tahap tersebut.



Gambar 4 16 Grafik Domain BAI06

4.8 *Maturity* level Proses

Berikut ini adalah hasil pengukuran level kedewasaan (*maturity* level) yang dilakukan pada berbagai proses dan aktivitas yang terkait. Pengukuran ini bertujuan untuk mengevaluasi sejauh mana kapabilitas yang ada dalam setiap proses dapat dijalankan dengan efektif dan efisien, serta untuk mengidentifikasi area yang perlu perbaikan lebih lanjut.

Hasil pengukuran ini mencakup berbagai indikator yang menggambarkan tingkat kedewasaan yang telah dicapai dalam setiap aktivitas. Dengan informasi ini, organisasi dapat merencanakan langkah-langkah perbaikan untuk meningkatkan kinerja dan kapabilitas, serta mencapai tujuan yang lebih optimal dalam proses yang sedang berjalan.

Selanjutnya, dalam komputasi *Exp Capability Level* pada setiap tahap, hasil pengukuran kapabilitas yang telah dilakukan akan dijelaskan secara lebih rinci. Tabel-tabel berikut ini menyajikan data yang diperoleh dari tahap tersebut, yang menggambarkan tingkat kapabilitas yang dicapai pada masing-masing sub-aktivitas.

Tabel-tabel tersebut memberikan gambaran yang lebih jelas mengenai hasil komputasi, dengan menunjukkan nilai capaian setiap aktivitas dalam proses

1 *Maturity Level* Proses Domain DSS05

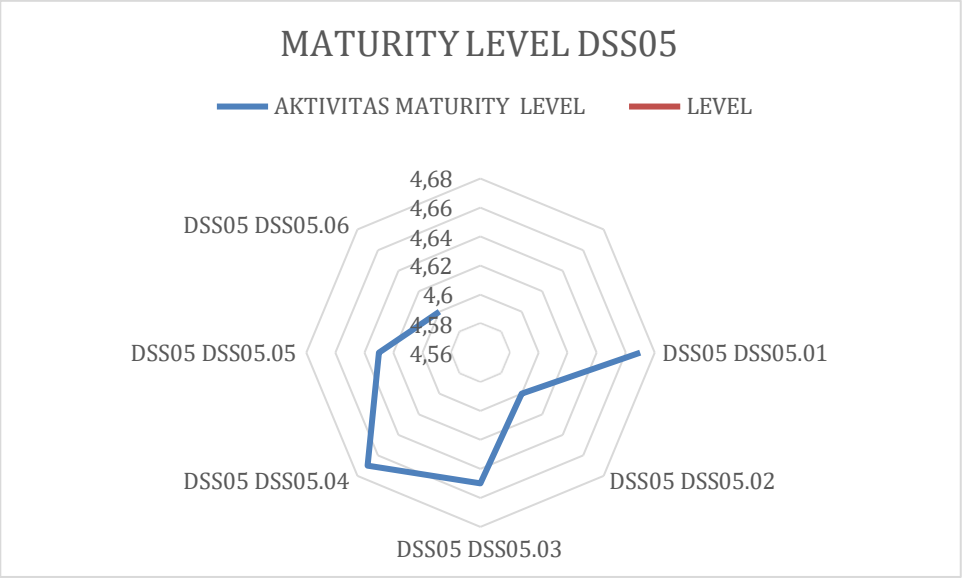
Tabel 4 17 *Maturity* Level Proses DSS05

Proses	Aktivitas	Aktivitas *Maturity* Level	Level
DSS05	DSS05.01	4.67	4.63
	DSS05.02	4.6	
	DSS05.03	4.65	
	DSS05.04	4.67	
	DSS05.05	4.63	
	DSS05.06	4.58	
	DSS05.07	4.60	

Proses DSS05 (*Manage Security Services*) memiliki *Maturity Level* 4.63, menunjukkan bahwa layanan keamanan telah terstandarisasi, dipantau, dan dapat diprediksi dengan baik. Untuk mencapai Level 5 (*Optimizing Process*), organisasi disarankan untuk:

1. Otomatisasi Keamanan – Menggunakan AI, SIEM, dan machine learning untuk deteksi serta respons ancaman.
2. Continuous Improvement – Mengevaluasi kebijakan keamanan secara berkala dan menerapkan framework terbaru.
3. Pelatihan Keamanan – Melakukan simulasi serangan dan meningkatkan kesadaran karyawan terhadap ancaman siber.
4. Respons Insiden Cepat – Mengembangkan playbook insiden serta menerapkan sistem otomatis untuk resolusi insiden.
5. Benchmarking Industri – Membandingkan praktik keamanan dengan standar industri dan berpartisipasi dalam forum keamanan.

Dengan langkah-langkah ini, organisasi dapat mencapai proses keamanan yang proaktif, inovatif, dan berkelanjutan, meningkatkan ketahanan terhadap ancaman siber.



Gambar 4 17 Grafik Domain DSS05

2. *Maturity Level* Proses Domain DSS02

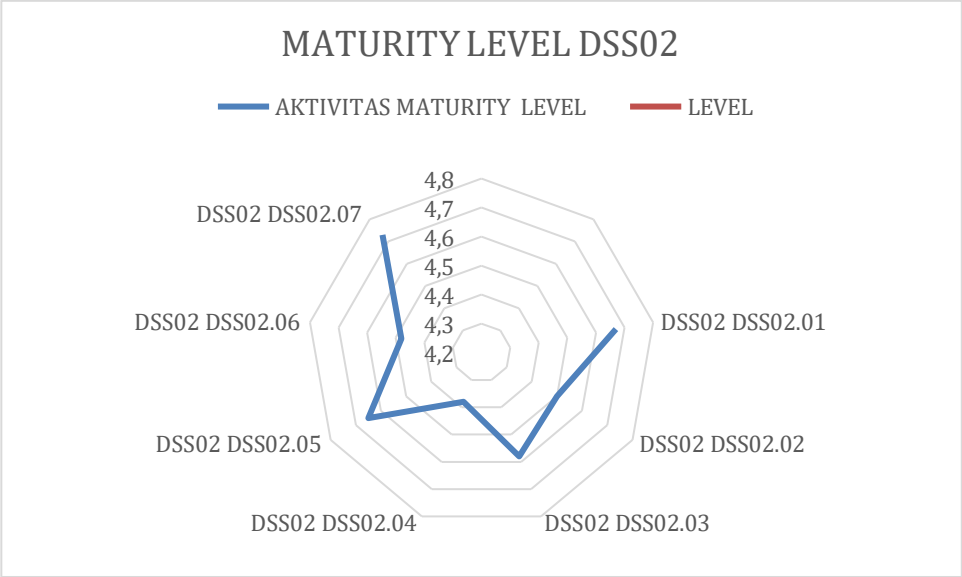
Tabel 4 18 *Maturity* Level Proses DSS02

Proses	Aktivitas	Aktivitas *Maturity* Level	Level
DSS02	DSS02.01	4.67	4.57
	DSS02.02	4.5	
	DSS02.03	4.58	
	DSS02.04	4.38	
	DSS02.05	4.65	
	DSS02.06	4.48	
	DSS02.07	4.73	

Proses DSS02 (*Manage Service Requests and Incidents*) memiliki *Maturity Level* 4.57, menandakan bahwa proses sudah terstandarisasi, dipantau, dan dikelola dengan baik, namun masih bisa ditingkatkan ke Level 5 (*Optimizing Process*).

Rekomendasi Peningkatan ke Level 5:

1. Otomatisasi ITSM – Menggunakan AI dan *chatbot* untuk respons insiden lebih cepat.
2. Efektivitas Resolusi – Meningkatkan *self-service* portal dan analitik prediktif.
3. Analisis Insiden Berulang – RCA lebih mendalam dan dashboard real-time monitoring.
4. Pelatihan Tim TI – Simulasi insiden dan pelatihan berbasis kasus nyata.
5. *Benchmarking & Continuous Improvement* – Mengadopsi ITIL dan COBIT lebih mendalam



Gambar 4 18 Grafik Domain DSS02

3. *Maturity Level* Proses Domain APO12

Tabel 4 19 *Maturity* Level Proses APO12

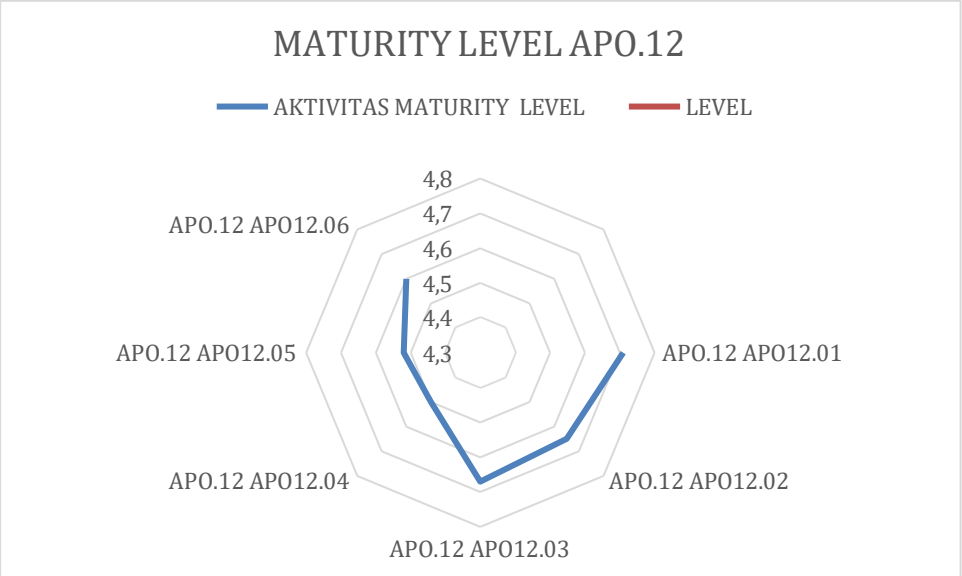
Proses	**Aktivitas**	**Aktivitas Maturity Level**	**Level**
APO.12	APO12.01	4.71	4.61

	APO12.02	4.65	
	APO12.03	4.67	
	APO12.04	4.50	
	APO12.05	4.52	
	APO12.06	4.60	

Proses APO12 (*Manage Risk*) memiliki *Maturity Level* 4.61, yang menunjukkan bahwa proses sudah dikelola secara terstandarisasi, dipantau, dan terus diperbaiki, namun masih bisa ditingkatkan ke Level 5 (*Optimizing Process*) untuk mencapai manajemen risiko yang lebih proaktif dan prediktif.

Rekomendasi Peningkatan ke Level 5:

1. *Automated Risk Assessment* – Menggunakan AI dan *machine learning* untuk mengidentifikasi ancaman lebih cepat.
2. *Continuous Monitoring & Predictive Analytics* – Implementasi sistem pemantauan berbasis *real-time* dengan BI tools.
3. *Integration with Business Strategy* – Menjadikan manajemen risiko bagian integral dari perencanaan strategis.
4. *Advanced Simulation & Scenario Planning* – Menggunakan model simulasi risiko untuk mengantisipasi potensi ancaman masa depan.
5. *Culture of Risk Awareness* – Meningkatkan kesadaran karyawan melalui pelatihan berkelanjutan dan kebijakan yang lebih adaptif.



Gambar 4 19 Grafik Domain APO12

4. *Maturity Level* Proses Domain BAI.06

Tabel 4 20 *Maturity* Level Proses BAI06

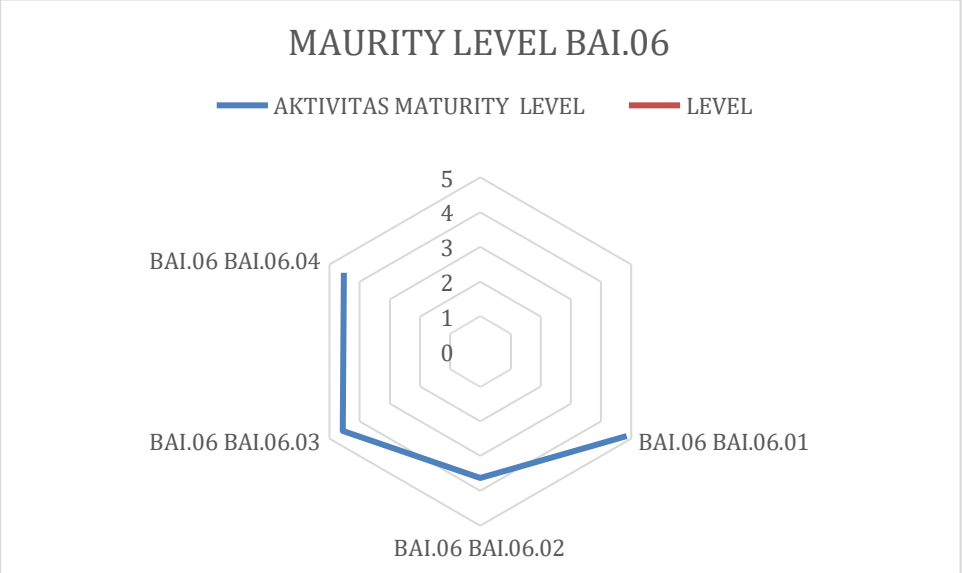
Proses	Aktivitas	Aktivitas *Maturity* Level	Level
BAI.06	BAI.06.01	4.85	4.39
	BAI.06.02	3.63	
	BAI.06.03	4.56	
	BAI.06.04	4.52	

Proses BAI06 (*Manage Changes*) memiliki *Maturity Level* 4.39, yang menunjukkan bahwa proses perubahan dalam organisasi sudah terstandarisasi, dipantau, dan dikelola dengan baik, tetapi masih memiliki ruang untuk peningkatan menuju Level 5 (*Optimizing Process*) agar lebih adaptif dan inovatif.

Rekomendasi Peningkatan ke Level 5:

1. Otomatisasi Manajemen Perubahan – Menggunakan AI dan *workflow* otomatis untuk validasi dan implementasi perubahan yang lebih cepat dan akurat.

2. *Continuous Improvement & Feedback Loop* – Menerapkan model *continuous improvement (Kaizen)* dengan umpan balik *real-time* dari pengguna.
3. Analisis Dampak Perubahan – Memanfaatkan *predictive analytics* untuk mengukur dampak perubahan sebelum diterapkan.
4. Integrasi dengan *DevOps* – Mempercepat siklus perubahan dengan integrasi yang lebih erat antara pengembangan dan operasional TI.
5. Peningkatan Pelatihan & *Awareness* – Memberikan pelatihan berkala kepada tim terkait agar lebih siap dalam menghadapi perubahan dan mengelola resistensi.



Gambar 4 20 Grafik Domain BAI06

5. Maturity Level Proses Domain BAI.10

Tabel 4 21 *Maturity* Level Proses BAI10

Proses	Aktivitas	Aktivitas *Maturity* Level	Level
BAI.10	BAI.10.01	4.79	4.68
	BAI.10.02	4.65	
	BAI.10.03	4.73	
	BAI.10.04	4.54	
	BAI.10.05	4.71	

Proses BAI10 (*Manage Configuration*) memiliki *Maturity Level* 4.68, yang menunjukkan bahwa proses pengelolaan konfigurasi sudah terdefinisi dengan baik, distandarisasi, dan dikendalikan, tetapi masih memerlukan peningkatan untuk mencapai Level 5 (*Optimized Process*).

Rekomendasi Peningkatan ke Level 5:

1. Implementasi AI & *Machine Learning* – Menggunakan AI untuk deteksi anomali dalam perubahan konfigurasi dan otomatisasi perbaikan.
2. Integrasi dengan ITSM & *DevOps* – Memastikan sistem konfigurasi selaras dengan pipeline DevOps untuk perubahan yang lebih cepat dan terkendali.
3. *Real-time Monitoring & Predictive Analysis* – Menggunakan analitik prediktif untuk mengidentifikasi potensi risiko dari perubahan konfigurasi sebelum diterapkan.
4. Otomatisasi *Compliance Check* – Memastikan semua konfigurasi selalu memenuhi standar keamanan dan regulasi melalui audit otomatis.
5. Peningkatan Dokumentasi & *Knowledge Management* – Memastikan informasi konfigurasi selalu diperbarui dan mudah diakses oleh tim TI.

4.6 Tingkat Kematangan (*Maturity Level*)

Berdasarkan hasil penilaian tingkat kematangan tata kelola TI, dilakukan analisis kesenjangan (gap) antara tingkat *maturity* proses TI saat ini (as-is) dan tingkat maturity proses TI yang diharapkan (to-be) dapat dilihat pada Tabel dibawah ini

Tabel 4 22 *Maturity* Level Proses

No	Domain COBIT	*Maturity* Level		GAP
		Performance	***Expected***	
1	DSS.05	2.46	4.63	2.17
2	DSS02	2.69	4.57	1.88
3	APO12	2.50	4.61	2.11
4	BAI.06	2.45	4.39	1.94
5	BAI.10	2.52	4.68	2.16
Rata – Rata				**2.05**

Tabel ini menunjukkan GAP analysis antara *maturity level* saat ini dan *expected* performance level untuk beberapa domain COBIT 2019.

- DSS05 (*Manage Security Services*): Saat ini berada di level 2.46, sedangkan ekspektasi adalah 4.63, sehingga ada GAP sebesar 2.17. Ini menunjukkan perlunya peningkatan dalam manajemen keamanan layanan TI.
- DSS02 (*Manage Service Requests and Incidents*): Memiliki *maturity level* 2.69 dengan target 4.57 (GAP 1.88). Perlu peningkatan dalam kecepatan dan efektivitas penanganan insiden.
- APO12 (*Manage Risk*): Saat ini di level 2.50, dengan target 4.61 (GAP 2.11). Organisasi perlu memperkuat proses manajemen risiko TI untuk mencapai standar yang lebih tinggi.
- BAI06 (*Manage Changes*): Level saat ini 2.45, target 4.39, dan GAP 1.94. Perlu peningkatan dalam pengelolaan perubahan sistem untuk mengurangi risiko gangguan operasional.
- BAI10 (*Manage Configuration*): Saat ini di level 2.52, dengan target 4.68 (GAP 2.16). Perlu optimalisasi dalam pengelolaan konfigurasi TI agar lebih terdokumentasi dan andal.

Kesimpulan:

Rata-rata *maturity level* saat ini adalah 2.05, yang menunjukkan bahwa sebagian

besar proses masih dalam tahap *Managed* (Level 2) dan belum mencapai *Defined* (Level 3) atau lebih tinggi. Perlu peningkatan standar, dokumentasi, automasi, dan pemantauan berkelanjutan untuk mengurangi GAP dan meningkatkan efektivitas pengelolaan TI.

Tabel 4.20 Identifikasi GAP dalam Pertanyaan Kuesioner

Domain	Pertanyaan	Nilai Rata-rata	Target	GAP
DSS02	Ada sistem tiket otomatis untuk menangani insiden?	2.8	4	1.2
DSS05	Audit keamanan dilakukan secara berkala?	2.6	4	1.4
BAI06	Setiap perubahan sistem TI melewati proses persetujuan yang ketat?	2.4	4	1.6
BAI10	Ada mekanisme otomatis untuk mendeteksi perubahan tidak sah?	2.5	4	1.5
APO12	Risiko TI dievaluasi secara berkala?	2.7	4	1.3

Dari tabel di atas, GAP tertinggi terdapat pada pertanyaan terkait **BAI06** dengan selisih **1.6 poin** dari target.

4.7 Rekomendasi Perbaikan Berdasarkan GAP

Berdasarkan temuan GAP di atas, berikut adalah rekomendasi perbaikannya:

1. DSS02 (Sistem Tiket Insiden)
    - Implementasi sistem *Helpdesk* yang mendukung pelacakan tiket otomatis.
    - Meningkatkan sosialisasi penggunaan sistem tiket kepada seluruh pengguna.
2. DSS05 (Audit Keamanan Berkala)
    - Menetapkan kebijakan audit keamanan yang dilakukan setiap 6 bulan sekali.
    - Melibatkan auditor eksternal untuk evaluasi yang lebih objektif.
3. BAI06 (Persetujuan Perubahan TI)

- Menerapkan prosedur *Change Management Framework* agar setiap perubahan terdokumentasi.
- Menggunakan sistem berbasis *approval* digital untuk mempercepat persetujuan.

4. BAI10 (Deteksi Perubahan Konfigurasi)
   - Menggunakan *Configuration Management Database* (CMDB) untuk mencatat semua perubahan konfigurasi.
   - Menerapkan notifikasi otomatis ketika ada perubahan tidak sah.
5. APO12 (Evaluasi Risiko TI Berkala)
   - Melakukan *Risk Assessment* setiap kuartal.
   - Menggunakan tools seperti ISO 27005 *Risk Management Framework* untuk validasi hasil analisis risiko.

4.8 Validasi GAP

Untuk memastikan setiap GAP tervalidasi dengan baik, langkah-langkah berikut akan dilakukan:

- Analisis Tren: Membandingkan hasil audit saat ini dengan audit sebelumnya.
- Diskusi dengan Pemangku Kepentingan: Mengadakan pertemuan rutin untuk mendiskusikan kemajuan implementasi rekomendasi.
- Uji Coba Implementasi: Mengimplementasikan sebagian rekomendasi dan mengukur efektivitasnya dalam 3 bulan pertama.
- Survei Kepuasan Pengguna: Menggunakan feedback pengguna sebagai bahan evaluasi dampak perbaikan yang dilakukan.

Dengan langkah-langkah ini, diharapkan setiap GAP dapat diatasi dan meningkatkan efektivitas pengelolaan TI di lingkungan Pemerintah Kabupaten Way Kanan.