Perancangan Tata Kelola TI untuk Transformasi Digital di Pemerintah Provinsi XYZ Menggunakan COBIT 2019 pada Domain DSS (*Deliver, Service, and Support*)

1st Ni Luh Putu Pawestri Ayuningtyas
S1 Sistem Informasi, Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
nlhpwstriii@student.telkomuniversity.ac.id

2nd Ryan Adithya Nugraha
S1 Sistem Informasi, Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
ryan.a.nugraha&gmail.com

3rd Yuli Adam Prasetyo
S1 Sistem Informasi, Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
adam@telkomuniversity.ac.id

Pemerintah Provinsi XYZ sebagai institusi publik dituntut untuk memiliki tata kelola teknologi informasi (TI) yang efektif dalam mendukung pelaksanaan transformasi digital dan peningkatan kualitas layanan publik. Namun, berdasarkan kondisi eksisting, tata kelola TI yang diterapkan masih belum optimal, khususnya pada aspek layanan, dukungan, dan keberlangsungan operasional TI. Oleh karena itu, diperlukan evaluasi dan perancangan tata kelola TI yang terstruktur sebagai acuan perbaikan berkelanjutan. Penelitian ini memiliki tujuan guna mengkaji kondisi tata kelola TI saat ini serta menyusun rekomendasi peningkatan tata kelola TI di Pemerintah Provinsi XYZ menggunakan framework COBIT 2019 dengan mengutamakan domain *Deliver, Service, and Support* (DSS). Tahap yang dievaluasi meliputi DSS03 (*Managed Problems*), DSS04 (*Managed Continuity*), DSS05 (*Managed Security Services*), dan DSS06 (*Managed Business Process Controls*). Metode penelitian yang digunakan adalah *Design Science Research* (DSR) dengan pendekatan studi kasus, melalui teknik pengumpulan data berupa wawancara, observasi, dan analisis dokumen. Hasil penelitian menunjukkan bahwa tingkat kapabilitas proses tata kelola TI berada pada level 2 (*Managed Process*), dengan sejumlah kesenjangan pada aspek proses, kebijakan, dokumentasi, dan sumber daya manusia. Rekomendasi yang dihasilkan diharapkan dapat menjadi acuan dalam penguatan tata kelola TI serta mendukung keberhasilan transformasi digital yang berkelanjutan di lingkungan Pemerintah Provinsi XYZ.

Kata kunci— COBIT 2019, Tata Kelola Teknologi Informasi, Pemerintah Provinsi XYZ, Domain DSS, Transformasi Digital

I. PENDAHULUAN

Teknologi informasi (TI) berperan penting dalam mendukung transformasi digital sektor pemerintahan melalui peningkatan efisiensi operasional, kualitas layanan publik, serta transparansi dan akuntabilitas kinerja pemerintah [1]. Pemanfaatan teknologi digital juga mendorong terwujudnya Sistem Pemerintahan Berbasis Elektronik (SPBE) yang terintegrasi dan berorientasi pada pelayanan masyarakat [2].

Namun, penerapan tata kelola TI di Pemerintah Provinsi XYZ masih menghadapi berbagai kendala, seperti belum optimalnya pengelolaan layanan TI, lemahnya pengendalian operasional, serta keterbatasan dokumentasi dan kebijakan pendukung [3]. Kondisi tersebut menunjukkan perlunya evaluasi tata kelola TI dari segi sistematis agar seiring dengan tujuan organisasi dan kebutuhan transformasi digital. Oleh karena itu, penelitian ini memiliki tujuan guna mengkaji dan merancang tata kelola TI menggunakan framework COBIT 2019 dengan mengutamakan domain *Deliver, Service, and Support* (DSS) melalui pendekatan *Design Science Research* (DSR), sehingga dapat menghasilkan rekomendasi perbaikan tata kelola TI yang berkelanjutan [4].

II. KAJIAN TEORI

a. Tata Kelola TI

Teknologi informasi (TI) mencakup perangkat keras, perangkat lunak, jaringan, serta prosedur yang digunakan untuk mengelola dan mendistribusikan informasi secara efektif. Dalam konteks pemerintahan, TI berperan penting dalam mendukung operasional organisasi, meningkatkan kualitas layanan publik, serta memperkuat transparansi dan akuntabilitas. Pemanfaatan TI yang optimal memerlukan pengelolaan yang terstruktur agar mampu memberikan nilai tambah bagi organisasi [1].

b. Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi merupakan seperangkat struktur, proses, dan mekanisme pengambilan keputusan yang bertujuan memastikan pemanfaatan TI selaras dengan tujuan strategis organisasi, mampu mengelola risiko, serta memaksimalkan nilai yang dihasilkan. Penerapan tata kelola TI yang baik menuntut keterlibatan manajemen, perencanaan yang sistematis, serta penerapan kerangka kerja yang terstandarisasi seperti COBIT 2019 agar pengelolaan TI tidak bersifat reaktif, melainkan mendukung transformasi digital secara berkelanjutan [3], [4].

c. COBIT 2019 dan Domain DSS

COBIT 2019 merupakan kerangka kerja tata kelola dan manajemen teknologi informasi yang dikembangkan oleh

ISACA utnuk membantu organisasi memastikan bahwa pemanfaatan TI memberikan nilai optimal, mengelola risiko, serta mendukung pencapaian tujuan strategis organisasi. Framework ini memiliki 40 tujuan tata kelola dan manajemen yang disusun berdasarkan enam prinsip utama, termasuk *holistic approach* dan *end-to-end governance system*, sehingga memungkinkan penerapan tata kelola TI secara komprehensif dan terintegrasi [5].

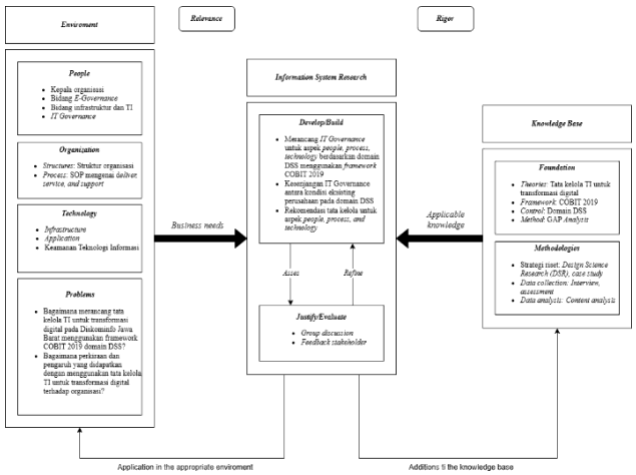
Domain *Deliver, Service, and Support* (DSS) dalam COBIT 2019 mengutamakan penyampaian layanan TI, keberlangsungan operasional, keamanan layanan, serta pengendalian proses bisnis berbasis TI. Domain ini terdiri dari enam proses utama, di antaranya DSS03 (*Managed Problems*), DSS04 (*Managed Continuity*), DSS05 (*Managed Security Services*), dan DSS06 (*Managed Business Process Controls*), yang berperan penting dalam memastikan layanan TI berjalan secara andal, aman, dan berkelanjutan, serta selaras dengan kebutuhan organisasi dan transformasi digital sektor pemerintahan [5].

d. *Design Science Research* (DSR)

Metode DSR menekankan pada pengembangan artefak sebagai solusi terhadap masalah nyata, dengan pendekatan iteratif dan berbasis kontribusi keilmuan.

III. METODE

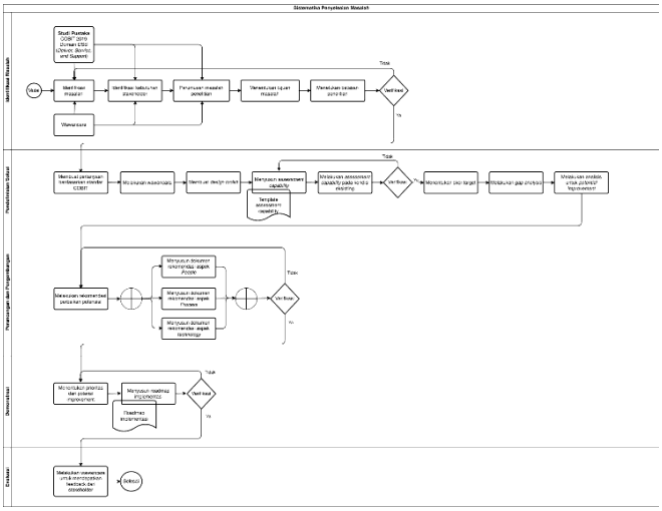
A. Model Konseptual



Gambar 1. Model Konseptual

Model ini menggambarkan alur pendekatan *Design Science Research* (DSR) yang digunakan dalam penelitian, dimulai dari identifikasi kebutuhan bisnis berdasarkan kondisi aktual organisasi (*people, organization, technology*), lalu dilanjutkan dengan pengembangan dan evaluasi artefak tata kelola TI berbasis domain DSS COBIT 2019, serta diakhiri dengan kontribusi terhadap basis pengetahuan melalui validasi dan refleksi hasil yang diperoleh.

B. Sistematika Penyelesaian Masalah



Gambar 2. Sistematika Penyelesaian Masalah

Gambar ini menggambarkan alur sistematis penyelesaian permasalahan penelitian yang mengacu pada COBIT 2019 Implementation Roadmap dengan mengutamakan domain *Deliver, Service, and Support* (DSS). Pendekatan ini digunakan untuk memastikan bahwa perancangan tata kelola TI dilakukan dengan cara yang terorganisir dan sejalan dengan tuntutan organisasi. Tahapan yang diterapkan dalam penelitian ini meliputi empat fase utama, yakni *what are the drivers, where are we now, where do we want to be, dan how do we get there.*

Fase *what are the drivers* diawali dengan identifikasi pemicu dan kebutuhan organisasi terkait pengelolaan layanan TI. Pada fase ini, peneliti mengumpulkan data awal melalui wawncara dengan stakeholder, observasi, serta penelaahan dokumen organisasi untuk memahami permasalahan dan tujuan tata kelola TI di Pemerintah Provinsi XYZ.

Table 1. Hasil Assessment DSS03

No	Aktivitas	Pencapaian	Level	Target
1	*DSS03.01 Identify and classify problems*	100%	2	2
2	*DSS03.02 Investigate and diagnose problems*	N.A	3	
3	*DSS03.03 Raise known errors*	0%	2	
4	*DSS03.04 Resolve and close problems*	N.A	5	
5	*DSS03.05 Perform proactive problem management*	N.A	4	

Table 2. Hasil *Assessment* DSS04

No	Aktivitas	Pencapaian	Level	Target
1	*DSS04.01 Define the business continuity policy, objectives and scope*	100%	2	3
2	*DSS04.02 Maintain business resilience*	38%	2	
		88%	3	
3	*DSS04.03 Develop and implement a business continuity response*	29%	2	
		0%	3	
4	*DSS04.04 Exercise, test and review the BCP and DRP*	N.A	5	
5	*DSS04.05 Review, maintain and improve the continuity plans*	100%	3	
6	*DSS04.06 Conduct continuity plan training*	N.A	4	
7	*DSS04.07 Manage backup arrangements*	100%	2	
8	*DSS04.08 Conduct post-incident review*	N.A	5	

Table 3. Hasil *Assessment* DSS05

No	Aktivitas	Pencapaian	Level	Target
1	*DSS05.01 Protect against malicious software*	0%	2	4
		25%	3	
		15%	4	
2	*DSS05.02 Manage network and connectivity security*	100%	4	
3	*DSS05.03 Manage endpoint security*	100%	3	
4	*DSS05.04 Manage user identity and logical access*	100%	4	
5	*DSS05.05 Manage physical access to I&T assets*	88%	3	
6	*DSS05.06 Manage sensitive documents and output devices*	83%	3	
7	*DSS05.07 Manage vulnerabilities and monitor infrastructure*	100%	3	

Table 4. Hasil *Assessment* DSS06

No	Aktivitas	Pencapaian	Level	Target
1	*DSS06.01 Align control activities with enterprise objectives*	100%	2	2
2	*DSS06.02 Control the processing of information*	100%	2	
3	*DSS06.03 Manage roles, responsibilities, and access privileges*	100%	2	
4	*DSS06.04 Manage errors and exceptions*	100%	2	
5	*DSS06.05 Ensure traceability and accountability*	100%	2	
6	*DSS06.06 Secure information assets*	100%	2	

Fase *where are we now* berfokus pada penilaian kondisi eksisting tata kelola TI. Penilaian dilakukan menggunakan proses-proses dalam domain DSS COBIT 2019, khususnya DSS03, DSS04, DSS05, dan DSS06, dengan mengacu pada model kapabilitas COBIT untuk mengevaluasi sejauh mana kemampuan proses yang sedang berjalan. Hasil dari fase ini digunakan sebagai dasar untuk mengidentifikasi kesenjangan (*gap*) antara keadaan saat ini dengan praktik terbaik yang diharapkan sebagai landasan penyusunan rekomendasi perbaikan pada fase selanjutnya.

Table 5. Gap Analysis DSS03

No	Aktivitas	*Level Capability Existing*	*Level Capability Targeting*	GAP
1	DSS03.01 *Identify and classify problems*	2	2	Tidak memiliki *gap*
2	DSS03.02 *Investigate and diagnose problems*	3	3	Tidak memiliki *gap*
3	DSS03.03 *Raise known errors*	2	2	Tidak ada pencatatan *known-error record* dan tidak ada pengembangan solusi sementara (*workaround*)

				setelah *root cause* diidentifikasi
4	DSS03.04 *Resolve and close problems*	N.A	5	Practice ini tidak relevan
5	DSS03.05 *Perform proactive problem management*	N.A	4	Practice ini tidak relevan

Tabel 5 menyajikan analisis kesenjangan tingkat kapabilitas pada proses DSS03 (*Managed Problems*). Secara umum, sebagian besar aktivitas telah mencapai tingkat kapabilitas yang ditargetkan dan tidak menunjukkan kesenjangan yang signifikan. Namun, pada aktivitas DSS03.03 (*Raise Known Errors*) masih terdapat kekurangan berupa belum adanya pencatatan *known-error record* dan pengembangan *workaround*. Sementara itu, aktivitas DSS03.04 dan DSS03.05 dinyatakan tidak relevan sehingga tidak dianalisis lebih lanjut.

Table 6.Gap Analysis DSS04

No	Aktivitas	Level Capability Existing	Level Capability Targeting	GAP
1	DSS04.01 *Define the business continuity policy, objectives and scope*	2	2	Tidak memiliki *gap*
2	DSS04.02 *Maintain business resilience*	3	3	Tidak ada analisis formal *Business Impact Analysis* (BIA). Tidak ditetapkan waktu minimum pemulihan layanan. Tidak didefinisikan kondisi atau penanggung jawab aktivasi *continuity plan*. Tidak ada identifikasi biaya rinci dan rekomendasi strategis berbasis opsi teknis
3	DSS04.03 *Develop and implement a business continuity response*	3	3	Tidak ada kewajiban *supplier* memiliki *continuity plan*. Tidak ada prosedur *recovery* untuk pemulihan layanan. Tidak ada BCP atau DRP yang mendefinisikan pemrosesan sementara atau integrasi dengan rencana penyedia *outsource*. Tidak ada identifikasi sumber daya pendukung *recovery*. Tidak ada persyaratan *backup* yang terdokumentasi. Tidak ada distribusi rencana keberlanjutan secara aman ke pihak berwenang atau jaminan akses pada semua skenario bencana
4	DSS04.04 *Exercise, test and review the BCP and DRP*	N.A	5	Practice ini tidak relevan
5	DSS04.05 *Review, maintain and improve the*	3	3	Tidak memiliki *gap*

	continuity plans			
6	DSS04.06 *Conduct continuity plan training*	N.A	4	Tidak Practice ini tidak relevan
7	DSS04.07 *Manage backup arrangements*	2	2	Tidak memiliki *gap*
8	DSS04.08 *Conduct post-incident review*	N.A	5	Practice ini tidak relevan

Tabel 6 menampilkan analisis kesenjangan tingkat kapabilitas pada proses DSS04 (*Managed Continuity*). Secara umum, sebagian besar aktivitas telah mencapai tingkat kapabilitas yang ditargetkan dan tidak menunjukkan kesenjangan yang signifikan. Namun, pada aktivitas DSS04.02 (*Maintain Business Resilience*) dan DSS04.03 (*Develop and Implement a Business Continuity Response*) masih terdapat kekurangan, terutama terkait ketiadaan *Business Impact Analysis* (BIA) formal, penetapan waktu pemulihan layanan, dokumentasi BCP/DRP, serta integrasi rencana keberlanjutan dengan pihak penyedia layanan.

Table 7. Gap Analysis DSS05

No	Aktivitas	Level Capability Existing	Level Capability Targeting	GAP
1	*DSS05.01 Protect against malicious software*	4	4	Beberapa kebijakan dan prosedur keamanan masih bersifat umum dan belum mencakup detail teknis seperti proteksi *malware* terpusat, peninjauan rutin terhadap *advisories* vendor, atau pembaruan *patch* perangkat lunak secara otomatis
2	*DSS05.02 Manage network and connectivity security*	4	4	Tidak memiliki *gap*
3	*DSS05.03 Manage endpoint security*	3	3	Tidak memiliki *gap*
4	*DSS05.04 Manage user identity and logical access*	4	4	Tidak memiliki *gap*
5	*DSS05.05 Manage physical access to I&T assets*	3	3	Tidak memiliki *gap*
6	*DSS05.06 Manage sensitive documents and output devices*	3	3	Tidak memiliki *gap*
7	*DSS05.07 Manage vulnerabilities and monitor infrastructure*	3	3	Tidak memiliki *gap*

Tabel 7 menyajikan analisis kesenjangan tingkat kapabilitas pada proses DSS05 (*Managed Security Services*). Secara umum, seluruh aktivitas telah mencapai tingkat kapabilitas yang ditargetkan dan tidak menunjukkan kesenjangan yang signifikan. Namun, pada aktivitas DSS05.01 (*Protect Against Malicious Software*) masih terdapat kekurangan berupa kebijakan dan prosedur keamanan yang belum mencakup detail teknis secara menyeluruh, seperti pengelolaan proteksi malware terpusat, peninjauan rutin vendor advisories, serta mekanisme pembaruan patch perangkat lunak secara otomatis. Aktivitas lainnya dinyatakan telah sesuai dengan target yang ditetapkan.

Table 8. Gap Analysis DSS06

No	Aktivitas	Level Capability Existing	Level Capability Targeting	GAP
1	*DSS06.01 Align control activities with enterprise objectives*	2	2	Tidak memiliki *gap*
2	*DSS06.02 Control the processing of information*	2	2	Tidak memiliki *gap*

3	*DSS06.03 Manage roles, responsibilities, and access privileges*	2	2	Tidak memiliki *gap*
4	*DSS06.04 Manage errors and exceptions*	2	2	Tidak memiliki *gap*
5	*DSS06.05 Ensure traceability and accountability*	2	2	Tidak memiliki *gap*
6	*DSS06.06 Secure information assets*	2	2	Tidak memiliki *gap*

Tabel 8 menunjukkan analisis kesenjangan tingkat kapabilitas pada proses DSS06 (*Managed Business Process Controls*). Hasil analisis memperlihatkan bahwa seluruh aktivitas pada proses ini telah mencapai tingkat kapabilitas yang ditargetkan, yaitu level 2, sehingga tidak ditemukan kesenjangan yang signifikan. Hal ini menunjukkan bahwa pengendalian proses bisnis berbasis TI telah diterapkan secara konsisten sesuai dengan kebutuhan organisasi.

Fase selanjutnya berfokus pada penyusunan rekomendasi perbaikan tata kelola TI. Rekomendasi dirancang untuk menutup kesenjangan yang ditemukan dengan memperhatikan aspek people, process, dan technology, sehingga dapat diimplementasikan secara bertahap dan berkelanjutan..

Table 9. *Potential Improvement*

Aspect	*Type*	Keterangan
People	*Roles*	Menambahkan detail spesifik mengenai peran yang berbeda dalam organisasi, serta bagaimana masing -masing dan berinteraksi dalam pelaksanaan tata kelola dan manajemen TI.
	Resposibility	Menambahkan tanggung jawab utama untuk setiap peran dalam menjalankan tugas dan wewenang dalam pengambilan keputusan serta pelaporan.
	Skill & Awareness	Rekomendasi pelatihan, peningkatan kapasitas, dan kesadaran untuk memastikan kompetensi personel sesuai dengan peran dan mendukung proses dari tata kelola TI.
	Communication	Menambahkan mekanisme komunikasi yang jelas, baik dalam bentuk rapat, laporan, atau sistem pelaporan digital antar unit peran.
Process	*Policy*	Menambahkan kebijakan formal yang menjadi acuan bagi pengambilan keputusan, pengendalian risiko, dan pelaksanaan praktik operasional dalam pengelolaan TI.
	Procedures	Menambahkan langkah – langkah prosedural yang sistematis dalam pelaksanaan suatu aktivitas, termasuk siapa yang bertanggung jawab dan bagaimana proses itu dilakukan.
	Work Instruction	Menambahkan panduan kerja teknis dan instruksi detail dalam bentuk dokumentasi operasional untuk mendukung pelaksanaan tugas harian.
	Record	Menambahkan pencatatan hasil kegiatan atau dokumentasi yang mendukung keandalan proses dan sebagai bukti audit atau monitoring.
Technology	*Tools*	Menambahkan alat bantu digital dan sistem otomatisasi (seperti audit tools, SIEM, atau monitoring platform) yang digunakan untuk mendukung efektivitas proses dan

Aspect	*Type*	Keterangan
		keputusan TI.
	Features	Menambahkan fitur atau fungsi dari sistem TI yang meningkatkan efisiensi keamanan, dan akurasi layanan.

Seluruh proses dalam tabel ini merupakan panduan metodologis yang dirancang untuk menghasilkan rekomendasi yang tidak hanya berbasis analisis teoretis, tetapi juga telah divalidasi melalui keterlibatan langsung dengan stakeholder, sehingga relevan terhadap konteks institusi dan mendukung pencapaian transformasi digital secara berkelanjutan.

A. Singkatan dan Akronim

Meskipun sebuah akronim atau singkatan telah didefinisikan dalam abstrak, definisikan kembali pada penggunaan pertama dalam teks. Tidak perlu menyebutkan singkatan seperti IEEE, SI, MKS, CGS, sc, dc, dan rms. Kecuali benar-benar diperlukan, hindari penggunaan akronim dalam judul atau header.
Beberapa singkatan yang digunakan antara lain:

- TI – Teknologi Informasi
- DSR – *Design Science Research*
- COBIT – *Control Objectives for Information and Related Technology*
- DSS – *Deliver, Service, and Support*
- FGD – *Focus Group Discussion*

IV. HASIL DAN PEMBAHASAN

Penelitian ini mengevaluasi tata kelola Teknologi Informasi (TI) pada Pemerintah Provinsi XYZ memanfaatkan framework COBIT 2019 dengan fokus pada dommain Deliver, Service, and Support (DSS), meliputi proses DSS03, DSS04, DSS05, dan DSS06. Proses asesmen dilakukan menggunakan assessment template COBIT 2019 berdasarkan hasil analisis design factor yang menunjukkan relevansi tinggi terhadap kebutuhan transformasi digital dan keberlangsungan layanan TI.

Hasil penilaian menunjukkan bahwa secara umum tingkat keahlian proses berada pdaa level 2 (Managed Process). Gap analysis mengidentifikasi kesenjangan utama pada proses DSS03 dan DSS04, terutama terkait dokumentasi, pencatatan known-error, Business Impact Analysis (BIA), serta penyusunan Busines Continuity Plan (BCP) dan Disaster Recovery Plan (DRP). Sementara itu, proses DSS05 dan DSS06 telah mencapai target kapabilitas, meskipun masih diperlukan penguatan pada aspek kebijakan teknis.

Berdasarkan temuan tersebut, disusun rekomendasi perbaikan yang berfokus pada 3 aspek utama, yaitu:

- *People*: meliputi perbaikan pada tanggung jawab peran, pelatihan dan kesadaran staf, serta mekanisme komunikasi yang lebih efektif antarunit;

Table 10. Rekomendasi Aspek *People (Responsibility)*

No.	Rekomendasi
DSS04.03 Develop and implement a business continuity response	
1.	Menetapkan tanggung jawab untuk memastikan semua sumber daya yang mendukung *recovery* (seperti SDM, infrastruktur, perangkat keras, dan perangkat lunak) sudah siap digunakan dalam prosedur *recovery*. Setiap tim harus bertanggung jawab untuk menjaga aksesibilitas data dan sistem dalam semua skenario bencana.

Table 11. Rekomendasi Aspek *People (Roles)*

No	Skill Area	Level	Practice	Rekomendasi
1	*Problem Management* (PBMG)	5	DSS03.03	Menambahkan peran Staf Pengelola Insiden dan Masalah TI di bawah Bidang Aplikasi Informatika untuk mendokumentasikan *known-error record* serta mengembangkan solusi sementara (*workaround*) menggunakan platform digital kolaboratif
2	*Business Continuity Management* (BUCO)	5	DSS04.02	Menambahkan peran Koordinator *Business Continuity Planning* (BCP) di bawah Bidang E-Government untuk mengelola analisis *Business Impact Analysis* (BIA), menentukan waktu pemulihan layanan minimum, serta menyusun rencana keberlanjutan layanan digital lintas bidang
3	*IT Service Continuity* (ITSC)	5	DSS04.03	Menambahkan peran Staf Pemulihan Layanan TI di bawah Bidang Persandian dan Keamanan Informasi untuk memastikan kesiapan *supplier* dan penyedia layanan dalam menjalankan prosedur *recovery* serta verifikasi kesiapan sistem dan infrastruktur pada semua skenario bencana
4	*Information Security* (SCTY)	5	DSS05.01	Menambahkan peran *Chief Information Security Officer* (CISO) di bawah Bidang Persandian dan Keamanan Informasi untuk mengembangkan kebijakan keamanan informasi, memperbarui definisi *malware*, serta melakukan koordinasi pemantauan keamanan dengan vendor secara berkelanjutan

Table 12. Rekomendasi Aspek *People (Skill&Awaerness))*

No	Rekomendasi	Keterampilan	Pelatihan dan Sertifikasi
1	Melaksanakan pelatihan *Business Impact Analysis* (BIA) untuk meningkatkan kemampuan identifikasi risiko	*Business Continuity Management* (BUCO)	(1) Pelatihan *Business Continuity Planning and Disaster Recovery*; (2) Sertifikasi CBCP (*Certified Business*

	operasional dan penentuan waktu pemulihan layanan minimum (RTO/RPO)		*Continuity Professional*)
2	Mengadakan pelatihan koordinasi dan komunikasi tanggap darurat TI untuk memastikan kesiapan tim teknis dalam aktivasi *continuity plan* dan koordinasi lintas bidang saat krisis	*Incident Management & Coordination* (USUP)	(1) Pelatihan *Crisis and Incident Response Management*; (2) Sertifikasi ITIL 4 *Specialist: Incident, Problem & Change Management*
3	Menyelenggarakan pelatihan pemantauan infrastruktur dan sistem digital untuk mendukung proses pemulihan dan menjaga keandalan layanan TI selama fase pemulihan	*IT Infrastructure Monitoring* (ITOP)	(1) Pelatihan *Infrastructure Monitoring and Recovery Operations*; (2) Sertifikasi CompTIA Server+ atau Microsoft Certified: Azure Administrator Associate
4	Melaksanakan *workshop* penggunaan platform digital kolaboratif untuk memperkuat koordinasi antar tim dan *monitoring* pelaksanaan *continuity plan* secara *real-time*	*Digital Collaboration* (COLM)	(1) Pelatihan *Collaborative Tools for Continuity and Crisis Management*; (2) Sertifikasi Microsoft Teams Collaboration Expert atau Google Workspace Administrator

- Process: penambahan kebijakan formal, prosedur standar, instruksi kerja teknis, serta sistem pencatatan kegiatan yang akuntabel;

Table 13. Aspek *Process (Procedure)*

No	Practice / Proses COBIT 2019	Rekomendasi
1	DSS03.03 – Raise Known Errors	Menyusun prosedur pengelolaan known-error record yang dilakukan segera setelah akar penyebab masalah diidentifikasi. Prosedur ini mencakup pembuatan known-error record, dokumentasi solusi sementara, serta identifikasi solusi permanen berdasarkan analisis dampak bisnis. Prosedur ini perlu diintegrasikan dengan manajemen perubahan dan sistem manajemen insiden agar permasalahan serupa dapat diminimalkan di masa mendatang
2	DSS04.02 – Maintain Business Resilience	Mengembangkan prosedur evaluasi dan pemeliharaan ketahanan bisnis yang berfokus pada pemilihan strategi yang efisien dan layak untuk menjamin kesinambungan layanan, pemulihan bencana, serta respons insiden besar. Prosedur ini harus mencakup penilaian risiko, analisis efektivitas biaya, serta langkah mitigasi terhadap potensi gangguan operasional
3	DSS04.03 – Develop and Implement a Business Continuity Response	Menyusun prosedur pengembangan dan penerapan Business Continuity Plan dan Disaster Recovery Plan berdasarkan strategi ketahanan organisasi. Prosedur ini harus mendokumentasikan langkah-langkah penting agar instansi dapat melanjutkan kegiatan kritikal selama atau setelah gangguan besar terjadi, termasuk mekanisme koordinasi antarunit, pengujian berkala, dan pelaporan hasil pemulihan layanan
4	DSS05.01 – Protect Against Malicious Software	Menetapkan prosedur perlindungan terhadap perangkat lunak berbahaya yang mencakup deteksi, pencegahan, dan pemulihan dari ancaman seperti ransomware, malware, virus, dan spyware. Prosedur ini harus mencakup pembaruan otomatis patch, pemindaian keamanan terjadwal, serta kebijakan penggunaan perangkat yang aman sesuai pedoman keamanan SPBE dan ISO/IEC 27001

Table 14. Aspek *Process (Policy)*

No	Proses (Policy)	Tanggung Jawab	Penjelasan
1	DSS04.02 – Maintain Business Resilience	Menetapkan kebijakan yang mewajibkan pelaksanaan Business Impact Analysis secara	Kebijakan ini bertujuan untuk memastikan seluruh unit kerja melakukan penilaian risiko dan

		berkala untuk menilai dampak gangguan terhadap layanan penting. Mengatur tanggung jawab antarunit kerja dalam menentukan strategi ketahanan bisnis dan evaluasi efektivitasnya	dampak gangguan layanan secara terukur, serta memilih strategi ketahanan bisnis yang efisien dan layak guna menjamin kesinambungan layanan publik saat terjadi bencana atau gangguan besar
2	DSS04.03 – Develop and Implement a Business Continuity Response	Menetapkan kebijakan formal yang mengharuskan setiap supplier atau mitra outsource memiliki Business Continuity Plan dan Disaster Recovery Plan yang terdokumentasi dan diverifikasi secara rutin. Mengatur mekanisme audit dan evaluasi berkala untuk memastikan kepatuhan terhadap rencana keberlanjutan layanan	Kebijakan ini bertujuan untuk menjamin bahwa semua pihak eksternal yang mendukung layanan pemerintah memiliki rencana keberlanjutan yang memadai, termasuk prosedur backup data, recovery plan, dan pelaporan insiden, sehingga risiko gangguan layanan akibat pihak ketiga dapat diminimalkan

- Technology: penerapan alat bantu pemantauan keamanan dan layanan TI, dashboard monitoring risiko, serta integrasi sistem dengan penyedia layanan pihak ketiga untuk mendukung keberlangsungan layanan.

Table 15. Aspek *Technology (Tools)*

No	Rekomendasi
DSS03.03 — Raise Known Errors	
1.	Menerapkan platform manajemen masalah berbasis cloud untuk mendukung pencatatan known-error record, penyimpanan workaround, serta integrasi alur kerja penanganan masalah antarunit.
DSS04.02 — Maintain Business Resilience	
2.	Mengembangkan platform terpusat untuk pencatatan biaya dan rekomendasi strategis setiap opsi teknis pemulihan layanan guna mendukung pengambilan keputusan yang cepat dan terukur.
DSS04.03 — Develop and Implement a Business Continuity Response	
3.	Membangun sistem digital terpusat untuk memantau status backup serta implementasi BCP/DRP pada setiap penyedia layanan atau mitra outsourcing.
DSS05.01 — Protect Against Malicious Software	
4.	Mengimplementasikan sistem proteksi malware terpusat yang mendukung pembaruan otomatis, pemantauan ancaman, dan pengendalian keamanan endpoint secara terintegrasi.

Table 16. Aspek *Technology (Features)*

No	Rekomendasi Kontrol Teknologi	Rekomendasi Features	Deskripsi
DSS03.03 – Raise Known Errors			
1	Mengaktifkan fitur otomasi pencatatan known-error record dan penerapan workaround dalam sistem manajemen insiden	Fitur Automated Known-Error Logging dan Workaround Tracking	Fitur ini secara otomatis membuat known-error record, mencatat akar masalah, melacak solusi sementara, dan memberikan notifikasi real-time kepada tim untuk mempercepat proses penyelesaian masalah
DSS04.02 – Maintain Business Resilience			
2	Menggunakan fitur simulasi pemulihan digital untuk mendukung analisis strategi ketahanan layanan	Fitur Resilience Scenario Simulation dan RTO Calculator	Fitur ini menyediakan simulasi skenario gangguan, perhitungan otomatis Recovery Time Objective, serta rekomendasi strategi pemulihan paling optimal berdasarkan data operasional
DSS04.03 – Develop and Implement a Business Continuity Response			
3	Mengaktifkan fitur monitoring otomatis untuk melacak status backup dan validasi BCP/DRP setiap unit dan mitra outsourcing	Fitur Automated Backup Monitoring dan DRP Validation Dashboard	Fitur ini memverifikasi backup harian, memantau kesiapan rencana pemulihan, memberikan

			peringatan otomatis atas kegagalan backup, serta menampilkan status pemulihan melalui dashboard terpadu
DSS05.01 – Protect Against Malicious Software			
4	Mengaktifkan fitur pembaruan definisi malware otomatis dan deteksi ancaman real-time pada seluruh perangkat	Fitur Auto Malware Definition Update & Real-Time Threat Detection	Fitur ini memperbarui definisi malware secara otomatis, mendeteksi ancaman secara real-time, melakukan karantina file berbahaya, serta meninjau security advisories vendor untuk menentukan patch keamanan yang diperlukan

Rancangan solusi ini diharapkan dapat meningkatkan kapabilitas proses tata kelola TI secara bertahap hingga mencapai level 3 (Established Process), serta mendukung terwujudnya tata kelola TI yang andal, terintegrasi, dan mendukung transformasi digital Pemerintah Provinsi XYZ.

V. KESIMPULAN

Berdasarkan hasil penelitian mengenai perancanga tata kelola teknologi informasi (TI) untuk membantu proses transformasi digital di Pemerintah Provinsi XYZ menngunakan kerangka kerja COBIT 2019, diperoleh beberapa simpulan penting. Kondisi eksisting tata kelola TI pada domain Deliver, Service, and Support (DSS) menunjukkan bahwa proses-proses utama, yaitu DSS03 (Managed Problems), DSS04 (Managed Continuity), DSS05 (Managed Security Services), dan DSS06 (Managed Business Process Controls) masih memiliki kesenjangan terhadap tingkat kapabilitas yang diharapkan. Hasil asesmen menunjukkan bahwa rata-rata tingkat kapabilitas proses brada pada level 2 (Managed Process), yang menandakan bahwa prosess telah berjalan namun tidak sepenuhnya terstandarisasi dan terdokumentasi dengan optimal.

Perbandingan antara kondisi eksisting dan rancangan tata kelola TI yang diusulkan menunjukkan bahwa penerapan solusi secara sistematis dan berkelanjutan berpotensi meningkatkan kapabilitas proses menuju level 3 (Established Process). Rancangan tata kelola TI ini juga berhasil mengidentifikasi tantangan utama serta merumuskannya ke dalam sejumlah inisiatif strategis yang dikategorikan ke dalam tiga aspek, yakni people, process, dan technology. Seluruh inisiatif tersebut disusun dalam roadmap implementasi sebagai upaya untuk memperkuat pengelolaan layanan TI, meningkatkan keberlangsungan dan keamanan operasional, serta mendukung transformasi digital dan peningkatan kualitas layanan publik di lingkungan Pemerintah Provinsi XYZ.

REFERENSI

[1] Rohimat, “Peran Teknologi Informasi dalam Pembangunan dan Tata Kelola Pemerintahan,” 2021.

[2] Rachmatullah, dkk., “Pemanfaatan Teknologi Digital dalam Pelayanan Publik,” 2022.

[3] Setyasih, “Tantangan Transformasi Digital pada Pemerintah Daerah,” 2022.

[4] Putri Efilda, dkk., “Penerapan Framework COBIT 2019 dalam Tata Kelola Teknologi Informasi,” 2023.

[5] ISACA, COBIT® 2019 Framework: Governance and Management Objectives, ISACA, 2019