Optimalisasi Transformasi Digital Telco Melalui *Cloud Governance* Dengan Pendekatan *Ambidextrous* Menggunakan Cobit 2019 Tradisional Dan *Focus Area*: *Devops*

1st Aria Riezki Fhadila
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
riezkiaria@student.telkomuniversity.ac.id

2nd Rohmat Saeduddin
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
rdrohmat@telkomuniversity.ac.id

3rd Rahmat Mulyana
Dept. of Computer and Systems
Universitas Stockholm
Stockholm, Swedia
rahmat@dsv.su.se

Penelitian ini bertujuan untuk mengoptimalkan transformasi digital di TelCo melalui penerapan *cloud governance* dengan pendekatan *ambidextrous* yang mengintegrasikan COBIT 2019 Tradisional dan *Focus Area: DevOps*. Transformasi digital memainkan peran penting dalam mendukung keberlanjutan dan daya saing perusahaan di era digital, meskipun menghadirkan tantangan terkait tata kelola teknologi informasi, keamanan, dan kepatuhan terhadap regulasi. *Framework* COBIT 2019 digunakan untuk mengevaluasi kapabilitas dan kesenjangan dalam implementasi *cloud governance* di TelCo, dengan fokus pada DSS05: *Managed Security Services*, DSS04: *Managed Continuity*, dan BAI08: *Managed Knowledge*. Berdasarkan analisis gap, penelitian ini merekomendasikan sembilan perbaikan, termasuk penguatan otomatisasi, peningkatan rencana kontinuitas bisnis berbasis *cloud*, serta pengembangan keterampilan terkait *DevOps* dan *cloud native technologies*. Hasil perbandingan tingkat kemampuan sebelum dan setelah perbaikan menunjukkan peningkatan signifikan, dengan skor total meningkat dari 3.52 menjadi 3.89. Peningkatan ini mencerminkan dampak positif dari inisiatif yang telah diimplementasikan, terutama dalam pengelolaan keamanan, kontinuitas bisnis, dan pengelolaan pengetahuan, sesuai dengan fokus pada DSS05, DSS04, dan BAI08, yang mendukung transformasi digital TelCo yang lebih aman, berkelanjutan, dan efisien.

Kata kunci— Transformasi Digital, *Design Science Research*, Penyusunan Tata Kelola TI, COBIT 2019 *Focus Area: DevOps*, TelCo.

I. PENDAHULUAN

Kemajuan teknologi yang pesat telah mempercepat transformasi digital (TD) di berbagai industri, mendorong organisasi untuk mengadopsi teknologi inovatif demi mempertahankan daya saing dan efisiensi operasional [1]. Di sektor telekomunikasi, TD mengubah pemanfaatan *cloud* untuk efisiensi, pengalaman pelanggan, dan inovasi berkelanjutan, memerlukan tata kelola yang skalabel dan *agile* [2]. Seiring meningkatnya kompleksitas layanan *cloud*, strategi tata kelola yang kuat menjadi krusial untuk mengelola risiko, memastikan kepatuhan, dan mendukung inovasi [3], [4]. *Cloud Governance* modern perlu mengintegrasikan aspek *cybersecurity*, evaluasi risiko, dan sertifikasi, sekaligus menyeimbangkan fleksibilitas dan kontrol [5]. Meski TelCo mulai memanfaatkan teknologi seperti *big data* dan IoT, adopsi model Tata Kelola Teknologi Informasi (TKTI) seperti COBIT 2019 masih terbatas, terutama dalam mendukung kebutuhan *agility cloud* [6]. Konsep TKTI *ambidextrous* yang memadukan kontrol tradisional dan praktik *DevOps* dinilai efektif mendukung TD, namun penerapannya di TelCo masih minim [7], [8].

Penelitian ini mengevaluasi dan meningkatkan kapabilitas *cloud governance* di TelCo melalui integrasi COBIT 2019 dan *DevOps*, dengan studi kasus untuk menilai kematangan GMO, mengidentifikasi *gap*, dan menyusun rekomendasi perbaikan prioritas.

II. KAJIAN TEORI

A. Transformasi Digital (TD)

Transformasi Digital (TD) merupakan perubahan kompleks mencakup teknologi, adaptasi sosial, dan kelembagaan, mengubah penciptaan nilai lewat SMACIT (Social, Mobile, Analytics, Cloud, IoT), yang memengaruhi perilaku konsumen dan persaingan [9]. Meski mendorong efisiensi dan pertumbuhan bisnis, TD juga meningkatkan risiko operasional seperti kegagalan sistem dan ancaman keamanan, sehingga perlu dikelola secara proaktif [10].

B. *Cloud Governance*

Cloud governance adalah disiplin pengelolaan teknologi cloud untuk menjamin keamanan, privasi, dan kepatuhan hukum [4]. Tata kelola ini mencakup struktur organisasi, proses, dan kebijakan yang dirancang untuk menghadapi tantangan dan peluang *cloud*, serta memastikan keselarasan dengan TKTI dan tujuan bisnis [11].

C. Tata Kelola Teknologi Informasi *Ambidextrous*

TKTI ambidextrous adalah kombinasi sinergis antara mekanisme agile-adaptive dan tradisional yang

menyeimbangkan fleksibilitas dan inovasi dengan stabilitas dan efisiensi, guna mengoptimalkan risiko dan sumber daya TI untuk pencapaian nilai strategis. Pendekatan ini memungkinkan percepatan inovasi tanpa mengabaikan kepatuhan dan kontrol risiko [12]. Struktur, proses, dan relasi dalam TKTI berperan penting dalam menyelaraskan strategi, mendorong inovasi teknologi, dan memperkuat kapabilitas organisasi. Elemen seperti kepemimpinan eksekutif, strategi arsitektur, manajemen data, serta kolaborasi lintas fungsi sangat memengaruhi keberhasilan TD dan kinerja organisasi [7], [13].

D. COBIT 2019 dan *Focus Area*: *DevOps*

COBIT 2019 adalah kerangka TKTI komprehensif yang menyelaraskan pengelolaan teknologi informasi (TI) dengan tujuan bisnis melalui domain tata kelola dan manajemen yang terstruktur [12], [13]. *Focus Area*: *DevOps* dalam COBIT 2019 mengintegrasikan prinsip *DevOps* untuk mendorong *agility*, kolaborasi, dan *continuous delivery* melalui lima pilar CALMS (*Culture, Automation, Lean, Measurement, Sharing*) [14], [15]. Integrasi ini memperkuat *cloud governance* dengan mendukung iterasi cepat, *delivery* andal, dan manajemen risiko yang adaptif tanpa menghambat inovasi [16].

E. Penelitian Terdahulu

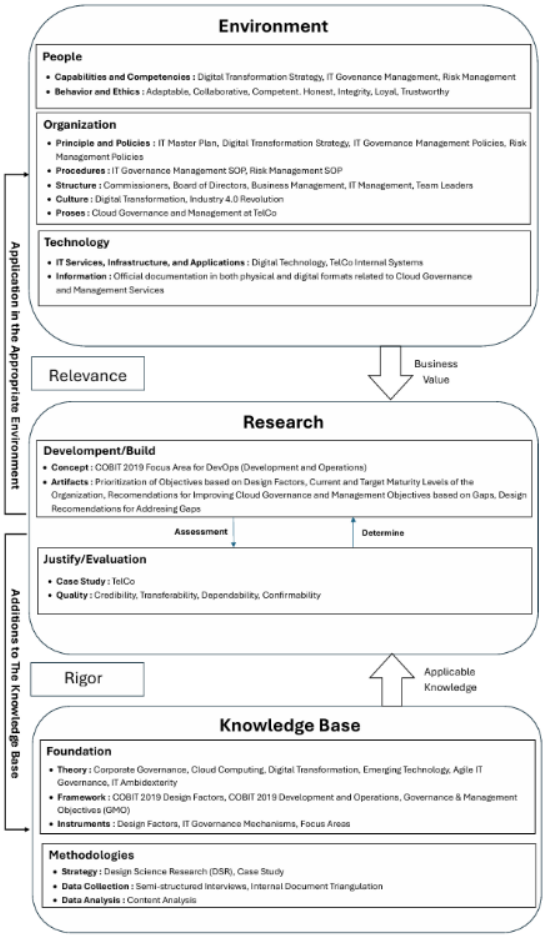
Penelitian ini mengacu pada tiga studi utama untuk memandu penilaian dan prioritisasi *Governance and Management Objectives* (GMO) dalam *cloud governance*. Studi pertama menekankan peran yang jelas, integrasi dengan strategi keamanan siber, serta evaluasi dan sertifikasi berkelanjutan [4]. Studi kedua menyoroti tantangan keamanan data di *cloud multi-tenant*, pentingnya enkripsi, manajemen akses, dan pemantauan berkelanjutan [17]. Studi ketiga membandingkan berbagai kerangka keamanan *cloud* dan menegaskan perlunya pendekatan adaptif yang menggabungkan kontrol akses granular, enkripsi, monitoring, dan respons insiden [18]. Ketiga studi ini membentuk dasar yang kuat untuk menyusun GMO yang responsif terhadap tantangan strategis dan teknis TD di TelCo.

F. Regulasi

Penelitian ini merujuk pada dua regulasi penting di Indonesia yang relevan bagi TelCo. Peraturan Menteri BUMN No. 3/2023 memberikan panduan menyeluruh terkait tata kelola dan aktivitas korporasi strategis di BUMN, dengan penekanan pada manajemen risiko dan keselarasan dengan tujuan organisasi. Sementara itu, Peraturan Menteri KOMINFO No. 5/2021 tentang Penyelenggaraan Telekomunikasi menetapkan standar keamanan dan operasional di sektor telekomunikasi, mencakup perlindungan data, kontinuitas layanan, dan manajemen insiden. Kepatuhan terhadap regulasi ini penting untuk memastikan legalitas, meningkatkan keamanan, dan mendukung proses TD.

III. METODE

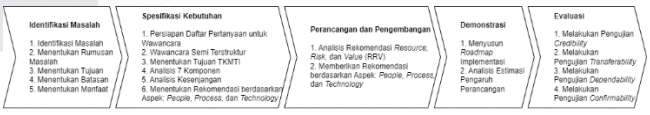
Penelitian ini menggunakan pendekatan studi kasus kualitatif yang didasarkan pada *Design Science Research* (DSR), yang bertujuan mengembangkan dan mengevaluasi model TKTI *ambidextrous* untuk optimalisasi *cloud*



Gambar 1 *Design Science Research [19]*

governance dan TD di TelCo. Pendekatan ini sesuai untuk mengkaji fenomena kompleks dalam konteks nyata, khususnya untuk menjawab pertanyaan "*how*" dan "*why*" [19], [20]. Gambar 1 menyajikan kerangka konseptual yang menggambarkan tahapan berurutan dan umpan balik dalam desain penelitian.

Gambar 1 menunjukkan kerangka DSR yang terdiri dari tiga elemen: *environment* (organisasi dan masalah), *research activities* (pengembangan dan evaluasi artefak), dan *knowledge base* (teori dan penelitian sebelumnya) [19]. Berdasarkan dasar tersebut, Gambar 2 menjelaskan metodologi penelitian terstruktur dalam lima fase berurutan, mulai dari identifikasi masalah hingga evaluasi dan validasi.



Gambar 2 Sistematika Penelitian

Berdasarkan Gambar 2. penelitian ini mengikuti lima fase: identifikasi masalah, perancangan solusi, pengembangan rekomendasi berbasis *people-process-technology*, penyusunan roadmap implementasi, dan evaluasi validitas multi-aspek. Pendekatan ini menghasilkan kerangka tata kelola adaptif untuk menghadapi kompleksitas *cloud*.

Penelitian ini menggabungkan wawancara semi-terstruktur dengan enam pemangku kepentingan TelCo dan analisis dokumen internal-eksternal untuk memastikan triangulasi dan validitas data [21]. Evaluasi dilakukan

terhadap tujuh komponen COBIT 2019 guna menilai kapabilitas dan keselarasan dengan tujuan *cloud governance* berbasis TKTI *ambidextrous*, serta mengidentifikasi kekuatan dan celah kritis. Hasil analisis digunakan untuk merumuskan rekomendasi peningkatan efektivitas tata kelola, manajemen risiko, dan mendukung transformasi digital TelCo [22].

IV. HASIL DAN PEMBAHASAN

A. Penentuan Prioritas Tujuan *Cloud Governance*

Penelitian ini memprioritaskan domain COBIT 2019 *Focus Area: DevOps* berdasarkan desain, regulasi, dan studi sebelumnya. Tabel 1 menunjukkan hasil akhir prioritisasi tersebut.

Tabel 1 Nilai Hasil Prioritasi

Acuan Kriteria	DSS05	DSS04	BAI08
COBIT 2019 *Focus Area*: *DevOps*	67	67	100
COBIT 2019 *Design Factor*	100	70	30
Peraturan Menteri KOMINFO No. 5/2021	100	100	100
Peraturan Menteri BUMN No. 3/2023	100	100	100
Cloud Governance	100	100	100
Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy	100	100	100
An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions	100	100	50
Akumulasi Bobot:	95	91	90

Hasil pada Tabel 1 menunjukkan DSS05 memiliki skor tertinggi (95), disusul dengan DSS04 (91), dan BAI08 pada skor (90).

B. Hasil Penilaian Tujuh Komponen

1. Komponen Proses

Tabel *2* menunjukkan setiap penilaian capaian dan tingkat kapabilitas untuk DSS05, DSS04, dan BAI08.

Tabel 2 Analisis Komponen Proses

DSS05				
No	**Aktivitas**	**Pencapaian**	**Tingkat Kemampuan**	**Target**
1	DSS05.01	100%	2	4
		100%	3	
		100%	4	
2	DSS05.02	100%	2	
		100%	3	
		100%	4	
3	DSS05.03	100%	2	
		100%	3	
		100%	4	
4	DSS05.04	100%	2	
		100%	3	
		83%	4	
5	DSS05.05	100%	2	
		100%	3	
		100%	4	
6	DSS05.06	100%	2	
		100%	3	
		50%	4	
7	DSS05.07	100%	2	
		100%	3	
Tingkat Kemampuan DSS05:			**4**	
DSS04				
1	DSS04.01	100%	2	3
		100%	3	
		50%	4	
2	DSS04.02	92%	2	
		90%	3	
3	DSS04.03	100%	2	
		100%	3	
		100%	4	
4	DSS04.04	100%	2	
		100%	3	
		100%	4	
		100%	5	
5	DSS04.05	100%	3	
6	DSS04.06	100%	2	
		100%	3	
		100%	4	
7	DSS04.07	92%	2	
		100%	3	
8	DSS04.08	100%	3	
		100%	4	
		100%	5	
Tingkat Kemampuan DSS04:			**4**	
BAI08				
1	BAI08.01	100%	2	2
		100%	3	
		100%	4	
2	BAI08.02	100%	2	
		100%	3	
3	BAI08.03	83%	2	
		100%	3	
		100%	4	
		100%	5	
4	BAI08.04	100%	3	
		100%	4	
Tingkat Kemampuan BAI08:			**4**	

2. Komponen Struktur Organisasi

Komponen ini menilai struktur organisasi sebagai pengambil keputusan utama. Tabel 3 menunjukkan tidak adanya kesenjangan pada aspek ini.

Tabel 3 Analisis Komponen Struktur Organisasi

No	Struktur Organisasi COBIT	Tujuan TKTI	Kondisi Eksisting
1	*Executive Committee*	DSS04	Dewan Komisaris
2	*Chief Operating Officer (COO)*	DSS04	Direktur *Network*
3	*Chief Information Officer (CIO)*	BAI08, DSS05, DSS04	Direktur *IT*
4	*Chief Technology Officer (CTO)*	BAI08, DSS04	Direktur *IT*
5	*Chief Information Security Officer (CISO)*	DSS05, DSS04	Direktur *IT*
6	*Chief Digital Officer (CDO)*	BAI08	Direktur Perencanaan & Transformasi
7	*Business Process Owners*	BAI08, DSS05, DSS04	Direktur dan Kepala Divisi Bisnis
8	*Portfolio Manager*	BAI08	*Portfolio Management*
9	*Program Manager*	BAI08	*IT Program Manager*
10	*Project Manager*	BAI08	*Project Manager*
11	*Data Management Function*	BAI08, DSS04	*Big Data Management Platform Division*
12	*Head Architect*	BAI08, DSS04	*Head of IT Enterprise Architecture*

No	Struktur Organisasi COBIT	Tujuan TKTI	Kondisi Eksisting
13	*Head Development*	BAI08, DSS05, DSS04	*Head of Application Development*
14	*Head IT Operations*	BAI08, DSS05, DSS04	*Vice President of IT Operations & Infrastructure Group*
15	*Head IT Administration*	BAI08	*IT Operation and Infrastructure Group*
16	*Service Manager*	BAI08, DSS04	Manajer Layanan TI
17	*Information Security Manager*	BAI08, DSS05, DSS04	Manajer Manajemen Risiko Keamanan TI
18	*Business Continuity Manager*	BAI08, DSS04	Direktorat Keuangan dan Risiko. namun tanggung jawab *cloud continuity* belum dilakukan
19	*Privacy Officer*	BAI08, DSS05,	Direktorat *Finance & Risk Management*
20	*Legal Counsel*	BAI08	*Vice President Corporate Counsel*
21	*Head Human Resources*	DSS05	Direktorat *Human Capital Management*
22	*Product Owner/Manager*	DSS05, DSS04	*Digital Product Solution* atau *Product, Fulfillment and Integration Platforms*
23	*Software Development Manager*	BAI08, DSS05, DSS04	*Corporate Solutions & Cloud CoE* atau *Customer Touchpoint and Digital Product Solution*
24	*Systems Operations Manager*	BAI08, DSS05, DSS04	*Head of IT Operation and Infrastructure Group*
25	*Testing Manager*	DSS05, DSS04	*Head of Quality Assurance & Testing Division*
26	*Release Manager*	DSS05, DSS04	*Corporate Solutions & Cloud CoE*
27	*Automation Manager*	DSS05, DSS04	*IT Operation and Infrastructure Group*
28	*Systems Architect Manager*	BAI08, DSS05, DSS04	*IT Enterprise Architecture and Strategy Group*

3. Komponen Informasi

Tabel 4 menunjukkan dalam DSS05, DSS04, dan BAI08 ditemukan adanya kesenjangan pada komponen informasi.

Tabel 4 Analisis Komponen Informasi

DSS05			
No	**Praktik Manajemen**	***Information Output***	**Kondisi Eksisting**
1.	*DSS05.01*	*Malicious software prevention policy*	Mengevaluasi ancaman malware sesuai ISO/IEC 27001.
		Evaluations of potential threats	Rutin uji kerentanan dan evaluasi.
2.	*DSS04.02*	*Connectivity security policy*	Mematuhi standar *provisioning cloud* dan investasi keamanan.
		Results of penetration tests	Menggandeng *partner* analisis kerentanan.
3.	*DSS05.03*	*Security policies for endpoint devices*	Terdapat kebijakan SOP keamanan *endpoint*.
4.	*DSS05.04*	*Results of reviews of user accounts and privileges*	Review akun dan akses dikelola sesuai standar.
		Approved user access rights	Dikelola otorisasi jelas dan terdokumentasi.
5.	*DSS05.05*	*Access logs*	Log akses dikelola akurat, aman, dan siap audit.
		Approved access requests	Prosedur jelas, terdokumentasi, dan diaudit.
6.	*DSS05.06*	*Access privileges*	Terstruktur dan diaudit.
		Inventory of sensitive documents and devices	Sistematis, diamankan ketat.
7.	*DSS05.07*	*Security incident tickets*	Terstruktur, terdokumentasi, dan responsif.
		Security incident characteristics	Didokumentasikan lengkap dan akurat untuk analisis.
		Security event logs	Dikelola *real-time*, aman, dan dianalisis.

DSS04			
1.	*DSS04.01*	*Policy and objectives for business continuity*	Terintegrasi.
		Assessments of current continuity capabilities and gaps	Dianalisis untuk identifikasi risiko dan mitigasi.
		Disruptive incident scenarios	Ditetapkan untuk mitigasi dan perencanaan kontinuitas.
2.	*DSS04.02*	*Approved strategic options*	Mendukung keputusan strategis.
		BIA	Digunakan untuk memetakan proses kritis.
		Continuity requirements	Dipenuhi lewat *backup*, redundansi, dan pengujian. Namun, TelCo masih mengimplementasikan sebagian *Infrastructure as Code* (IaC) untuk penyediaan dan pemulihan *cloud*.
3.	*DSS04.03*	*Incident response actions and communications*	Dirumuskan dengan jelas.
		BCP	Ditegakkan untuk core billing.
4.	*DSS04.04*	*Test results and recommendations*	*Failover* dan DRP diuji rutin.
		Test exercises	Terdapat latihan BCP dan DRP periodik.
		Test objectives	Menjamin kontinuitas layanan
5.	*DSS04.05*	*Recommended changes to plans*	Diperbarui dengan BCM ISO 22301 dan pemantauan *DevOps*.
		Results of reviews of plans	Didokumentasikan untuk perbaikan berkelanjutan.
6.	*DSS04.06*	*Monitoring results of skills and competencies*	Pelatihan keamanan *cloud* rutin dipantau.

DSS04			
		Training requirements	Ditawarkan, secara periodik.
7.	*DSS04.07*	*Security incident tickets*	Dikelola melalui sistem tiket dengan tim keamanan.
		Test results of backup data	Dilakukan., secara periodik.
		Backup data	Diamankan dengan enkripsi dan redundansi, tanpa version control dan *Infrastructure as Code*.
8.	*DSS04.08*	*Approved changes to the plans*	Didukung SIEM dan CloudWatch.
		Post resumption review report	Disimpan internal dan tidak dibagikan eksternal.
BAI08			
1.	*BAI08.01*	*Classification of information sources*	Dikenali dan teridentifikasi.
2.	*BAI08.02*	*Published Knowledge repositories*	Diterapkan dan menggunakan Google Cloud AI untuk efisiensi.
3.	*BAI08.03*	*Knowledge awareness and training schemes*	Dilaksanakan untuk meningkatkan kesadaran pengetahuan, terutama keamanan dan operasional.
		Knowledge user database	Dicatat sesuai peran dan kebutuhan.
4.	*BAI08.04*	*Rules for Knowledge retirement*	Terdapat penghapusan repositori informasi perangkat karyawan.
		Knowledge use evaluation results	Dilakukan untuk kegunaan, relevansi, dan nilai pengetahuan.

4. Komponen Individu, Keterampilan, dan Kompetensi

Tabel 5 menunjukkan dalam DSS05, DSS04, dan BAI08 ditemukan adanya kesenjangan pada komponen individu, keterampilan, dan kompetensi.

Tabel 5 Analisis Komponen Individu, Keterampilan, dan Kompetensi

No	Praktik Manajemen	Kondisi Eksisting
DSS05		
1.	*Information security*	Melaksanakan patroli siber 24/7.
2.	*Information security management*	Kurangnya evaluasi rutin terhadap efektivitas implementasi manajemen keamanan yang telah diterapkan.
3.	*Penetration testing*	Dilakukan rutin dengan mitra keamanan dan diintegrasikan dalam siklus SDLC.
4.	*Security administration*	Dikelola dengan alat canggih, patch dan pembaruan perangkat lunak otomatis.
DSS04		
1.	*Continuity management*	Dilakukan, perlu frekuensi pelatihan BCP, DRP, *cloud*, dan *DevOps* lebih tinggi.
BAI08		
1.	*Information and Knowledge management*	Dikelola dengan strategi terstruktur, pelatihan rutin, repositori pengetahuan, dan integrasi teknologi.

5. Komponen Prinsip, Kebijakan, dan Prosedur

Tabel 6 menunjukkan bahwa setiap praktik manajemen dalam DSS05, DSS04, dan BAI08 ditemukan adanya kesenjangan pada komponen prinsip, kebijakan, dan prosedur.

Tabel 6 Analisis Komponen Prinsip, Kebijakan, dan Prosedur

No	Kebijakan Yang Relevan	Kondisi Eksisting
DSS05		
1.	*Information security policy*	Kebijakan sesuai standar dan peraturan, perlu evaluasi dan pembaruan berkala.
DSS04		
1.	*Business continuity policy*	Tim di Direktorat Perencanaan dan Transformasi mengelola kontinuitas bisnis, namun kontinuitas *cloud* belum terintegrasi sepenuhnya.
2.	*Crisis management policy*	Kebijakan krisis telah didefinisikan dan dipantau.
BAI08		
1.	*Governance Knowledge use policy*	Memiliki d*ata governance* etis, akses aman, dan sistem manajemen pengetahuan untuk pembelajaran dan kolaborasi karyawan.

6. Komponen Budaya, Etika, dan Perilaku

Tabel 7 menunjukkan dalam DSS05, DSS04, dan BAI08 ditemukan adanya kesenjangan pada komponen budaya, etika, dan perilaku.

Tabel 7 Analisis Komponen Budaya, Etika, dan Perilaku

No	Elemen Kunci Budaya	Kondisi Eksisting
DSS05		
1.	Ciptakan budaya kesadaran keamanan dan privasi.	Dibangun melalui pelatihan dan kampanye aktif.
DSS04		
1.	Tanamkan ketahanan bisnis, uji prosedur rutin.	Membangun ketahanan bisnis melalui budaya, komunikasi, pelatihan, dan pengujian rutin.
BAI08		
1.	Tanamkan budaya berbagi pengetahuan, komunikasikan nilainya, dan dorong pembuatan serta transfer pengetahuan.	Meluncurkan inisiatif berbagi pengetahuan, mendorong kolaborasi, pelatihan berkelanjutan, dan menyediakan repositori dokumen internal.

7. Komponen Layanan, Infrastruktur, dan Aplikasi

Tabel 8 menunjukkan dalam DSS05, DSS04, dan BAI08 ditemukan adanya kesenjangan pada komponen layanan, infrastruktur, dan aplikasi.

Tabel 8 Analisis Komponen Layanan, Infrastruktur, dan Aplikasi

No	Layanan, Infrastruktur, dan Aplikasi	Kondisi Eksisting
DSS05		
1.	*Directory services*	Mengimplementasikan layanan direktori terintegrasi untuk manajemen identitas dan autentikasi pengguna.
2.	*Email filtering systems*	Menerapkan sistem penyaringan email dan simulasi phishing rutin untuk meningkatkan kesadaran keamanan.
3.	*Identity and access management system*	Sistem IAM diterapkan efektif dengan RBAC dan MFA untuk kontrol akses ketat.
4.	*Security awareness services*	Mengadakan pelatihan dan kampanye kesadaran keamanan siber untuk seluruh karyawan.
5.	*Security information and event management (SIEM) tools*	Memanfaatkan teknologi SIEM untuk pemantauan kejadian keamanan real-time dan respon cepat. Namun, otomatisasi insiden belum dikembangkan.

DSS05		
No	**Layanan, Infrastruktur, dan Aplikasi**	**Kondisi Eksisting**
6.	*Security operations center (SOC) services*	Memiliki SOC yang beroperasi 24/7.
7.	*Third-party security assessment services*	Bekerja sama dengan mitra keamanan untuk penilaian keamanan, penetration testing, dan vulnerability scanning.
8.	*URL filtering systems*	Menerapkan sistem penyaringan URL untuk membatasi akses ke situs berisiko dan melindungi jaringan.
DSS04		
1.	*External hosting services*	Memanfaatkan penyedia cloud global untuk meningkatkan skalabilitas, ketersediaan, dan keamanan layanan digital.
2.	*Incident monitoring tools*	Tim security digital memantau 24/7, namun respons insiden *DevOps* otomatis perlu pengembangan lebih lanjut.
3.	*Remote storage facility services*	Menawarkan penyimpanan data jarak jauh dengan enkripsi *end-to-end*, replikasi redundan, dan pemulihan bencana berbasis *cloud*.
BAI08		
1.	*Collaboration platform*	Memanfaatkan Microsoft Office 365 dan Jira untuk kolaborasi, komunikasi, dan operasional internal.
2.	*Knowledge repository*	Menyediakan repositori dokumen yang dapat diakses seluruh pegawai untuk berbagi informasi.

C. Analisis Potential Improvement

Tabel 9 menyajikan rekomendasi strategis TelCo untuk penguatan organisasi (*people*), kebijakan (*process*), dan teknologi (*technology*).

Tabel 9 Analisis Potential Improvement

Komponen Kemampuan	*Type*	*Potential Improvement*
Struktur Organisasi	*Responsibility*	Mengintegrasikan aspek kontinuitas *cloud* dalam deskripsi tugas BCM, sehingga mencakup pengelolaan risiko dan pemulihan bencana untuk layanan berbasis *cloud*.
Individu, Keterampilan, dan Kompetensi	*Skill & Awareness*	Meningkatkan frekuensi pelatihan terkait BCP, DRP, kontinuitas *cloud*, dan *DevOps* untuk kesiapan tim.
	Skill & Awareness	Kurangnya evaluasi rutin terhadap efektivitas implementasi manajemen keamanan yang telah diterapkan.
	Procedure	Menyusun prosedur otomatisasi manajemen hak akses untuk mempercepat pemberian dan pencabutan akses.
	Work Instruction	Menyusun instruksi kerja untuk pengujian ketahanan *DevOps* dan *Chaos Engineering*, terintegrasi dalam prosedur pengujian rutin.
	Policy	Menyusun kebijakan untuk melibatkan lebih banyak bagian dalam berbagi pengetahuan dan mendokumentasikan pengguna pengetahuan.
	Work Instruction	Meningkatkan otomatisasi dengan panduan kerja jelas untuk integrasi dalam proses bisnis kompleks dan penyesuaian alat.
Prinsip, Kebijakan, dan Prosedur	*Policy*	Membuat kebijakan untuk memastikan perencanaan kontinuitas *cloud* dimulai sejak tahap perencanaan awal penerapan *cloud*.
Informasi	*Policy*	Menerapkan *Infrastructure as Code* (IaC) secara menyeluruh di seluruh layanan untuk memastikan konsistensi, efisiensi, dan kemampuan untuk melacak perubahan dengan lebih baik.
Layanan, Infrastruktur dan Aplikasi	*Features*	Meningkatkan alat otomasi respons insiden *DevOps* untuk meningkatkan kecepatan dan efisiensi penanganan insiden.

D. Analisis *Resource, Risk, Value*

Error! Reference source not found. menunjukkan prioritas perbaikan berdasarkan nilai akhir yang diperoleh dari hasil analisis RRV untuk setiap potensi perbaikan terhadap 3 aspek.

Tabel 10 Analisis *Resource, Risk, Value*

Potential Improvement	*Type*	*Score*	Kategori
Meningkatkan alat otomasi respons insiden *DevOps* untuk meningkatkan kecepatan dan efisiensi penanganan insiden.	*Features*	18	*Medium*
Mengintegrasikan aspek kontinuitas *cloud* dalam deskripsi tugas BCM, sehingga mencakup pengelolaan risiko dan pemulihan bencana untuk layanan berbasis *cloud*.	*Responsibility*	18	*Medium*
Kurangnya evaluasi rutin terhadap efektivitas implementasi manajemen keamanan yang telah diterapkan.	*Skill & Awareness*	18	*Medium*
Menyusun prosedur otomatisasi manajemen hak akses untuk mempercepat pemberian dan pencabutan akses.	*Procedure*	18	*Medium*
Menyusun kebijakan untuk melibatkan lebih banyak bagian dalam berbagi pengetahuan dan mendokumentasikan pengguna pengetahuan.	*Policy*	18	*Medium*
Membuat kebijakan untuk memastikan perencanaan kontinuitas *cloud* dimulai sejak tahap perencanaan awal penerapan *cloud*.	*Policy*	18	*Medium*
Menerapkan *Infrastructure as*	*Policy*	18	*Medium*

Potential Improvement	*Type*	*Score*	Kategori
Code (IaC) secara menyeluruh di seluruh layanan untuk memastikan konsistensi, efisiensi, dan kemampuan untuk melacak perubahan dengan lebih baik.			
Meningkatkan frekuensi pelatihan terkait BCP, DRP, kontinuitas *cloud*, dan *DevOps* untuk kesiapan tim.	*Skill & Awareness*	12	*Medium*
Menyusun instruksi kerja untuk pengujian ketahanan *DevOps* dan *Chaos Engineering*, terintegrasi dalam prosedur pengujian rutin.	*Work Instruction*	12	*Medium*
Meningkatkan otomatisasi dengan panduan kerja jelas untuk integrasi dalam proses bisnis kompleks dan penyesuaian alat.	*Work Instruction*	12	*Medium*

E. Rekomendasi *Roadmap* Implementasi

Tabel 11 menunjukkan *roadmap* strategis TelCo untuk mengimplementasikan rekomendasi berdasarkan analisis *resource*, *risk*, dan *value*.

Tabel 11 *Roadmap* Implementasi

Rekomendasi	*Roadmap Timeline*							
	2026				2027			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Aspek *People*								
Kurangnya evaluasi rutin terhadap efektivitas implementasi manajemen keamanan yang telah diterapkan.								
Mengintegrasikan aspek kontinuitas *cloud* dalam deskripsi tugas BCM, sehingga mencakup pengelolaan risiko dan pemulihan bencana untuk layanan berbasis *cloud*.								
Meningkatkan frekuensi pelatihan terkait BCP, DRP, kontinuitas *cloud*, dan *DevOps* untuk kesiapan tim.								
Aspek *Process*								
Menyusun prosedur otomatisasi manajemen hak akses untuk mempercepat pemberian dan pencabutan akses.								
Menyusun kebijakan untuk melibatkan lebih banyak bagian dalam berbagi pengetahuan dan mendokumentasikan pengguna pengetahuan.								
Membuat kebijakan untuk memastikan perencanaan kontinuitas *cloud* dimulai sejak tahap perencanaan awal penerapan *cloud*.								
Meningkatkan otomatisasi dengan panduan kerja jelas untuk integrasi dalam proses bisnis kompleks dan penyesuaian alat.								
Menyusun instruksi kerja untuk pengujian ketahanan *DevOps* dan *Chaos Engineering*, terintegrasi dalam prosedur pengujian rutin.								
Menerapkan *Infrastructure as Code* (IaC) secara menyeluruh di seluruh layanan untuk memastikan konsistensi, efisiensi, dan kemampuan untuk melacak perubahan dengan lebih baik.								
Aspek *Technology*								
Meningkatkan alat otomasi respons insiden *DevOps* untuk meningkatkan kecepatan dan efisiensi penanganan insiden.								

F. Pengaruh Rancangan

1. Komponen Proses

Tabel *12* menunjukkan peningkatan tingkat kemampuan manajemen TelCo dari skor 64 (3.4) menjadi 74 (3.9) setelah perbaikan.

Tabel 12 Perbandingan Komponen Proses

Praktik Manajemen	Tingkat Kemampuan Sebelum Perbaikan	Tingkat Kemampuan Sesudah Perbaikan
DSS05	25	27
DSS04	30	31
BAI08	12	16
Jumlah Total	**67**	**74**
Skor Total	**3.52**	**3.89**

2. Komponen Struktur Organisasi

Tabel 13 membandingkan struktur organisasi *cloud governance* TelCo berdasarkan COBIT.

Tabel 13 Perbandingan Komponen Struktur Organisasi

Struktur Organisasi COBIT	Tujuan TKTI	Sebelum Perbaikan	Sesudah Perbaikan
Executive Committee	DSS04	Dewan Komisaris	Dewan Komisaris
Chief Operating Officer (COO)	DSS04	Direktur *Network*	Direktur *Network*
Chief Information Officer (CIO)	BAI08, DSS05, DSS04	Direktur *IT*	Direktur *IT*
Chief Technology Officer (CTO)	BAI08, DSS04	Direktur *IT*	Direktur *IT*
Chief Information Security Officer (CISO)	DSS05, DSS04	Direktur *IT*	Direktur *IT*
Chief Digital Officer (CDO)	BAI08	Direktur Perencanaan & Transformasi	Direktur Perencanaan & Transformasi
Business Process Owners	BAI08, DSS05, DSS04	Direktur dan Kepala Divisi Bisnis	Direktur dan Kepala Divisi Bisnis
Portfolio Manager	BAI08	*Portfolio Management*	*Portfolio Management*
Program Manager	BAI08	*IT Program Manager*	*IT Program Manager*
Project Manager	BAI08	*Project Manager*	*Project Manager*
Data Management Function	BAI08, DSS04	*Big Data Management Platform Division*	*Big Data Management Platform Division*
Head Architect	BAI08, DSS04	*Head of IT Enterprise Architecture*	*Head of IT Enterprise Architecture*
Head Development	BAI08, DSS05, DSS04	*Head of Application Development*	*Head of Application Development*
Head IT Operations	BAI08, DSS05, DSS04	*Vice President of IT Operations & Infrastructure Group*	*Vice President of IT Operations & Infrastructure Group*
Head IT Administration	BAI08	*IT Operation and Infrastructure Group*	*IT Operation and Infrastructure Group*
Service Manager	BAI08, DSS04	Manajer Layanan TI	Manajer Layanan TI
Information Security Manager	BAI08, DSS05, DSS04	Manajer Manajemen Risiko Keamanan TI	Manajer Manajemen Risiko Keamanan TI
Business Continuity Manager	BAI08, DSS04	Direktorat Keuangan dan Risiko	Direktorat Keuangan dan Risiko. Dengan penambahan tanggung jawab *cloud continuity*
Privacy Officer	BAI08, DSS05,	Direktorat *Finance & Risk Management*	Direktorat *Finance & Risk Management*
Legal Counsel	BAI08,	*Vice President Corporate Counsel*	*Vice President Corporate Counsel*
Head Human Resources	DSS05	Direktorat *Human Capital Management*	Direktorat *Human Capital Management*
Product Owner/Manager	DSS05, DSS04	*Digital Product Solution* atau *Product, Fulfillment and Integration Platforms*	*Digital Product Solution* atau *Product, Fulfillment and Integration Platforms*
Software Development Manager	BAI08, DSS05, DSS04	*Corporate Solutions & Cloud CoE* atau *Customer Touchpoint and Digital Product Solution*	*Corporate Solutions & Cloud CoE* atau *Customer Touchpoint and Digital Product Solution*
Systems Operations Manager	BAI08, DSS05, DSS04	*Head of IT Operation and Infrastructure Group*	*Head of IT Operation and Infrastructure Group*
Testing Manager	DSS05, DSS04	*Head of Quality Assurance & Testing Division*	*Head of Quality Assurance & Testing Division*
Release Manager	DSS05, DSS04	*Corporate Solutions & Cloud CoE*	*Corporate Solutions & Cloud CoE*
Automation Manager	DSS05, DSS04	*IT Operation and Infrastructure Group*	*IT Operation and Infrastructure Group*
Systems Architect Manager	BAI08, DSS05, DSS04	*IT Enterprise Architecture and Strategy Group*	*IT Enterprise Architecture and Strategy Group*

3. Komponen Informasi

Tabel 14 membandingkan komponen informasi *cloud governance* TelCo berdasarkan COBIT.

Tabel 14 Perbandingan Komponen Informasi

No	*Information Output*	Sebelum Perbaikan	Sesudah Perbaikan
	DSS04		
1.	Continuity requirements	Memenuhi kontinuitas dengan backup, redundansi, dan pengujian, namun adopsi IaC terbatas.	Mengadopsi IaC untuk *provisioning* dan pemulihan *cloud* secara efisien.

4. Komponen Individu, Keterampilan, dan Kompetensi

Tabel 15 membandingkan komponen individu, keterampilan, dan kompentensi *cloud governance* TelCo berdasarkan COBIT.

Tabel 15 Perbandingan Komponen Prinsip, Kebijakan, dan Prosedur

No	Keterampilan	Sebelum Perbaikan	Sesudah Perbaikan
	DSS04		
1.	*Continuity management*	Perlu frekuensi lebih tinggi untuk BCP, DRP, dan *DevOps*.	Meningkatkan frekuensi pelatihan BCP, DRP, *cloud*, dan *DevOps*.
	DSS05		
1.	*Information security management*	Kurangnya evaluasi rutin terhadap efektivitas implementasi manajemen	Evaluasi rutin terhadap efektivitas implementasi manajemen keamanan yang telah diterapkan secara rutin.

No	Keterampilan	Sebelum Perbaikan	Sesudah Perbaikan
		keamanan yang telah diterapkan.	

5. Komponen Prinsip, Kebijakan, dan Prosedur

Tabel 15 membandingkan komponen prinsip, kebijakan, dan prosedur *cloud governance* TelCo berdasarkan COBIT.

Tabel 16 Perbandingan Komponen Prinsip, Kebijakan, dan Prosedur

No	Kebijakan	Sebelum Perbaikan	Sesudah Perbaikan
DSS04			
1.	*Business continuity policy*	Belum terintegrasi sejak awal penerapan *cloud*.	Mengintegrasikan perencanaan kontinuitas *cloud* sejak awal penerapan.

6. Komponen Budaya, Etika, dan Perilaku

Tabel 17 membandingkan komponen budaya, etika, dan perilaku *cloud governance* TelCo berdasarkan COBIT.

Tabel 17 Perbandingan Komponen Budaya, Etika, dan Perilaku

No	Elemen Kunci Budaya	Sebelum Perbaikan	Sesudah Perbaikan
DSS05			
1.	Ciptakan budaya kesadaran keamanan dan privasi.	Dibangun melalui pelatihan dan kampanye aktif.	Dibangun melalui pelatihan dan kampanye aktif.
DSS04			
1.	Tanamkan ketahanan bisnis, uji prosedur rutin.	Membangun ketahanan bisnis melalui budaya, komunikasi, pelatihan, dan pengujian rutin.	Membangun ketahanan bisnis melalui budaya, komunikasi, pelatihan, dan pengujian rutin.
BAI08			
1.	Tanamkan budaya berbagi pengetahuan, komunikasikan nilainya, dan dorong pembuatan serta transfer pengetahuan.	Meluncurkan inisiatif berbagi pengetahuan, mendorong kolaborasi, pelatihan berkelanjutan, dan menyediakan repositori dokumen internal.	Meluncurkan inisiatif berbagi pengetahuan, mendorong kolaborasi, pelatihan berkelanjutan, dan menyediakan repositori dokumen internal.

7. Komponen Layanan, Infrastuktur, dan Aplikasi

Tabel 17 membandingkan komponen layanan, infrastuktur, dan aplikasi *cloud governance* TelCo berdasarkan COBIT.

Tabel 18 Perbandingan Komponen Layanan, Infrastuktur, dan Aplikasi

No	Kebijakan	Sebelum Perbaikan	Sesudah Perbaikan
DSS04			
1.	*Incident monitoring tools*	Belum terdapat fitur otomatisasi insiden berbasis *DevOps*.	Terdapat fitur otomatisasi insiden berbasis *DevOps*.

V. KESIMPULAN

Penelitian ini menyarankan TelCo untuk meningkatkan pelatihan rutin terkait BCP, DRP, kontinuitas *cloud*, dan *DevOps*, serta evaluasi berkala manajemen keamanan. TelCo juga perlu menambahkan tanggung jawab kontinuitas cloud kepada BCM dan menyusun kebijakan strategis serta menerapkan *Infrastructure as Code* (IaC) untuk efisiensi layanan. Implementasi otomatisasi manajemen hak akses, pengujian ketahanan berbasis *DevOps*, dan integrasi otomatis dalam proses bisnis sangat penting. Pengembangan alat otomatisasi respons insiden *DevOps* juga direkomendasikan untuk mempercepat respons terhadap insiden, meningkatkan kapabilitas organisasi dalam menghadapi tantangan digital dan operasional.

REFERENSI

[1] M. A. Berawi *et al.*, "Digital Innovation: Creating Competitive Advantages," *International Journal of Technology*, vol. 11, no. 6, pp. 1076–1080, 2020, doi: 10.14716/ijtech.v11i6.4581.

[2] C. P. Amajuoyi, L. K. Nwobodo, and M. D. Adegbola, "Transforming Business Scalability and Operational Flexibility with Advanced Cloud Computing Technologies," *Computer Science & IT Research Journal*, vol. 5, no. 6, pp. 1469–1487, Jun. 2024, doi: 10.51594/csitrj.v5i6.1248.

[3] O. Shareef, "Building Organizational Defense: A Comprehensive Approach to Implementing IT Controls for Sox Compliance," *International Journal of Computer Science and Mobile Computing*, vol. 13, no. 2, pp. 69–71, Feb. 2024, doi: https://doi.org/10.47760/ijcsmc.2024.v13i02.006.

[4] B. Thuraisingham, "Cloud Governance," in *IEEE International Conference on Cloud Computing, CLOUD*, IEEE Computer Society, Oct. 2020, pp. 86–90. doi: 10.1109/CLOUD49709.2020.00025.

[5] L. Y. Chang, S. F. Wong, U. Eze, and H. Lee, "The Effect of IT Ambidexterity and Cloud Computing Absorptive Capacity on Competitive Advantage," *Industrial Management & Data Systems*, vol. 119, Nov. 2018, doi: 10.1108/IMDS-05-2018-0196.

[6] M. Lubis, A. R. Lubis, H. Nuraliza, M. I. Alhari, S. F. Azzahra, and J. R. Maulana, "Designing IT Governance using COBIT 2019: An Examination of a Telecommunications Company's Case Study," in *2023 7th International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM)*, 2023, pp. 269–274. doi: 10.1109/ELTICOM61905.2023.10443159.

[7] R. Mulyana, L. Rusu, and E. Perjons, "Key Ambidextrous IT Governance Mechanisms Influence on Digital Transformation and Organizational Performance in Indonesian Banking and Insurance Industry," *Pacific Asia Conference on Information Systems (PACIS)*, 2024, Accessed: Jun. 07, 2025. [Online]. Available: https://aisel.aisnet.org/pacis2024/track15_govce/track15_govce/7

[8] L. Pintor, L. Atzori, and A. Iera, "Sustainability in Telecommunication Networks and Key Value

Indicators: a Survey," *ArXiv*, vol. abs/2501.04356, 2025, [Online]. Available: https://api.semanticscholar.org/CorpusID:275358132

[9] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital Transformation: An Overview of the Current State of the Art of Research," *Sage Open*, vol. 11, no. 3, 2021, doi: 10.1177/21582440211047576.

[10] H. Uddin, S. Mollah, N. Islam, and H. Ali, "Does Digital Transformation Matter for Operational Risk Exposure?," *Technol Forecast Soc Change*, vol. 197, pp. 40–1625, 2023, doi: 10.1016/j.techfore.2023.122919.

[11] S. Khalil and V. Fautrero, "Cloud Impact on IT Governance," *SSRN Electronic Journal*, Jan. 2016, doi: 10.2139/ssrn.2847087.

[12] F. Febrianti and D. N. Utama, "Enhancing IT Maturity in the DevOps Focus Area: A Comprehensive Assessment with COBIT 2019," *Edelweiss Applied Science and Technology*, vol. 8, no. 4, pp. 926–934, 2024, doi: 10.55214/25768484.v8i4.1472.

[13] M. Lestari, A. Iriani, and H. Hendry, "Information Technology Governance Design in DevOps-Based E-Marketplace Companies Using COBIT 2019 Framework," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 233–252, Aug. 2022, doi: 10.29407/intensif.v6i2.18104.

[14] A. F. Satriardi, R. Mulyana, and R. Fauzi, "Agile IT Service Management Design of FinTechCo Digitalization Based on COBIT 2019 DevOps Focus Area," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1165–1177, Oct. 2023, doi: 10.52436/1.jutif.2023.4.5.1304.

[15] ISACA, *COBIT Focus Area: DevOps*. 2021. [Online]. Available: www.isaca.org

[16] L. Setiadi and M. Fianty, "Enhancing Organizational Performance through COBIT 2019-Based IT Governance Audit: A Case Study of a Digital Technology Company," *Journal of Information Systems and Informatics*, vol. 6, pp. 676–688, Jun. 2024, doi: 10.51519/journalisi.v6i2.715.

[17] S. Naik, "Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy," 2023. doi: http://dx.doi.org/10.58812/esiscs.v1i01.452.

[18] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," Sep. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/network3030018.

[19] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, Mar. 2004, doi: 10.2307/25148625.

[20] K. R. Yin, "How to do Better Case Studies," *SAGE Publications, Inc.*, pp. 254–282, 2009, doi: 10.4135/9781483348858.n8.

[21] P. I. Fusch and L. R. Ness, "Are We There Yet? Data Saturation in Qualitative Research," *Qualitative Report*, vol. 20, no. 9, pp. 1408–1416, Sep. 2015, doi: 10.46743/2160-3715/2015.2281.

[22] O. Kalinin, V. Gonchar, N. Abliazova, L. Filipishyna, O. Onofriichuk, and M. Maltsev, "Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability," *Nat Eng Sci*, vol. 9, no. 1, pp. 26–45, 2024, doi: 10.28978/nesciences.1469858.