JTK3TI Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi

Volume 12 Nomor 2, 2026, pp 171-181
ISSN: 2460-1799 P-ISSN: 1432-602743

Evaluasi Layanan Keamanan Terkelola PT OGN Menggunakan COBIT 2019

Alya Devia Rachmah[1*], Salsabila Lathifa[2], Nasya Nurli Sukmono Putri[3], Najwa Ulya Najjini[4], Puji Rahayu[5]

Program Studi Sistem Informasi, Universitas Telkom Jakarta, Jalan Minangkabau Barat No 50 RT 1 / RW 1, Pasar Manggis, Kecamatan Setiabudi, Kota Jakarta Selatan, DKI Jakarta 12970, alyadevia@student.telkomuniversity.ac.id, salsalathifa@student.telkomuniversity.ac.id, nasyanurli@student.telkomuniversity.ac.id, najwaulyanajjini@student.telkomuniversity.ac.id, pujirahayupr@telkomuniversity.ac.id

* Korespondensi: e-mail: alyadevia29@gmail.com, pujisekar@gmail.com

Diterima: 20/07/2026 ; Review: 20/07/2026 Disetujui: 30/07/2026

ABSTRAK *– Meningkatnya kompleksitas ancaman siber menuntut organisasi, khususnya penyedia layanan teknologi informasi, untuk menerapkan tata kelola keamanan yang mampu menjamin keberlangsungan layanan sekaligus memenuhi kepatuhan regulasi. Sebagai perusahaan yang bergerak di bidang konsultasi teknologi informasi, keamanan siber, dan perlindungan data, PT OGN perlu melakukan evaluasi sistematis terhadap efektivitas pengelolaan layanan keamanannya. Penelitian ini bertujuan untuk mengevaluasi layanan keamanan terkelola pada PT OGN menggunakan kerangka kerja COBIT 2019 melalui analisis faktor desain (design factors), pengukuran tingkat kapabilitas, analisis kesenjangan, serta penyusunan rekomendasi peningkatan. Hasil analisis faktor desain menunjukkan bahwa domain DSS05 (Managed Security Services) merupakan domain yang paling relevan berdasarkan karakteristik organisasi, kebutuhan kepatuhan, dan profil risiko perusahaan. Pengukuran tingkat kapabilitas menunjukkan bahwa praktik manajemen (management practice) DSS05.02 (Manage Network and Connectivity Security) dan DSS05.03 (Manage Endpoint Security) masih berada pada kapabilitas tingkat 1 (Level 1), sehingga belum memenuhi target tingkat 2 (Level 2) yang ditetapkan organisasi. Berdasarkan temuan tersebut, rekomendasi peningkatan disusun mencakup aspek manusia (people), proses (process), dan teknologi (technology), serta diorganisasikan ke dalam peta jalan (roadmap) implementasi selama 12 bulan. Penelitian ini memberikan kontribusi berupa rekomendasi tata kelola yang selaras dengan kebutuhan bisnis, profil risiko, dan kepatuhan organisasi guna mendukung peningkatan pengelolaan layanan keamanan terkelola di PT OGN.*

Kata Kunci *– COBIT 2019; capability assessment; design factors; managed security services; tata kelola keamanan informasi.*

Evaluation of Managed Security Services Governance at PT OGN Using COBIT 2019

ABSTRACT *– The increasing complexity of cyber threats requires organizations, particularly information technology service providers, to implement effective security governance that ensures service continuity while complying with applicable regulatory requirements. As a company specializing in IT consulting, cybersecurity, and data protection, PT OGN requires a systematic evaluation of its managed security services to strengthen its governance practices. This study aims to evaluate the managed security services at PT OGN using the COBIT 2019 framework through design factors analysis, capability assessment, gap analysis, and the development of improvement recommendations. The design factors analysis identified DSS05 (Managed Security Services) as the most relevant domain based on the organization's characteristics, compliance requirements, and cybersecurity risk profile. The capability assessment revealed that DSS05.02 (Manage Network and Connectivity Security) and DSS05.03 (Manage Endpoint Security) remain at Capability Level 1, indicating that both practices have not yet achieved the organization's target of Capability Level 2. Based on these findings, improvement recommendations were formulated across the people, process, and technology dimensions and organized into a 12-month implementation roadmap. This study contributes governance recommendations aligned with business needs, organizational risk profiles, and compliance requirements, thereby supporting the improvement of managed security services governance at PT OGN.*

Keywords *– COBIT 2019; capability assessment; design factors; managed security services; information security governance.*

This is an open access article under the CC BY-SA license

Volume 12 Nomor 2, 2026, pp 171-181
ISSN: 2460-1799 P-ISSN: 1432-602743

1. PENDAHULUAN

Implementasi teknologi informasi (TI) dalam bisnis modern berkembang pesat dan menjadi faktor utama keberhasilan organisasi dalam mempertahankan daya saing. TI tidak lagi sekadar berperan sebagai alat pendukung operasional, tetapi telah menjadi komponen strategis yang mendukung pengambilan keputusan, inovasi, serta penciptaan nilai bisnis. Seiring meningkatnya ketergantungan organisasi terhadap teknologi, risiko keamanan informasi juga semakin kompleks. Ancaman seperti *malware*, *ransomware*, *phishing*, dan *insider threat* terus mengalami peningkatan dan berpotensi menyebabkan kebocoran data, kerugian finansial, hingga pelanggaran regulasi. Oleh karena itu, keamanan informasi menjadi bagian yang tidak terpisahkan dari tata kelola TI guna menjaga keberlangsungan operasional organisasi [1], [2], [3], [4].

Bagi perusahaan yang bergerak di bidang konsultasi teknologi informasi, kualitas tata kelola TI memiliki pengaruh langsung terhadap keberhasilan implementasi solusi bagi klien. Pengelolaan keamanan informasi yang belum optimal tidak hanya meningkatkan risiko operasional perusahaan, tetapi juga dapat menurunkan tingkat kepercayaan pelanggan terhadap layanan yang diberikan. Penelitian Simatupang dan Fianty [5] serta Fianty dan Hardjadinata [6] menunjukkan bahwa penerapan tata kelola TI yang sesuai dengan karakteristik perusahaan jasa TI mampu meningkatkan efektivitas proses pengelolaan layanan sekaligus mendukung pencapaian tujuan bisnis.

PT OGN merupakan perusahaan yang bergerak di bidang konsultasi teknologi informasi, integrasi sistem, keamanan siber, serta perlindungan data dengan cakupan layanan pada sektor perbankan, telekomunikasi, dan Badan Usaha Milik Negara (BUMN). Aktivitas bisnis perusahaan sangat bergantung pada pemanfaatan teknologi informasi karena hampir seluruh produk dan layanan yang ditawarkan berbasis TI. Berdasarkan hasil wawancara, perusahaan telah menerapkan berbagai mekanisme pengamanan seperti *Virtual Private Network* (VPN), *firewall*, *endpoint security*, *Security Information and Event Management* (SIEM), *OpenText Data Protection*, serta *Identity Access Management* (IAM). Selain itu, perusahaan juga memanfaatkan infrastruktur *on-premise*, *hybrid*, dan *cloud* sesuai dengan kebutuhan operasional maupun regulasi perlindungan data yang berlaku.

Meskipun demikian, hasil observasi dan wawancara menunjukkan bahwa kebijakan keamanan informasi di PT OGN masih bersifat umum dan belum sepenuhnya mengadopsi kerangka tata kelola formal. Sebagian praktik keamanan masih disesuaikan dengan kebutuhan proyek maupun standar klien sehingga konsistensi pengendalian keamanan internal belum sepenuhnya tercapai. Kondisi tersebut paling terlihat pada layanan *Managed Security Services*, khususnya pada aspek keamanan *endpoint*, pengamanan akses melalui *email* dan *web browser*, penggunaan perangkat pribadi dalam lingkungan pengembangan, serta belum terdokumentasinya mekanisme penyaringan *email* berbahaya, pemblokiran situs berisiko, maupun pengelolaan tautan *phishing* dan *malware*. Kondisi ini meningkatkan risiko akses tidak sah, infeksi perangkat, serta kebocoran informasi yang dapat mengganggu keberlangsungan operasional perusahaan.

Apabila dikaitkan dengan hasil analisis *Design Factors* COBIT 2019, karakteristik PT OGN menunjukkan tingkat kebutuhan kepatuhan (*Compliance Requirements*) yang tinggi serta profil risiko yang didominasi oleh ancaman keamanan siber, pengelolaan data, dan akses tidak sah terhadap sistem informasi. Kondisi tersebut menunjukkan perlunya suatu kerangka kerja yang mampu mengevaluasi tingkat kapabilitas proses secara sistematis sekaligus menghasilkan rekomendasi peningkatan yang sesuai dengan karakteristik organisasi. COBIT 2019 menyediakan pendekatan tersebut melalui *Design Factors*, pengukuran tingkat kapabilitas proses (*Capability Assessment*), dan *Gap Analysis* sehingga organisasi dapat merancang sistem tata kelola yang selaras dengan strategi bisnis, profil risiko, kebutuhan kepatuhan, serta prioritas peningkatan proses [7], [8], [9]

Secara konseptual, tata kelola TI merupakan bagian dari tata kelola organisasi yang berfokus pada aktivitas evaluasi, pengarahan, dan pemantauan penggunaan TI agar selaras dengan kebutuhan organisasi dan pemangku kepentingan, sedangkan manajemen TI berfokus pada perencanaan, implementasi, dan operasional TI sehari-hari [7], [9]. COBIT 2019 merupakan kerangka kerja tata kelola dan manajemen TI yang dikembangkan oleh ISACA untuk membantu organisasi dalam mengevaluasi serta meningkatkan kapabilitas tata kelola TI. Dalam penelitian ini, evaluasi difokuskan pada domain DSS05 (*Managed Security Services*) karena domain tersebut berperan dalam menjaga keamanan informasi melalui pengelolaan otorisasi akses, perlindungan terhadap *malware*, keamanan jaringan dan konektivitas, keamanan *endpoint*, serta pemantauan infrastruktur secara berkelanjutan guna mendeteksi dan menangani potensi insiden

keamanan [7], [8]

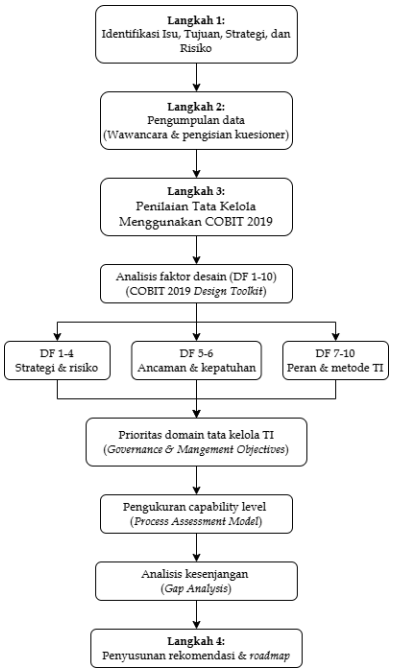
Berbagai penelitian terdahulu menunjukkan bahwa COBIT 2019 efektif digunakan untuk mengevaluasi tata kelola TI melalui pengukuran tingkat kapabilitas, identifikasi kesenjangan, dan penyusunan rekomendasi peningkatan pada berbagai jenis organisasi [10], [11], [12], [13]. Selain itu, pendekatan *Design Factors* terbukti mampu menghasilkan rancangan tata kelola yang lebih sesuai dengan karakteristik organisasi [14]. Pada perusahaan penyedia layanan TI, COBIT 2019 juga telah diterapkan untuk mengevaluasi kapabilitas proses dan mendukung penyusunan rekomendasi tata kelola yang selaras dengan kebutuhan bisnis [5], [6]. Penelitian Asro [15] turut menunjukkan bahwa kerangka kerja COBIT 2019 efektif digunakan untuk mengevaluasi tingkat kapabilitas keamanan sistem informasi sehingga dapat menjadi dasar dalam penyusunan rekomendasi peningkatan tata kelola TI.

Meskipun demikian, sebagian besar penelitian terdahulu masih berfokus pada pengukuran tingkat kapabilitas organisasi secara umum tanpa memberikan pembahasan yang lebih mendalam mengenai akar penyebab kesenjangan pada setiap *management practice*. Selain itu, penelitian yang secara khusus membahas implementasi domain DSS05 pada perusahaan konsultan keamanan siber masih relatif terbatas. Padahal, domain tersebut memiliki peran penting dalam memastikan efektivitas pengelolaan layanan keamanan, khususnya pada aspek keamanan *endpoint*, pengamanan akses pengguna, perlindungan *email*, serta pengendalian akses terhadap layanan berbasis *web* yang saat ini menjadi salah satu sasaran utama serangan siber.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk mengevaluasi tingkat kapabilitas tata kelola keamanan informasi pada domain DSS05 menggunakan kerangka kerja COBIT 2019, mengidentifikasi kesenjangan kapabilitas, serta menyusun rekomendasi peningkatan yang sesuai dengan karakteristik PT OGN . Berbeda dengan penelitian sebelumnya yang umumnya hanya berfokus pada pengukuran tingkat kapabilitas, penelitian ini mengintegrasikan hasil *Design Factors*, *Governance System Canvas*, *Capability Assessment*, dan *Gap Analysis* untuk menentukan prioritas peningkatan tata kelola TI secara lebih komprehensif. Kontribusi penelitian ini berupa rekomendasi peningkatan berbasis aspek *people*, *process*, dan *technology* yang diharapkan mampu memperkuat pengelolaan layanan keamanan informasi sekaligus mendukung kepatuhan organisasi terhadap berbagai regulasi yang berlaku.

2. METODOLOGI PENELITIAN

Metodologi penelitian disusun untuk merancang tata kelola teknologi informasi (TI) pada PT OGN dengan mengadopsi kerangka kerja COBIT 2019. Tahapan penelitian dimulai dari identifikasi isu, tujuan, strategi, dan risiko, dilanjutkan dengan pengumpulan data, analisis faktor desain, penentuan prioritas tata kelola TI, pengukuran tingkat kapabilitas, analisis kesenjangan, hingga penyusunan rekomendasi dan roadmap implementasi. Alur penelitian ditunjukkan pada gambar 1.



Gambar 1. Tahap Penelitian

Langkah 1: Identifikasi Isu, Tujuan, Strategi, dan Risiko

Tahap awal penelitian dilakukan dengan mengidentifikasi isu, tujuan, strategi, dan risiko yang berkaitan dengan tata kelola teknologi informasi di PT OGN . Identifikasi ini bertujuan untuk menentukan aspek-aspek yang akan digali dalam penelitian. Berdasarkan hasil identifikasi tersebut disusun indikator dan butir pertanyaan yang digunakan sebagai pedoman pelaksanaan wawancara dan pengisian kuesioner pada tahap pengumpulan data.

Langkah 2: Pengumpulan Data

Tahap pengumpulan data dilakukan melalui wawancara dan pengisian kuesioner oleh pihak yang bertanggung jawab pada Divisi Data Security PT OGN menggunakan instrumen yang telah disusun pada tahap sebelumnya. Data yang diperoleh digunakan sebagai dasar dalam pelaksanaan penilaian tata kelola menggunakan COBIT 2019,

khususnya pada analisis faktor desain yang dilakukan dengan COBIT 2019 *Design Toolkit*.

Langkah 3: Penilaian Tata Kelola Menggunakan COBIT 2019

1) Analisis Faktor Desain

Data hasil pengumpulan selanjutnya dianalisis menggunakan COBIT 2019 *Design Toolkit* untuk menghasilkan rancangan tata kelola yang sesuai dengan karakteristik dan kebutuhan organisasi. Analisis dilakukan terhadap 10 faktor desain (*Desaign Factors*), yaitu *Enterprise Strategy, Enterprise Goals, Risk Profile, I&T-Related Issues, Threat Landscape, Compliance Requirements, Role of IT, Sourcing Model for IT*, *IT Implementation Methods*, dan *Technology Adoption Strategy*.

2) Penentuan Domain Prioritas

Hasil analisis faktor desain selanjutnya diproses menggunakan COBIT 2019 *Design Toolkit* untuk menghasilkan nilai *importance* pada setiap *Governance and Management Objectives* (GMO). Beberapa domain dengan nilai importance tertinggi ditetapkan sebagai prioritas tata kelola karena dinilai paling sesuai dengan karakteristik organisasi dan kebutuhan bisnis. Selanjutnya, dilakukan pemilihan satu domain yang paling relevan dengan ruang lingkup penelitian sebagai fokus pengukuran tingkat kapabilitas. Pemilihan domain tersebut mempertimbangkan keterkaitan dengan studi kasus penelitian serta dukungan dari domain prioritas lainnya sebagai dasar penentuan fokus analisis.

3) Pengukuran Tingkat Kapabilitas

Domain yang telah ditetapkan sebagai fokus penelitian selanjutnya diukur tingkat kapabilitasnya menggunakan COBIT 2019 *Process Assessment Model* (PAM). Pengukuran dilakukan terhadap setiap management practice untuk mengetahui tingkat kapabilitas proses berdasarkan kondisi organisasi saat ini. Hasil pengukuran digunakan untuk mengidentifikasi pencapaian kapabilitas pada setiap *management practice* sesuai dengan kriteria penilaian COBIT 2019.

4) Analisis Kesenjangan

Hasil pengukuran tingkat kapabilitas dibandingkan dengan tingkat kapabilitas yang menjadi target organisasi untuk memperoleh nilai kesenjangan (*gap*). Analisis difokuskan pada *management practice* yang belum mencapai target kapabilitas sehingga dapat diidentifikasi area yang memerlukan perbaikan. Hasil analisis kesenjangan menjadi dasar dalam penyusunan rekomendasi peningkatan tata kelola teknologi informasi.

Langkah 4: Penyusunan Rekomendasi dan *Roadmap*

Tahap akhir penelitian adalah menyusun rekomendasi peningkatan berdasarkan hasil analisis kesenjangan pada domain yang menjadi fokus penelitian. Rekomendasi disusun berdasarkan tiga aspek utama, yaitu *People, Process,* dan *Technology*. Aspek *People* difokuskan pada peningkatan kompetensi sumber daya manusia dengan mengacu pada *Skills Framework for the Information Age* (SFIA) versi 8 [16]. Aspek *Process* meliputi penyusunan dan penyempurnaan kebijakan serta *Standard Operating Procedure* (SOP), sedangkan aspek *Technology* difokuskan pada optimalisasi kontrol teknis untuk meningkatkan keamanan infrastruktur dan layanan teknologi informasi.

Selanjutnya, rekomendasi tersebut diprioritaskan berdasarkan tingkat urgensi, ketergantungan antaraktivitas, serta kemudahan implementasinya. Hasil prioritisasi kemudian disusun ke dalam *roadmap* implementasi yang menggambarkan urutan pelaksanaan rekomendasi dalam beberapa fase implementasi sebagai acuan pelaksanaan peningkatan tata kelola TI secara bertahap sesuai dengan prioritas organisasi.

3. HASIL DAN PEMBAHASAN

A. Melakukan pemetaan COBIT *Core Model* 2019

Pada tahap ini analisis dilakukan berdasarkan hasil wawancara dan observasi pada PT OGN. Data kemudian dipetakan menggunakan COBIT 2019 Design Toolkit untuk menentukan prioritas tata kelola dan manajemen teknologi informasi sesuai kebutuhan organisasi. Pemetaan mempertimbangkan strategi perusahaan, tujuan bisnis, profil risiko, isu TI, tingkat ancaman, kebutuhan kepatuhan, peran TI, model sourcing, metode implementasi, dan strategi adopsi teknologi.

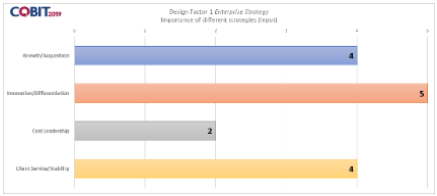
Step 1: Memahami Konteks dan Strategi Organisasi

PT OGN merupakan perusahaan konsultasi teknologi informasi yang berfokus pada *cyber security*, *data protection*, *system integration*, dan pengembangan aplikasi. Perusahaan melayani sektor perbankan, telekomunikasi, dan BUMN yang memiliki kebutuhan tinggi terhadap keamanan informasi. Oleh karena itu, teknologi informasi menjadi fondasi utama bisnis sehingga diperlukan tata kelola TI yang efektif untuk mendukung pencapaian tujuan organisasi sekaligus mengendalikan risiko bisnis [17].

Step 2: Menentukan Lingkup Awal Sistem Tata Kelola

1) Design Factor 1 (Enterprise Strategy)

PT OGN berfokus pada pengembangan layanan inovatif di bidang keamanan siber dan perlindungan data.

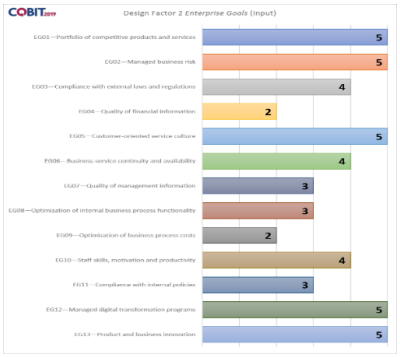


Gambar 2. Hasil *Design Factor 1 (Enterprise Strategy)*

Pada Gambar 2 hasil menunjukkan strategi *Innovation/Differentiation* memperoleh nilai tertinggi (5), diikuti *Growth/Acquisition* dan *Client Service/Stability* (4). Sementara itu, *Cost Leadership* memperoleh nilai terendah (2), sehingga inovasi menjadi strategi utama perusahaan.

2) Design Factor 2 (Enterprise Goals)

Tujuan organisasi berfokus pada inovasi, pengelolaan risiko, dan peningkatan kualitas layanan sebagai dasar penentuan prioritas tata kelola TI.



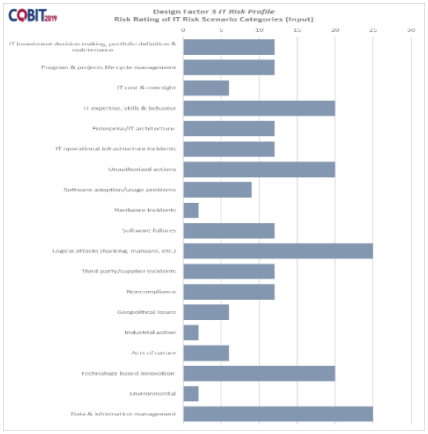
Gambar 3. Hasil *Design Factor 2 (Enterprise Goals)*

Pada Gambar 3 terlihat bahwa EG01 (*Portfolio of Competitive Products and Services*), EG02 (*Managed Business Risk*), EG05 (*Customer-Oriented Service Culture*), EG12 (*Managed Digital Transformation Programs*), dan EG13 (*Product and Business Innovation*) memperoleh nilai tertinggi sebesar 5. Meskipun beberapa *enterprise goals* memiliki tingkat kepentingan yang sama, penelitian ini memfokuskan analisis pada EG02 (*Managed Business Risk*) karena memiliki keterkaitan yang paling kuat dengan domain DSS05 (*Managed Security Services*).

Pemilihan EG02 didasarkan pada tujuan perusahaan untuk mengelola risiko bisnis yang dapat memengaruhi keberlangsungan operasional, khususnya risiko yang berasal dari teknologi informasi. Pengelolaan risiko tersebut mencakup perlindungan terhadap aset informasi, pencegahan ancaman keamanan siber, pengendalian akses, serta upaya menjaga kerahasiaan, integritas, dan ketersediaan informasi. Oleh karena itu, pencapaian EG02 sangat bergantung pada efektivitas layanan keamanan yang dikelola dalam domain DSS05.

3) Design Factor 3 (Risk Profile)

Pengelolaan risiko menjadi aspek yang sangat penting bagi PT OGN karena perusahaan bergerak pada bidang keamanan informasi dan perlindungan data. Risiko yang dihadapi tidak hanya berasal dari faktor teknologi, tetapi juga dari pengelolaan data dan sumber daya manusia.



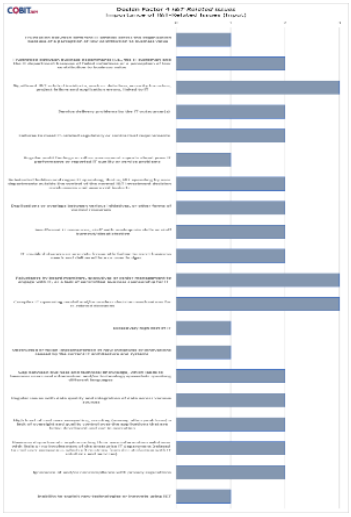
Gambar 4. Hasil *Design Factor 3 (Risk Profile)*

Berdasarkan hasil kategori *Logical Attacks* dan *Data & Information Management* memperoleh nilai tertinggi (25). *Risiko Unauthorized Actions*, *IT Expertise, Skills and Behavior*, serta *Technology-Based Innovation* memperoleh nilai 20. Hasil ini menunjukkan bahwa keamanan siber, perlindungan data, dan kompetensi SDM menjadi perhatian utama perusahaan.

4) Design Factor 4 (I&T Related Issues)

Hasil identifikasi *I&T Related Issues* menunjukkan bahwa organisasi masih menghadapi beberapa permasalahan yang berpotensi memengaruhi efektivitas tata kelola TI. Isu-isu tersebut berasal dari aspek keamanan informasi, pengelolaan TI, maupun keterlibatan manajemen dalam mendukung fungsi TI.

Rincian tingkat kepentingan setiap isu disajikan pada Gambar 5.



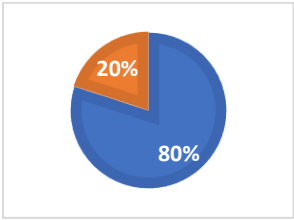
Gambar 5. Hasil *Design Factor 4 (I&T Related Issues)*

Terlihat bahwa *isu Significant I&T-Related Incidents, Reluctance by Management to Engage with IT*, dan *Complex IT Operating Model and/or Unclear Decision Mechanisms for IT-Related Decisions* memperoleh nilai tertinggi sebesar 3. Hasil ini menunjukkan bahwa perusahaan perlu memperkuat pengelolaan keamanan informasi, meningkatkan dukungan manajemen terhadap TI, serta memperjelas mekanisme pengambilan keputusan yang berkaitan dengan teknologi informasi.

Step 3: Penyelarasan Ruang Lingkup Tata Kelola Berdasarkan *Design Factors*

1) *Design Factor 5 (Threat Landscape)*

Analisis pada *design factor* ini difokuskan untuk mengidentifikasi tingkat ancaman yang berpotensi memengaruhi operasional maupun layanan teknologi informasi di PT OGN . Hasil pemetaan disajikan pada Diagram lingkaran berikut:

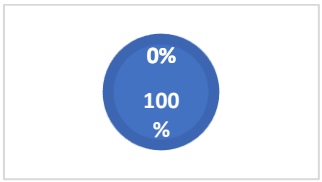


Gambar 6. Hasil *Design Factor 5 (Threat Landscape)*

Kategori *High* memperoleh 80% dan Normal 20%, menunjukkan perusahaan berada pada lingkungan dengan ancaman siber tinggi. Kondisi ini dipengaruhi oleh layanan keamanan siber yang diberikan kepada sektor perbankan, telekomunikasi, dan BUMN. Untuk mengurangi risiko, perusahaan menerapkan kontrol seperti firewall, VPN, enkripsi data, SIEM, dan 2FA.

2) *Design Factor 6 (Compliance Requirements)*

Design factor ini digunakan untuk mengevaluasi tingkat kebutuhan organisasi dalam memenuhi regulasi, standar, maupun ketentuan yang berkaitan dengan pengelolaan teknologi informasi dan keamanan data. Hasil analisis dapat dilihat pada diagram lingkaran berikut:

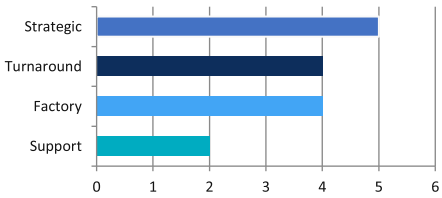


Hasil. *Design Factor 6 (Compliance Requirements)*

Hasil penilaian menunjukkan bahwa kebutuhan kepatuhan berada pada kategori *High* (100%), menunjukkan bahwa kepatuhan merupakan prioritas utama. Perusahaan mengacu pada UU PDP, GDPR, dan PCI DSS, meskipun masih diperlukan peningkatan tata kelola internal, seperti pengelolaan data produksi untuk pengujian dan penerapan standar keamanan yang lebih terintegrasi.

3) *Design Factor 7 (Role of IT)*

Analisis *design factor* ini bertujuan untuk mengetahui posisi dan kontribusi teknologi informasi dalam mendukung aktivitas bisnis perusahaan. Hasil penilaian ditunjukkan pada diagram batang berikut:

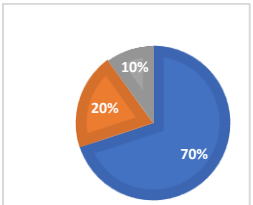


Gambar 7. Hasil. *Design Factor 7 (Role of IT)*

Berdasarkan hasil analisis, kategori *Strategic* memperoleh nilai tertinggi (5), diikuti *Factory* dan *Turnaround* (4), serta *Support* (2). Hasil ini menunjukkan bahwa TI berperan strategis dalam mendukung layanan utama perusahaan sekaligus mendorong inovasi.

4) *Design Factor 8 (Sourcing Model for IT)*

Tahap selanjutnya adalah menganalisis model penyediaan layanan teknologi informasi yang digunakan perusahaan. Hasil pemetaan dapat dilihat pada diagram lingkaran berikut:

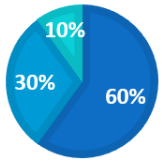


Gambar 8. Hasil *Design Factor 8 (Sourcing Model for IT)*

Berdasarkan hasil model *Outsourcing* mendominasi sebesar 70%, diikuti *Cloud* (20%) dan *Insourced* (10%). Hal ini menunjukkan ketergantungan perusahaan terhadap solusi vendor eksternal, sementara tim internal berfokus pada keamanan data, integrasi sistem, dan pengelolaan infrastruktur.

5) Design Factor 9 (IT Implementation Methods)

Design factor ini menganalisis pendekatan yang digunakan perusahaan dalam mengembangkan dan mengimplementasikan solusi teknologi informasi. Hasil analisis disajikan pada diagram lingkaran berikut:

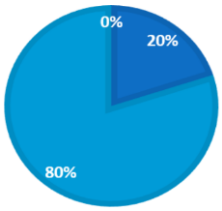


Gambar 9. Hasil *Design Factor 9 (IT Implementation Methods)*

Berdasarkan hasil pemetaan, metode *Agile* memperoleh 60%, *DevOps* 30%, dan *Traditional* 10%. Hasil ini menunjukkan bahwa perusahaan lebih mengutamakan pendekatan yang adaptif, dengan DevOps mendukung proses pengujian dan implementasi, sedangkan metode tradisional digunakan pada aktivitas yang membutuhkan dokumentasi formal.

6) Design Factor 10 (Technology Adoption Strategy)

Analisis terakhir pada tahap ini dilakukan untuk mengetahui strategi perusahaan dalam mengadopsi perkembangan teknologi. Hasil penilaian ditunjukkan pada diagram lingkaran berikut:

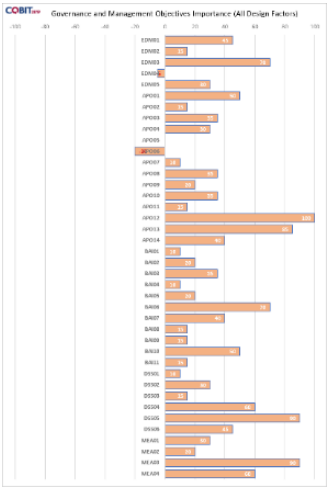


Gambar 10. Hasil *Design Factor 10 (Technology Adoption Strategy)*

Berdasarkan hasil analisis, kategori *Follower* mendominasi sebesar 80%, sedangkan *First Mover* sebesar 20%. Hal ini menunjukkan bahwa PT OGN mengadopsi teknologi setelah mempertimbangkan kesiapan implementasi, kebutuhan pelanggan, dan regulasi, namun tetap melakukan riset pada teknologi baru seperti *Artificial Intelligence* (AI) dan keamanan informasi.

Step 4: Menyusun Rancangan Tata Kelola TI

Pada tahap ini, hasil analisis *Design Factor* 1–10 diintegrasikan menggunakan COBIT 2019 *Design Toolkit* untuk menghasilkan rekomendasi *Governance and Management Objectives* yang sesuai dengan karakteristik dan kebutuhan PT OGN. Hasil pemetaan ditunjukkan pada Gambar 11.



Gambar 11. *Governance and Management Objectives Importance*

Berdasarkan hasil pemetaan, diperoleh empat domain dengan nilai *importance* tertinggi sebagai prioritas tata kelola TI, sebagaimana disajikan pada Tabel 1.

Tabel 1. Domain Prioritas Tata Kelola dan Manajemen TI

Domain	**Objektif Tata Kelola/Manajemen**	**Nilai Kepentingan *(Importance)***
APO12	*Managed Risk*	100
DSS05	*Managed Security Services*	90
MEA03	*Managed Compliance with External Requirements*	90
APO13	*Managed Security*	85

Berdasarkan hasil COBIT 2019 *Design Toolkit* pada Tabel 1, terdapat empat domain dengan nilai *importance* tertinggi, yaitu APO12 (*Managed Risk*) sebesar 100, DSS05 (*Managed Security Services*) dan MEA03 (*Managed Compliance with External Requirements*) masing-masing sebesar 90, serta APO13 (*Managed Security*) sebesar 85. Hasil ini menunjukkan bahwa prioritas tata kelola TI di PT OGN berfokus pada pengelolaan risiko, keamanan informasi, dan kepatuhan terhadap regulasi. Dari keempat domain tersebut, penelitian ini

memfokuskan analisis pada DSS05 karena paling sesuai dengan karakteristik PT OGN yang bergerak di bidang *cyber security*, sehingga pengelolaan layanan keamanan menjadi aspek yang paling relevan untuk dievaluasi.

B. Pengukuran Tingkat Kapabilitas

Berdasarkan hasil COBIT 2019 *Design Toolkit*, diperoleh empat domain prioritas, yaitu APO12, APO13, DSS05, dan MEA03. Penelitian ini memfokuskan pengukuran kapabilitas pada DSS05 (*Managed Security Services*) karena paling sesuai dengan karakteristik PT OGN yang bergerak di bidang *cyber security*.

Pengukuran tingkat kapabilitas dilakukan berdasarkan hasil wawancara dan observasi terhadap proses keamanan yang diterapkan di perusahaan. Penilaian mengacu pada COBIT 2019 *Process Assessment Model* (PAM), dengan kategori penilaian sebagai berikut:

- *Fully* (F) : > 85%
- *Largely* (L) : 50% – 85%
- *Partially* (P) : 15% – 50%
- *Not* (N) : < 15%

Apabila suatu level memperoleh nilai *Fully* (F), maka proses dapat dilanjutkan ke level berikutnya. Sebaliknya, apabila hasil penilaian berada pada kategori *Largely* (L), *Partially* (P), atau *Not* (N), maka penilaian berhenti pada level tersebut dan level kapabilitas yang dicapai adalah level sebelumnya.

Hasil pengukuran pada domain DSS05 *(Managed Security Services)* dilakukan terhadap tujuh *management practice* yang berkaitan dengan pengelolaan keamanan layanan TI. Ringkasan hasil pengukuran tingkat kapabilitas setiap praktik disajikan pada Tabel 2.

Tabel 2. Hasil Pengukuran Tingkat Kapabilitas yang Dicapai Domain DSS05

Management Practice	***Capability Level***
DSS05.01 *Protect Against Malicious Software*	Level 4
DSS05.02 *Manage Network and Connectivity Security*	Level 1
DSS05.03 *Manage Endpoint Security*	Level 1
DSS05.04 *Manage User Identity and Logical Access*	Level 4
DSS05.05 *Manage Physical Access to I&T Assets*	Level 3
DSS05.06 *Manage Sensitive Documents and Output Devices*	Level 3
DSS05.07 *Manage Vulnerabilities and Monitor Infrastructure for Security-Related Events*	Level 3

Berdasarkan Hasil pengukuran menunjukkan bahwa DSS05.01 dan DSS05.04 telah mencapai Level 4, menandakan proses keamanan telah diterapkan secara konsisten dan dievaluasi secara berkala. DSS05.05, DSS05.06, dan DSS05.07 mencapai Level 3, yang menunjukkan proses telah terdefinisi dan diterapkan, namun masih memerlukan peningkatan agar lebih terukur. Sementara itu, DSS05.02 dan DSS05.03 hanya mencapai Level 1, sehingga keamanan jaringan dan *endpoint* menjadi prioritas utama untuk ditingkatkan di PT OGN.

C. Analisis Kesenjangan

Analisis kesenjangan merupakan pendekatan yang digunakan untuk mengukur perbedaan antara tingkat kapabilitas tata kelola TI saat ini dan tingkat yang ditargetkan, sehingga dapat diketahui area yang memerlukan perbaikan [18]. Selanjutnya, peneliti memilih domain yang relevan dengan studi kasus pada perusahaan, yaitu Data Security. Domain yang dipilih adalah DSS05. Hasil analisis kesenjangan pada domain tersebut disajikan pada Tabel 3.

Tabel 3. Hasil analisis kesenjangan [1]

Management Practice	***Existing***	***Target***	***Gaps***
DSS05.02 Manage network and connectivity security	1	2	1
DSS05.03 Manage endpoint security.	1	2	1

Berdasarkan hasil pengukuran pada Tabel 3, kedua *management practice* yang dianalisis, yaitu *DSS05.02 Manage Network and Connectivity Security* dan *DSS05.03 Manage Endpoint Security*, memiliki tingkat kapabilitas saat ini pada level 1. Sementara itu, target kapabilitas yang ditetapkan berada pada level 2. Dengan demikian, masing-masing management practice memiliki nilai kesenjangan sebesar 1 level. Oleh karena itu, diperlukan upaya perbaikan pada kedua management practice tersebut agar tingkat kapabilitas tata kelola keamanan data dapat mencapai level 2.

D. Rekomendasi Perbaikan

Rekomendasi perbaikan disusun untuk membantu perusahaan mencapai target kapabilitas level 2 melalui penguatan pengelolaan keamanan jaringan, konektivitas, dan perangkat *endpoint* secara lebih terstruktur, terdokumentasi, dan konsisten. Rekomendasi diformulasikan berdasarkan hasil analisis kesenjangan pada praktik *DSS05.02 (Manage Network and Connectivity Security)* dan *DSS05.03 (Manage Endpoint Security)* dengan mengacu pada aspek manusia, proses, dan teknologi.

1. *Rekomendasi perbaikan DSS05.02*

Implementasi DSS05.02 di PT OGN berada pada tingkat kapabilitas 1 dengan target level 2. Kesenjangan utama terletak pada belum optimalnya pengelolaan keamanan perangkat yang mengakses sistem sensitif, khususnya dalam pengaturan prioritas perangkat resmi, pembatasan perangkat pribadi, serta penerapan standar keamanan pada lingkungan *development*. Oleh karena itu, rekomendasi perbaikan difokuskan pada aspek manusia, proses, dan teknologi.

Pada aspek manusia, perusahaan perlu meningkatkan kompetensi personel melalui pelatihan terstruktur berbasis SFIA versi 8, khususnya pada keterampilan *Information Security* dan *Security Operations*. Materi pelatihan mencakup penerapan enkripsi *data at rest*, penggunaan VPN, serta implementasi *Role-Based Access Control (RBAC)* berbasis LDAP. Selain itu, sosialisasi keamanan informasi perlu dilaksanakan secara berkala untuk meningkatkan kesadaran terhadap risiko akses internal dan pentingnya perlindungan data.

Pada aspek proses, perusahaan perlu menyusun kebijakan keamanan *endpoint* dan lingkungan *development* yang mewajibkan penerapan *full disk encryption* serta prinsip *least privilege*. Perusahaan juga perlu menetapkan SOP validasi perangkat pribadi maupun perangkat remote sebelum memperoleh akses VPN, menyusun Prosedur Penggunaan Perangkat TI dan Prosedur Keamanan Jaringan, serta menerapkan peninjauan audit log berbasis risiko melalui SIEM untuk mendeteksi anomali akses terhadap sistem sensitif.

Pada aspek teknologi, perusahaan perlu mengoptimalkan solusi enkripsi *OpenText* pada penyimpanan lokal perangkat *developer*, mengintegrasikan VPN dengan RBAC berbasis LDAP, serta menyusun rencana implementasi *Identity and Access Management/Privileged Access Management (IAM/PAM)* terpusat. Selain itu, fitur *Host Check* pada VPN perlu diaktifkan agar hanya perangkat yang memenuhi standar keamanan yang dapat mengakses repositori maupun sistem sensitif.

2. *Rekomendasi perbaikan DSS05.03*

Implementasi DSS05.03 di PT OGN berada pada tingkat kapabilitas 1 dengan target level 2. Kesenjangan utama terletak pada belum terdokumentasinya mekanisme pengelolaan akses berisiko melalui surel dan peramban, seperti pemblokiran URL berbahaya dan penyaringan surel phishing, meskipun kontrol keamanan endpoint telah diterapkan. Oleh karena itu, rekomendasi perbaikan difokuskan pada aspek manusia, proses, dan teknologi.

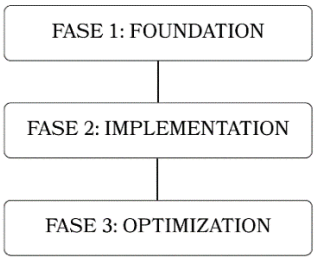
Pada aspek manusia, perusahaan perlu membentuk Tim *Data Security* yang bertanggung jawab terhadap penerapan dan pengawasan kontrol keamanan surel serta peramban. Kompetensi tim perlu ditingkatkan melalui pelatihan berbasis SFIA versi 8 pada keterampilan *Information Security* dan *Security Administration* agar mampu melakukan deteksi, pemantauan, dan penanganan ancaman secara efektif.

Pada aspek proses, perusahaan perlu menyusun kebijakan keamanan email dan web browser, menetapkan SOP pengelolaan keamanan email, serta menyusun Prosedur Pertukaran Informasi melalui Media Telekomunikasi yang mengatur mekanisme penggunaan email, penyaringan surel berbahaya, pemblokiran URL berisiko, pemantauan aktivitas, dan penanganan insiden keamanan. Sebagai bukti implementasi, perusahaan juga perlu mendokumentasikan log serta laporan pemantauan aktivitas secara berkala.

Pada aspek teknologi, perusahaan perlu mengoptimalkan *firewall, Security Operations Center (SOC)*, dan solusi keamanan *endpoint* yang telah dimiliki dengan menambahkan fungsi *Email Security Gateway* dan *Web Filtering*. Selain itu, fitur *URL Filtering, Anti-Phishing, Safe Browsing*, dan *Email Threat Protection* perlu diaktifkan untuk memperkuat perlindungan terhadap ancaman yang berasal dari email maupun aktivitas penelusuran *web*.

3. *Roadmap Rekomendasi Perbaikan*

Rekomendasi perbaikan yang telah disusun selanjutnya diterjemahkan ke dalam roadmap implementasi sebagai panduan pelaksanaan yang sistematis. Berbeda dengan subbab sebelumnya yang menjelaskan apa rekomendasi yang perlu diterapkan, roadmap ini menggambarkan urutan pelaksanaan, prioritas implementasi, serta luaran *(deliverable)* yang dihasilkan pada setiap tahap. Penyusunan *roadmap* didasarkan pada ketergantungan antaraktivitas, sehingga penguatan tata kelola ditempatkan sebagai fondasi sebelum implementasi teknis dilakukan. *Roadmap* dibagi ke dalam tiga fase strategis selama 12 bulan sebagaimana ditunjukkan pada Gambar 12.



Gambar 12. Roadmap Rekomendasi Perbaikan

Fase 1: *Foundation* (bulan 1–3) berfokus pada penyediaan fondasi tata kelola melalui penyusunan kebijakan, prosedur, SOP, struktur organisasi, serta dokumen pendukung lainnya yang diperlukan sebelum implementasi teknis dilakukan. Luaran pada fase ini menjadi acuan dalam pelaksanaan pengendalian keamanan pada tahap berikutnya. Rincian aktivitas beserta luaran yang dihasilkan pada fase ini disajikan pada Tabel 4.

Tabel 4. Fase 1: *Foundation*

Aktivitas	*Deliverable*
Pengesahan Kebijakan Keamanan *Endpoint* dan Lingkungan *Development*	Dokumen Kebijakan Keamanan *Endpoint* dan *Development*
Penyusunan Kebijakan Keamanan Email dan *Web Browser*	Dokumen Kebijakan Keamanan Email dan *Web Browser*
Penyusunan Prosedur Keamanan Jaringan	Dokumen Prosedur Keamanan Jaringan
Penyusunan Prosedur Penggunaan Perangkat TI	Dokumen Prosedur Penggunaan Perangkat TI
Penyusunan Prosedur Pertukaran Informasi melalui Media Telekomunikasi	Dokumen Prosedur Pertukaran Informasi melalui Media Telekomunikasi
Finalisasi SOP BYOD	SOP BYOD
Penyusunan Matriks Kompetensi SFIA 8	Dokumen Matriks Kompetensi
Penyusunan Materi Pelatihan Kemanan Informasi	Modul Pelatihan

Fase 2: *Implementation* (Bulan 4-8) berfokus pada penerapan kebijakan dan prosedur yang telah disusun pada fase sebelumnya melalui implementasi kontrol keamanan, pelaksanaan sosialisasi dan pelatihan, serta penguatan mekanisme perlindungan *endpoint*, jaringan, email, dan pengelolaan akses. Pada tahap ini, perusahaan mulai mengoperasikan kontrol keamanan sesuai dengan kebijakan yang telah ditetapkan. Rincian aktivitas beserta deliverable pada fase ini disajikan pada Tabel 5.

Tabel 5. Fase 2: *Implementation*

Aktivitas	*Deliverable*
Sosialisasi Kebijakan Keamanan Informasi	Laporan Sosialisasi
Pelatihan Keamanan Informasi bagi Seluruh Personel	Laporan Pelatihan
Pelatihan Teknis Tim *Data Security*	Laporan/Sertifikat Pelatihan
Implementasi *Full Disk Encryption* menggunakan OpenText	*Endpoint* terenkripsi
Implementasi SOP BYOD	SOP diterapkan
Aktivasi *Email Threat Protection*, *Anti-Phishing*, *URL Filtering*, dan *Safe Browsing*	Konfigurasi Keamanan Email dan *Web Browser*
Integrasi VPN dengan RBAC berbasis LDAP	VPN dengan RBAC aktif
Penyusunan Desain Awal IAM/PAM Terpusat	Dokumen Desain IAM/PAM

Selanjutnya, Fase 3: *Optimization* (Bulan 9-12) merupakan tahap akhir yang berfokus pada monitoring, evaluasi, dan penyempurnaan terhadap implementasi yang telah dilakukan. Tujuan utama fase ini adalah memastikan efektivitas kontrol keamanan, meningkatkan kepatuhan terhadap kebijakan yang telah ditetapkan, serta mendukung peningkatan kapabilitas keamanan informasi secara berkelanjutan. Rincian aktivitas beserta deliverable pada fase ini disajikan pada Tabel 6.

Tabel 6. Fase 3: *Optimization*

Aktivitas	*Deliverable*
Aktivasi Fitur *Host Check* pada VPN	VPN dengan *Host Check* aktif
Pembangunan *Dashboard Log* dan Pelaporan Kepatuhan	*Dashboard Monitoring*
Integrasi Log ke Splunk/SIEM	Sistem Monitoring Log Terintegrasi
Pelaksanaan *Risk-Based Audit Log*	Laporan Audit Log
Implementasi SOP BYOD	SOP diterapkan
Evaluasi Efektivitas Kontrol Keamanan	Laporan Evaluasi Kontrol
Peninjauan Kompetensi Tim *Data Security*	Laporan Evaluasi Kompetensi
Finalisasi *Blueprint* IAM/PAM	Dokumen *Blueprint* IAM/PAM

Penyusunan Laporan Kepatuhan COBIT 2019 DSS05	Laporan Kepatuhan Tata Kelola

4. KESIMPULAN

Evaluasi layanan keamanan terkelola pada PT OGN menggunakan kerangka kerja COBIT 2019 menunjukkan bahwa DSS05 (*Managed Security Services*) merupakan domain yang paling relevan berdasarkan hasil analisis *Design Factors*. Pengukuran tingkat kapabilitas menunjukkan bahwa DSS05.02 (*Manage Network and Connectivity Security*) dan DSS05.03 (*Manage Endpoint Security*) masih memerlukan peningkatan, sehingga disusun rekomendasi perbaikan pada aspek *people*, *process*, dan *technology* dalam bentuk *roadmap* implementasi. Hasil penelitian ini menunjukkan bahwa COBIT 2019 mampu mengidentifikasi tingkat kapabilitas, kesenjangan proses, serta menghasilkan rekomendasi yang selaras dengan kebutuhan bisnis, profil risiko, dan kepatuhan PT OGN. Penelitian selanjutnya dapat berfokus pada implementasi *roadmap* yang telah diusulkan serta mengevaluasi dampaknya terhadap peningkatan tingkat kapabilitas, maupun memperluas cakupan evaluasi pada domain COBIT 2019 lainnya agar diperoleh gambaran tata kelola teknologi informasi yang lebih menyeluruh.

UCAPAN TERIMA KASIH

Kelancaran penyusunan jurnal ini tidak terlepas dari dukungan akademik Program Studi Sistem Informasi Universitas Telkom Jakarta serta bantuan data dan informasi yang diberikan oleh PT OGN. Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan sehingga penelitian ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

[1] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," 2024. doi: 10.6028/NIST.CSWP.29.

[2] IBM Security, "IBM X-Force Threat Intelligence Index 2025," 2025.

[3] European Union Agency for Cybersecurity, "ENISA Threat Landscape 2024," 2024.

[4] Verizon, "2025 Data Breach Investigations Report," 2025.

[5] S. C. I. Simatupang and M. I. Fianty, "Assessment of Capability Levels and Improvement Recommendations Using COBIT 2019 for the IT Consulting Industry," *G-Tech: Jurnal Teknologi Terapan*, vol. 7, no. 4, 2023, doi: 10.33379/gtech.v7i4.3141.

[6] M. I. Fianty and M. B. Hardjadinata, "Leveraging COBIT 2019 Framework to Implement IT Governance in Business Process Outsourcing Company," *Journal of Information Systems Engineering and Business Intelligence*, vol. 5, no. 2, pp. 568–579, 2023, doi: 10.51519/journalisi.v5i2.492.

[7] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Rolling Meadows, Illinois: ISACA, 2020.

[8] ISACA, *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*. Rolling Meadows, IL: ISACA, 2019.

[9] S. De Haes, W. Van Grembergen, A. Joshi, and T. Huygh, *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*. Springer, 2020. doi: 10.1007/978-3-030-25918-1.

[10] R. Yulita and J. J. C. Tambotoh, "Risk Management Analysis of PT OGN Using COBIT 2019 with Domain EDM03, APO12, APO13, and DSS05," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 5, pp. 2033–2047, 2024, doi: 10.32520/stmsi.v13i5.4430.

[11] A. M. Vasya, "Audit Sistem Informasi Tata Kelola Keamanan Pada Layanan Website Online Single Submission Menggunakan COBIT 2019," *JUSTIKPEN*, vol. 5, no. 1, pp. 165–172, 2025, doi: 10.55338/justikpen.v5i1.332.

[12] M. Destriani and Y. H. Putra, "Rencana Audit Tata Kelola Sistem Informasi di Universitas Subang Menggunakan Framework COBIT 2019," *JTK3TI*, vol. 9, no. 1, pp. 12–25, 2023, doi: 10.34010/jtk3ti.v9i1.9164.

[13] A. R. S. Sembiring, S. S. Ahmad, and M. I. Rosadi, "Audit of Academic Information System Governance using COBIT 2019 (Case Study: Subang University)," in *AIP Conference Proceedings*, 2024, p. 40005. doi: 10.1063/5.0253883.

[14] B. V Tulus and A. R. Tanaamah, "Design of Information Technology Governance in Educational Institutions using COBIT 2019 Framework," *Journal of Information Systems and Informatics*, vol. 5, no. 1, pp. 31–43, 2023, doi: 10.51519/journalisi.v5i1.408.

[15] A. Nisri, "Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja COBIT 2019," *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi (JTK3TI)*, vol. 9, no. 1, pp. 34–41, 2023, doi: 10.34010/jtk3ti.v9i1.9672.

[16] "Introduction to SFIA documentation Contents," 2021. [Online]. Available: www.sfia-online.org

[17] R. Afdhani and B. Soewito, "Perancangan Tata Kelola TI Menggunakan Framework COBIT 2019 pada Pusat Data dan Informasi Kementerian," *Jurnal Tata Kelola dan Kerangka Kerja TI*, vol. 10, no. 1, p. 22, 2024.

[18] G. R. Amalia, A. F. Santoso, and D. Praditya, "Analisis Dan Perancangan Tata Kelola Teknologi Informasi PT. XYZ Menggunakan COBIT 2019 Pada Objektif BAI01, BAI02, DAN BAI11," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 586–589, May 2024, doi: 10.29100/jipi.v9i2.4612.