

Evaluasi Keamanan Informasi Menggunakan COBIT 2019 APO13 dalam Mendukung Kualitas Layanan TI

Zulmi Gurhono^{*1}, Alva Hendi Muhammad², Asro Nasiri³

^{1,2,3} Magister Informatika, Fakultas Pascasarjana, Universitas AMIKOM Yogyakarta

e-mail: ¹zulmi_gurhono@students.amikom.ac.id, ²alva@amikom.ac.id, ³asro@amikom.ac.id

**Correspondence author*

Abstrak

Kualitas layanan teknologi informasi di institusi pendidikan tinggi kesehatan sangat bergantung pada tata kelola keamanan informasi yang terancang dengan baik. Poltekkes Kemenkes Bengkulu mengelola data akademik dan data kesehatan yang rentan terhadap ancaman siber, namun belum pernah dirancang sistem tata kelola TI berbasis kerangka kerja terstandar untuk menentukan prioritas keamanan informasinya. Penelitian ini bertujuan merancang sistem tata kelola TI dan menentukan prioritas *governance and management objectives* menggunakan COBIT 2019 Governance System Design Workflow, dengan APO13 – Managed Security sebagai *objective* fokus studi kasus. Metode yang digunakan adalah analisis sepuluh Design Factors yang diisi berdasarkan kondisi aktual institusi melalui wawancara mendalam, observasi, dan studi dokumentasi. Hasil analisis menghasilkan tiga luaran utama. Pertama, dari 40 *governance and management objectives* COBIT 2019 teridentifikasi 17 *objective* prioritas, dipimpin oleh BAI10 – Managed Configuration (skor 100), APO13 – Managed Security (skor 90), dan APO12 – Managed Risk (skor 85). Kedua, ditetapkan target *capability level* 4 (kategori Kritis) untuk sembilan *objective* teratas termasuk APO13, yang skornya secara konsisten didorong oleh risiko *logical attacks* pada profil risiko (DF3), *threat landscape* yang dinilai High (DF5), dan *compliance requirements* terhadap regulasi Kementerian Kesehatan yang juga High (DF6). Ketiga, disusun rekomendasi operasional berupa penguatan kebijakan keamanan informasi (ISMS), manajemen insiden dan risiko keamanan, serta kontrol akses sebagai acuan peningkatan kualitas layanan TI di Poltekkes Kemenkes Bengkulu. Penelitian ini masih terbatas pada penentuan prioritas dan target *capability level*, sehingga pengukuran *capability level* aktual dan analisis gap disarankan sebagai agenda penelitian lanjutan.

Kata kunci—COBIT 2019, APO13, keamanan informasi, kualitas layanan TI, tata kelola TI

1. PENDAHULUAN

Poltekkes Kemenkes Bengkulu sebagai perguruan tinggi kesehatan di bawah naungan Kementerian Kesehatan Republik Indonesia memiliki ketergantungan yang tinggi terhadap pemanfaatan teknologi informasi dalam mendukung proses akademik, administrasi, dan pelayanan institusi. Berbagai layanan digital seperti sistem informasi akademik, keuangan, kepegawaian, pembelajaran daring, hingga pelaporan data kesehatan telah menjadi bagian penting dalam operasional organisasi. Kondisi ini menunjukkan bahwa teknologi informasi tidak lagi hanya berfungsi sebagai alat bantu administratif, melainkan telah berkembang menjadi aset strategis yang menentukan efektivitas layanan, efisiensi organisasi, serta daya saing institusi pendidikan tinggi kesehatan [1]. Pengelolaan teknologi informasi yang terencana terbukti mampu meningkatkan mutu layanan dan kualitas pengambilan keputusan di lingkungan perguruan tinggi [2]. Oleh karena itu, keberhasilan pengelolaan teknologi informasi menjadi salah satu faktor penting dalam mendukung pencapaian visi dan misi institusi.

Urgensi penguatan tata kelola teknologi informasi semakin meningkat seiring dengan percepatan transformasi digital di sektor kesehatan. Institusi kesehatan dituntut menyediakan layanan digital yang aman, terintegrasi, dan adaptif, sementara pada saat yang sama menghadapi peningkatan ancaman siber terhadap data pasien dan data institusional [3]. Namun demikian, implementasi teknologi informasi tanpa tata kelola yang baik berpotensi menimbulkan berbagai risiko, seperti pemborosan anggaran TI, duplikasi sistem, lemahnya keamanan informasi, rendahnya efektivitas layanan, hingga ketidaksesuaian antara investasi TI dengan tujuan strategis

organisasi. Sejumlah evaluasi pada fasilitas layanan kesehatan menunjukkan bahwa tingkat kapabilitas pengelolaan keamanan sistem informasi masih berada di bawah target yang diharapkan, sehingga diperlukan penguatan kontrol dan kebijakan secara sistematis [4].

Keamanan informasi merupakan salah satu faktor penting dalam menjamin kualitas layanan teknologi informasi, karena kemampuan organisasi dalam menjaga kerahasiaan data berpengaruh terhadap keandalan dan kepercayaan pengguna terhadap layanan yang diberikan. ISO/IEC 27001:2022 menempatkan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi sebagai sasaran utama sistem manajemen keamanan informasi [5], dan penerapannya di lingkungan perguruan tinggi terbukti membantu institusi menilai tingkat kepatuhan sekaligus menutup celah kontrol yang belum terpenuhi [6]. Tata kelola keamanan informasi juga perlu bersifat dinamis dan adaptif agar mampu merespons perubahan lanskap ancaman siber yang berlangsung cepat [7]. Evaluasi pada institusi pendidikan juga memperlihatkan bahwa pengelolaan risiko dan keamanan yang belum optimal berdampak langsung pada rendahnya mutu tata kelola layanan TI [8]. Dalam perspektif manajemen layanan TI, praktik information security management melekat pada keseluruhan rantai nilai layanan sehingga pengamanan informasi tidak dapat dipisahkan dari upaya menjaga mutu layanan [9]. Dengan demikian, penerapan keamanan informasi yang memadai berkontribusi secara langsung terhadap peningkatan kualitas layanan teknologi informasi yang diberikan organisasi kepada para pemangku kepentingannya.

Tata kelola teknologi informasi merupakan bagian integral dari tata kelola organisasi yang mencakup kepemimpinan, struktur organisasi, dan proses untuk memastikan bahwa teknologi informasi mendukung strategi dan tujuan organisasi. Tata kelola TI yang efektif tidak hanya berorientasi pada pencapaian nilai (value delivery), tetapi juga pengelolaan risiko (risk management) dan optimalisasi sumber daya TI [10]. Dalam konteks organisasi publik, keberhasilan tata kelola TI sangat ditentukan oleh kesesuaian desain tata kelola dengan karakteristik dan kebutuhan kontekstual organisasi yang bersangkutan [11]. Pada perguruan tinggi kesehatan, tantangan tersebut menjadi lebih kompleks karena tata kelola TI harus mendukung proses akademik sekaligus memenuhi standar layanan kesehatan dan regulasi pemerintah, sehingga pengelolaan TI yang tidak terstruktur dapat berdampak langsung terhadap kualitas layanan pendidikan, akurasi data kesehatan, serta kepercayaan publik terhadap institusi.

Untuk mewujudkan tata kelola TI yang efektif diperlukan suatu kerangka kerja yang sistematis dan terstandarisasi. Salah satu framework yang banyak digunakan secara internasional adalah COBIT (Control Objectives for Information and Related Technologies) 2019 yang dikembangkan oleh ISACA [12]. COBIT 2019 merupakan pengembangan dari COBIT 5 yang dirancang untuk membantu organisasi dalam mengelola dan mengendalikan teknologi informasi secara terintegrasi dengan tujuan organisasi. Framework ini terdiri atas 40 governance and management objectives yang terbagi ke dalam lima domain utama, yaitu EDM (Evaluate, Direct and Monitor), APO (Align, Plan and Organise), BAI (Build, Acquire and Implement), DSS (Deliver, Service and Support), dan MEA (Monitor, Evaluate and Assess) [13]. Keunggulan COBIT 2019 dibandingkan framework sebelumnya terletak pada adanya konsep Design Factors yang memungkinkan organisasi menyesuaikan desain tata kelola TI berdasarkan kondisi dan kebutuhan organisasi secara kontekstual [14].

Konsep Design Factors dalam COBIT 2019 menjadi sangat relevan untuk diterapkan pada institusi pendidikan tinggi kesehatan karena mempertimbangkan faktor strategis organisasi, profil risiko, kebutuhan kepatuhan regulasi, kondisi ancaman keamanan, hingga strategi adopsi teknologi. Melalui pendekatan ini, organisasi dapat menentukan prioritas governance and management objectives yang paling sesuai dengan kondisi aktual institusi, sebagaimana ditunjukkan pada penyesuaian sistem tata kelola COBIT 2019 di institusi pendidikan tinggi dengan sumber daya terbatas [15]. Selain itu, COBIT 2019 juga menyediakan pendekatan capability level untuk mengukur tingkat kematangan proses tata kelola TI mulai dari level 0 (Incomplete) hingga level 5 (Optimizing). Pendekatan ini memungkinkan organisasi mengetahui kondisi tata kelola TI saat ini sekaligus menentukan target peningkatan yang ingin dicapai secara berkelanjutan [16].

Sejumlah penelitian terdahulu telah membuktikan efektivitas COBIT 2019 dalam merancang dan mengevaluasi tata kelola TI pada berbagai jenis organisasi. Penelitian pada sektor korporasi menunjukkan bahwa analisis berbasis Design Factors menghasilkan prioritas tata kelola TI yang lebih akurat dan kontekstual dibandingkan pendekatan asesmen generik [17], [18]. Kajian literatur terhadap penerapan COBIT 2019 juga menegaskan bahwa pemilihan domain yang tepat sangat menentukan kualitas temuan audit dan relevansi rekomendasi yang dihasilkan [19]. Selain itu, perancangan model tata kelola berbasis domain tertentu dalam COBIT 2019 terbukti mampu menghasilkan panduan operasional yang dapat langsung diterapkan oleh unit pengelola TI [20].

Berdasarkan kondisi aktual di Poltekkes Kemenkes Bengkulu, masih ditemukan beberapa permasalahan terkait tata kelola teknologi informasi, seperti pengendalian biaya TI yang belum optimal, adanya insiden keamanan siber, belum jelasnya proses pengambilan keputusan investasi TI, serta pengelolaan layanan TI berbasis pihak ketiga (outsourcing) yang belum terstruktur secara baik. Permasalahan tersebut menunjukkan bahwa pengelolaan TI di lingkungan institusi masih menghadapi tantangan dalam aspek pengendalian, pengawasan, dan penyelarasan strategi TI dengan tujuan organisasi. Jika kondisi ini tidak segera ditangani, maka dapat berkembang menjadi risiko strategis yang lebih besar, seperti kegagalan sistem layanan, kebocoran data sensitif, pemborosan anggaran TI, hingga terganggunya proses akademik dan administrasi institusi.

Dari sisi praktis, terdapat kesenjangan yang melatarbelakangi penelitian ini. Pertama, hingga saat ini belum pernah dilakukan evaluasi keamanan informasi berbasis COBIT 2019 di Poltekkes Kemenkes Bengkulu, sehingga institusi belum memiliki gambaran sistematis mengenai kondisi tata kelola keamanan informasinya. Kedua, belum diketahui governance and management objectives mana yang menjadi prioritas untuk mendukung keamanan layanan TI, sehingga upaya perbaikan yang selama ini dilakukan cenderung bersifat reaktif dan belum berbasis kerangka kerja yang terstandarisasi.

Dari sisi penelitian, juga terdapat kesenjangan dengan studi-studi terdahulu. Sebagian besar penelitian keamanan informasi berbasis COBIT 2019 sebelumnya berfokus pada pengukuran capability level domain keamanan seperti DSS05 dan APO13 pada organisasi yang diteliti [8], [21], [22], tanpa terlebih dahulu memastikan apakah objective tersebut memang merupakan prioritas bagi organisasi yang bersangkutan. Penelitian ini mengisi kesenjangan tersebut dengan memanfaatkan Governance System Design Workflow melalui analisis sepuluh Design Factors [14], sehingga prioritas objectives keamanan informasi beserta target capability level-nya ditentukan secara kontekstual berdasarkan strategi, profil risiko, dan kebutuhan kepatuhan institusi, bukan ditetapkan secara apriori.

Berdasarkan uraian tersebut, diperlukan suatu pendekatan analisis yang komprehensif, sistematis, dan kontekstual untuk memetakan kondisi eksisting tata kelola TI serta menentukan prioritas perbaikan yang sesuai dengan kebutuhan organisasi. Oleh karena itu, penelitian ini dilakukan dengan menggunakan pendekatan COBIT 2019 khususnya pada analisis sepuluh Design Factors untuk menentukan prioritas governance and management objectives beserta target capability level yang perlu dicapai oleh Poltekkes Kemenkes Bengkulu.

Penelitian ini secara khusus difokuskan pada perancangan sistem tata kelola dan prioritasasi objective menggunakan seluruh sepuluh Design Factors COBIT 2019, dengan APO13 – Managed Security dijadikan objective fokus karena posisinya sebagai prioritas kedua tertinggi hasil agregasi seluruh Design Factors. Objective lain yang turut dibahas, seperti BAI10, APO12, dan DSS05, disertakan bukan sebagai temuan yang berdiri sendiri, melainkan sebagai objective pendukung (supporting objectives) yang secara langsung berkorelasi dan memperkuat kapabilitas keamanan informasi pada APO13, sehingga pembahasannya tetap konsisten dengan fokus penelitian. Kontribusi penelitian ini mencakup tiga hal. Pertama, mengidentifikasi governance and management objectives prioritas berdasarkan analisis sepuluh Design Factors COBIT 2019 sesuai kondisi aktual institusi. Kedua, menentukan target capability level keamanan informasi, khususnya pada objective APO13 – Managed Security beserta objectives pendukungnya. Ketiga, menyusun rekomendasi operasional peningkatan keamanan informasi yang dapat langsung diadopsi oleh institusi pendidikan tinggi kesehatan dalam memperkuat kualitas layanan teknologi informasinya.

2. METODE PENELITIAN

Jenis dan pendekatan penelitian

Penelitian ini menggunakan pendekatan deskriptif-kualitatif dengan analisis kuantitatif berbasis toolkit. Pendekatan ini dipilih karena tujuan penelitian adalah mendeskripsikan kondisi aktual tata kelola TI dan menghasilkan skor prioritas objectives berdasarkan perhitungan terstruktur dari COBIT 2019 Design Toolkit [14].

Lokasi dan informan penelitian

Penelitian dilaksanakan di Poltekkes Kemenkes Bengkulu, Jalan Indra Giri Nomor 3, Padang Harapan, Kota Bengkulu. Informan penelitian terdiri atas enam orang pejabat dan staf yang dipilih secara purposive berdasarkan keterlibatan langsung dengan pengelolaan TI institusi, yaitu Direktur, Wakil Direktur II, Kepala Unit Teknologi Informasi dan Komunikasi, dua orang staf operasional TI, serta Kepala Bagian Keuangan.

Teknik pengumpulan data

Pengumpulan data dilakukan melalui empat teknik, yaitu wawancara mendalam (in-depth interview) dengan para informan untuk memperoleh gambaran kondisi tata kelola TI saat ini; observasi langsung terhadap infrastruktur TI, kebijakan, dan prosedur yang ada; studi dokumentasi terhadap laporan keuangan TI, laporan audit, kebijakan keamanan, dan dokumen perencanaan; serta pengisian COBIT 2019 Governance System Design Workbook sebagai instrumen utama yang mengintegrasikan seluruh data yang diperoleh.

Instrumen penelitian

Instrumen utama adalah COBIT 2019 Governance System Design Workbook versi resmi ISACA. Workbook ini terdiri atas sheet Canvas yang memuat ringkasan hasil dan sepuluh sheet Design Factors (DF1–DF10). Setiap Design Factor memiliki skala pengisian yang berbeda: DF1, DF2, dan DF4 menggunakan skala Likert 1–5; DF3 menggunakan matriks dampak (1–5) dikalikan kemungkinan (1–5); sedangkan DF5 hingga DF10 menggunakan distribusi persentase dengan total 100%.

Proses analisis

Proses analisis mengikuti tiga langkah utama COBIT 2019 Governance System Design. Langkah pertama adalah penentuan cakupan awal melalui analisis DF1 (Enterprise Strategy), DF2 (Enterprise Goals), DF3 (Risk Profile), dan DF4 (IT-Related Issues) yang menghasilkan initial scope. Langkah kedua adalah penyempurnaan cakupan melalui analisis DF5 hingga DF10 yang menghasilkan refined scope. Langkah ketiga adalah penyimpulan cakupan akhir dari agregasi seluruh Design Factors, yang menghasilkan prioritas dan target capability level untuk setiap objective.

Secara keseluruhan, tahapan penelitian yang dilakukan mulai dari identifikasi masalah hingga penyusunan rekomendasi ditunjukkan pada Gambar 1.

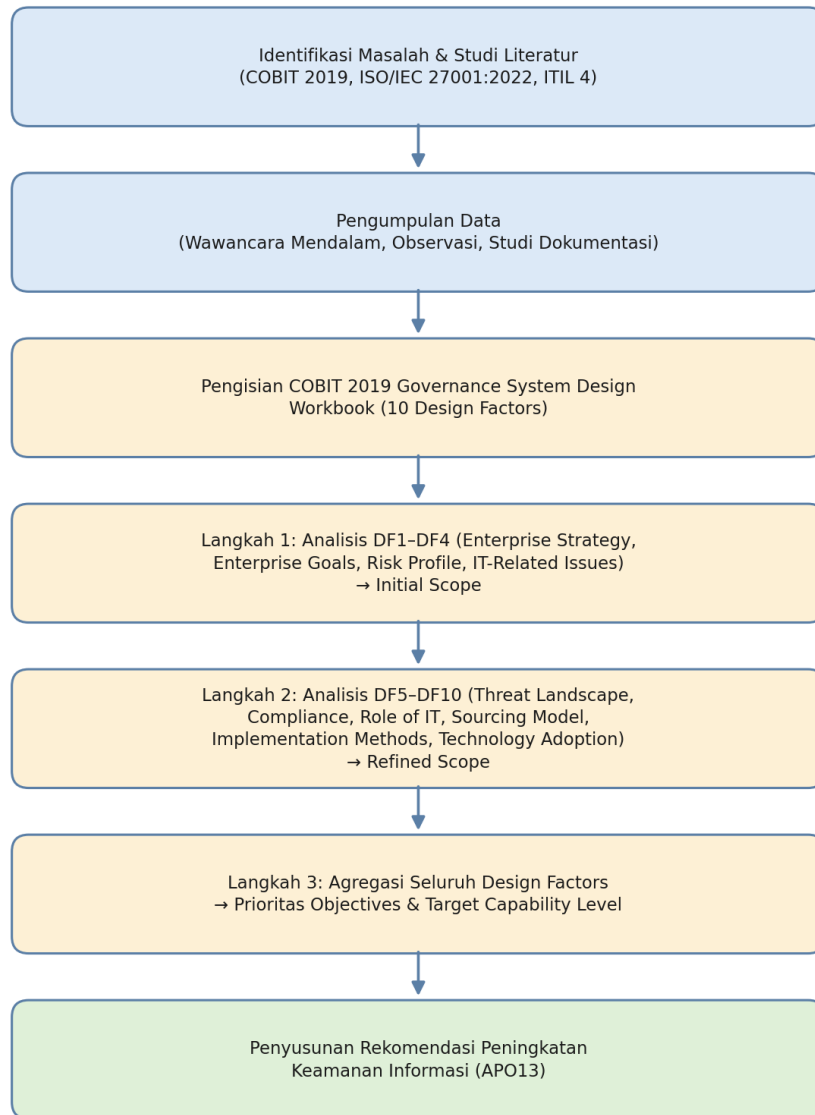
3. HASIL DAN PEMBAHASAN

Gambaran umum Poltekkes Kemenkes Bengkulu

Poltekkes Kemenkes Bengkulu menyelenggarakan program studi Diploma III dan Sarjana Terapan di bidang Keperawatan, Kebidanan, Analis Kesehatan, Gizi, dan Kesehatan Lingkungan. Dalam operasionalnya, institusi ini mengelola sejumlah sistem informasi, di antaranya Sistem Informasi Akademik (SIKAD), Sistem Informasi Keuangan, Sistem Informasi Kepegawaian, dan sistem pelaporan Kemenkes. Pengelolaan TI saat ini berada di bawah Unit Teknologi Informasi dan Komunikasi dengan dukungan sebagian layanan dari pihak ketiga (outsourcing).

Hasil analisis sepuluh design factors

Hasil pengisian COBIT 2019 Governance System Design Workbook berdasarkan kondisi aktual Poltekkes Kemenkes Bengkulu ditunjukkan pada Tabel 1.



Gambar 1. Diagram alur metode penelitian

Analisis design factor 1: enterprise strategy

Hasil pengisian DF1 menunjukkan bahwa strategi Cost Leadership dan Client Service/Stability mendominasi dengan nilai 5 (Critical), sementara strategi Growth/Acquisition dan Innovation/Differentiation masing-masing mendapat nilai 1 (Not Important). Temuan ini mencerminkan karakteristik Poltekkes Kemenkes Bengkulu sebagai institusi pendidikan tinggi negeri yang berorientasi pada efisiensi anggaran dan kualitas pelayanan kepada mahasiswa, bukan pada ekspansi bisnis atau inovasi teknologi. Strategi Cost Leadership mendorong tingginya prioritas pada objectives yang terkait pengelolaan anggaran dan sumber daya TI, seperti APO06 – Managed Budget & Costs dan EDM04 – Ensured Resource Optimization. Sementara itu, strategi Client Service/Stability mendorong prioritas pada APO09 – Managed Service

Agreements, DSS02 – Managed Service Requests & Incidents, dan DSS04 – Managed Continuity.

Tabel 1. Hasil analisis sepuluh design factors COBIT 2019 di Poltekkes Kemenkes Bengkulu

Kode	Design factor	Nilai	Implikasi terhadap tata kelola TI
DF1	Enterprise Strategy	Cost Leadership (5), Client Service/Stability (5)	Efisiensi biaya dan kualitas layanan menjadi prioritas utama
DF2	Enterprise Goals	Customer-oriented Service Culture (5), Optimization of Business Process Costs (5)	Layanan kepada mahasiswa dan optimasi biaya operasional TI
DF3	Risk Profile	IT Cost & Oversight (25), Logical Attacks (20), IT Investment (16)	Tiga risiko dengan rating Very High mendominasi profil risiko
DF4	IT-Related Issues	Insiden TI signifikan (3), Hidden IT spending (3), Biaya TI tinggi (3)	Isu kritis terkait insiden keamanan dan pengeluaran TI tidak terkontrol
DF5	Threat Landscape	High	Ancaman siber dinilai tinggi, memperkuat urgensi keamanan informasi
DF6	Compliance Requirements	High (0,25)	Kepatuhan regulasi Kemenkes RI menjadi pertimbangan penting
DF7	Role of IT	Support (1)	TI masih berperan sebagai pendukung, belum strategis
DF8	Sourcing Model	Outsourcing (0,3)	Sebagian layanan TI dikelola pihak ketiga
DF9	IT Implementation Methods	Agile (0,5)	Pendekatan agile mendominasi metode implementasi TI
DF10	Technology Adoption Strategy	First Mover (0,75)	Institusi cenderung mengadopsi teknologi baru lebih awal

Sumber: Hasil pengolahan data peneliti, 2026

Analisis design factor 2: enterprise goals

Pada DF2, dari 13 enterprise goals yang tersedia, Customer-oriented Service Culture dan Optimization of Business Process Costs mendapatkan nilai tertinggi (5), konsisten dengan hasil DF1. Tingginya nilai kedua enterprise goals ini berdampak pada penguatan prioritas objectives di domain DSS (Deliver, Service and Support) yang langsung bersinggungan dengan kualitas layanan kepada mahasiswa, serta objectives di domain APO yang berkaitan dengan efisiensi operasional.

Analisis design factor 3: risk profile

DF3 menghasilkan temuan paling signifikan dalam penelitian ini. Dari 19 kategori risiko TI yang dianalisis, tiga kategori memperoleh rating Very High dan menjadi faktor pendorong utama prioritas governance objectives. Rincian profil risiko TI Poltekkes Kemenkes Bengkulu ditunjukkan pada Tabel 2.

IT Cost & Oversight memperoleh risk rating tertinggi (25) dengan dampak 5 dan kemungkinan 5, mencerminkan bahwa pengeluaran TI yang tidak terkontrol merupakan masalah nyata yang berdampak besar dan sangat mungkin terjadi. Hal ini berkorelasi langsung dengan isu yang teridentifikasi pada DF4 tentang adanya hidden IT spending dan biaya TI yang dinilai terlalu tinggi. Logical Attacks memperoleh rating 20 (dampak 4 dikalikan kemungkinan 5), menunjukkan bahwa ancaman siber seperti hacking dan malware sangat mungkin terjadi dan berpotensi menimbulkan kerusakan signifikan terhadap data akademik dan data kesehatan yang dikelola institusi.

Tabel 2. Profil risiko TI Poltekkes Kemenkes Bengkulu berdasarkan design factor 3

Kategori risiko TI	Impact	Likelihood	Rating	Level	Objectives terdampak
IT Cost & Oversight	5	5	25	Very High	APO06, BAI10, MEA01
Logical Attacks (Hacking/Malware)	4	5	20	Very High	APO13, DSS05
IT Investment Decision Making	4	4	16	Very High	EDM02, APO05
Unauthorized Actions	3	3	9	High	DSS05, APO13
Program & Projects Life Cycle Mgmt	1	1	1	Normal	BAI01, BAI11
IT Expertise, Skills & Behavior	1	1	1	Normal	APO07

Sumber: Hasil pengolahan data peneliti, 2026

Analisis design factor 4: IT-related issues

Pada DF4, dari 20 isu TI yang dievaluasi, tiga isu mendapatkan nilai Serious Issue (3), yaitu significant IT-related incidents berupa kehilangan data dan kegagalan sistem, substantial hidden and rogue IT spending berupa pengeluaran TI tersembunyi di luar kendali anggaran resmi, dan excessively high cost of IT berupa biaya TI yang dinilai terlalu tinggi. Temuan ini konsisten dengan profil risiko pada DF3 dan memperkuat urgensi penguatan objectives terkait konfigurasi, keamanan, dan pengelolaan anggaran TI.

Analisis design factors 5 sampai 10

Threat Landscape (DF5) dinilai High, memperkuat prioritas objectives keamanan informasi. Compliance Requirements (DF6) dinilai High karena adanya regulasi dari Kementerian Kesehatan RI yang harus dipenuhi, termasuk instruksi perubahan sistem TI dari pusat yang secara langsung meningkatkan prioritas BAI06 – Managed IT Changes. Role of IT (DF7) saat ini berada pada posisi Support dengan nilai 1, mengindikasikan bahwa TI belum berperan strategis dalam transformasi organisasi. Sourcing Model (DF8) mencatat proporsi outsourcing sebesar 0,3 yang mendorong prioritas APO10 – Managed Vendors. IT Implementation Methods (DF9) dengan pendekatan Agile sebesar 0,5 mendorong prioritas BAI02 dan BAI03. Technology Adoption Strategy (DF10) dengan kecenderungan First Mover sebesar 0,75 memperkuat prioritas pada objectives inovasi dan adaptasi teknologi.

Prioritas governance and management objectives

Berdasarkan agregasi seluruh sepuluh Design Factors, diperoleh prioritas dan target capability level untuk setiap governance and management objectives. Tujuh belas objectives dengan prioritas Kritis (target level 4) dan Penting (target level 3) ditunjukkan pada Tabel 3.

Skor setiap objective pada Tabel 3 tidak berdiri sendiri, melainkan merupakan hasil agregasi pengaruh dari Design Factors yang relevan, sehingga setiap skor dapat dijelaskan sumber pendorongnya. Pada kelompok prioritas Kritis, BAI10 – Managed Configuration memperoleh skor tertinggi (100) karena ditarik sekaligus oleh dua risiko Very High pada DF3, yaitu IT Cost & Oversight (25) dan Logical Attacks (20); tanpa pengelolaan konfigurasi yang baik, aset TI tidak dapat diawasi biayanya maupun diamankan dari serangan. APO13 – Managed Security memperoleh skor 90 sebagai hasil agregasi tertimbang (weighted aggregation) pada sheet Canvas COBIT 2019 Design Toolkit, yang menjumlahkan kontribusi setiap Design Factor terhadap tiap objective sesuai bobot baku yang ditetapkan ISACA [14]. Pada APO13, tiga Design Factor memberi kontribusi positif secara konsisten: (1) DF3 – Risk Profile, di mana kategori Logical Attacks memperoleh rating Very High (20) sehingga menaikkan skor seluruh objective yang beririsan dengannya, termasuk APO13 dan DSS05; (2) DF5 – Threat Landscape yang dinilai High

menaikkan skor objective-objective terkait keamanan informasi secara langsung; dan (3) DF6 – Compliance Requirements yang juga dinilai High turut menambah skor APO13 karena kepatuhan terhadap regulasi Kementerian Kesehatan RI mensyaratkan pengelolaan keamanan informasi yang terstruktur. Akumulasi ketiga kontribusi tersebut pada Canvas menghasilkan skor akhir 90, menjadikan APO13 sebagai objective dengan skor tertinggi kedua setelah BAI10. Rincian nilai kontribusi per Design Factor sebagaimana tercatat pada Canvas Workbook COBIT 2019 dapat dilihat pada Lampiran. APO12 – Managed Risk memperoleh skor 85 karena seluruh risiko bernilai tinggi pada DF3 menuntut adanya proses manajemen risiko TI yang formal sebagai fondasi pengendaliannya. APO10 – Managed Vendors juga memperoleh skor 85, terutama dipicu oleh sourcing model pada DF8 yang menunjukkan 30% layanan TI dikelola pihak ketiga sehingga ketergantungan kepada vendor harus dikendalikan secara kontraktual.

Tabel 3. Prioritas governance and management objectives COBIT 2019 di Poltekkes Kemenkes Bengkulu

No	Kode	Governance/management objective	Skor	Target level	Prioritas
1	BAI10	Managed Configuration	100	4	Kritis
2	APO13	Managed Security	90	4	Kritis
3	APO12	Managed Risk	85	4	Kritis
4	APO10	Managed Vendors	85	4	Kritis
5	APO09	Managed Service Agreements	80	4	Kritis
6	EDM01	Ensured Governance Framework Setting & Maintenance	80	4	Kritis
7	DSS04	Managed Continuity	80	4	Kritis
8	MEA01	Managed Performance & Conformance Monitoring	75	4	Kritis
9	BAI06	Managed IT Changes	75*	4	Kritis
10	BAI02	Managed Requirements Definition	70	3	Penting
11	BAI03	Managed Solutions Identification & Build	70	3	Penting
12	EDM05	Ensured Stakeholder Engagement	65	3	Penting
13	DSS05	Managed Security Services	65	3	Penting
14	APO06	Managed Budget & Costs	60	3	Penting
15	APO01	Managed I&T Management Framework	60	3	Penting
16	DSS02	Managed Service Requests & Incidents	60	3	Penting
17	EDM04	Ensured Resource Optimization	60	3	Penting

Keterangan: *BAI06 mendapat penyesuaian prioritas karena adanya instruksi perubahan sistem TI dari Kementerian Kesehatan RI

Sumber: Hasil pengolahan data peneliti, 2026

APO09 – Managed Service Agreements dan DSS04 – Managed Continuity masing-masing memperoleh skor 80 sebagai konsekuensi langsung dari strategi Client Service/Stability (DF1) dan enterprise goal layanan berorientasi pelanggan (DF2) yang menuntut kepastian tingkat layanan dan keberlangsungan layanan digital bagi mahasiswa. EDM01 – Ensured Governance Framework Setting & Maintenance memperoleh skor 80 karena belum adanya kerangka tata kelola TI formal di institusi, padahal seluruh objective lain membutuhkan kerangka tersebut sebagai payung. MEA01 – Managed Performance & Conformance Monitoring memperoleh skor

75 yang bersumber dari risiko IT Cost & Oversight pada DF3, karena lemahnya pemantauan kinerja dan kepatuhan menjadi akar dari pengeluaran TI yang tidak terkendali. Adapun BAI06 – Managed IT Changes memperoleh skor 75 setelah penyesuaian manual, karena adanya instruksi perubahan sistem TI dari Kementerian Kesehatan RI (DF6) yang mengharuskan perubahan TI dikelola secara terkendali.

Pada kelompok prioritas Penting, BAI02 – Managed Requirements Definition dan BAI03 – Managed Solutions Identification & Build masing-masing memperoleh skor 70 yang bersumber dari metode implementasi Agile (DF9) dan kecenderungan First Mover (DF10), karena adopsi teknologi yang cepat menuntut kedisiplinan dalam pendefinisian kebutuhan dan pembangunan solusi. EDM05 – Ensured Stakeholder Engagement memperoleh skor 65 karena peran TI yang masih bersifat Support (DF7) mencerminkan rendahnya keterlibatan pimpinan dalam tata kelola TI, namun belum menjadi risiko langsung sebesar faktor keamanan dan biaya. DSS05 – Managed Security Services memperoleh skor 65 sebagai pasangan operasional dari APO13; skornya lebih rendah karena DSS05 berfokus pada pelaksanaan teknis harian, sedangkan pendorong utama dari Design Factors mengarah pada kebutuhan kebijakan dan manajemen keamanan di tingkat APO13 terlebih dahulu. APO06 – Managed Budget & Costs dan EDM04 – Ensured Resource Optimization masing-masing memperoleh skor 60 sebagai turunan dari strategi Cost Leadership (DF1) serta isu hidden IT spending dan biaya TI yang tinggi (DF4); skornya tidak lebih tinggi karena sebagian besar tekanan risiko biaya telah terdistribusi ke BAI10 dan MEA01. APO01 – Managed I&T Management Framework memperoleh skor 60 karena diperlukan sebagai pelengkap EDM01 di tataran manajemen, sementara DSS02 – Managed Service Requests & Incidents memperoleh skor 60 yang bersumber dari isu insiden TI signifikan pada DF4 serta tuntutan layanan berorientasi pelanggan pada DF2. Pola skor tersebut menunjukkan bahwa keluaran Governance System Design Workflow bersifat dapat ditelusuri (traceable), yaitu setiap prioritas dapat dijelaskan kembali ke Design Factors yang menjadi pendorongnya [11], [14].

Pembahasan

Tingginya prioritas BAI10 – Managed Configuration dengan skor 100 merupakan konsekuensi langsung dari profil risiko yang tinggi pada IT Cost & Oversight dan Logical Attacks. Pengelolaan konfigurasi yang baik akan memberikan visibilitas menyeluruh atas aset TI yang dimiliki institusi sehingga setiap pengeluaran TI dapat dipertanggungjawabkan dan setiap perubahan konfigurasi dapat dilacak. Temuan ini sejalan dengan hasil evaluasi pada organisasi pendidikan dan layanan publik yang menunjukkan bahwa kelemahan pengelolaan konfigurasi dan aset TI merupakan salah satu penyebab utama rendahnya kapabilitas tata kelola TI [16], [20].

APO13 – Managed Security memperoleh skor 90 yang didorong oleh tingginya ancaman logical attacks serta threat landscape yang berada pada kategori tinggi. Kebutuhan akan kebijakan dan prosedur keamanan informasi yang komprehensif menjadi sangat mendesak mengingat Poltekkes Kemenkes Bengkulu mengelola data sensitif mahasiswa dan data kesehatan yang tunduk pada regulasi perlindungan data. Absennya kebijakan keamanan informasi formal akan meningkatkan eksposur institusi terhadap risiko kebocoran data dan gangguan layanan digital, sebagaimana ditemukan pada evaluasi keamanan sistem informasi di fasilitas layanan kesehatan [3], [4]. Dalam COBIT 2019, APO13 dijabarkan ke dalam tiga praktik utama, yaitu membangun dan memelihara sistem manajemen keamanan informasi (ISMS), mendefinisikan dan mengelola rencana penanganan risiko keamanan informasi, serta memantau dan mengkaji ISMS secara berkala [13]. Praktik-praktik tersebut selaras dengan persyaratan sistem manajemen keamanan informasi pada ISO/IEC 27001:2022 [5], [6], sehingga implementasi APO13 dapat sekaligus menjadi jalan menuju kesesuaian dengan standar internasional tersebut. Selain itu, praktik information security management dalam kerangka manajemen layanan TI dapat dimanfaatkan institusi untuk mengintegrasikan pengamanan informasi ke dalam pengelolaan layanan TI sehari-hari [9].

Perbandingan dengan penelitian terdahulu memperlihatkan perbedaan pendekatan yang penting. Studi-studi sebelumnya umumnya menetapkan domain keamanan seperti APO13 dan DSS05 sebagai objek evaluasi sejak awal kemudian mengukur capability level-nya [8], [21], [22].

Penelitian ini menempuh urutan yang berbeda, yaitu menurunkan prioritas objective terlebih dahulu dari kondisi kontekstual institusi melalui sepuluh Design Factors, sehingga posisi APO13 sebagai prioritas kedua tertinggi merupakan temuan yang dihasilkan analisis, bukan asumsi awal. Pendekatan berbasis Design Factors semacam ini juga terbukti menghasilkan desain tata kelola yang lebih sesuai dengan karakteristik organisasi pada konteks organisasi publik maupun institusi pendidikan tinggi [11], [15].

Posisi TI sebagai Support menunjukkan bahwa institusi belum sepenuhnya memanfaatkan TI sebagai strategic enabler. Kondisi ini juga mencerminkan rendahnya keterlibatan pimpinan dalam tata kelola TI yang terlihat dari skor EDM05 – Ensured Stakeholder Engagement yang berada pada kelompok Penting. Keberhasilan tata kelola TI sangat dipengaruhi oleh keterlibatan pimpinan dan keselarasan strategi organisasi dengan teknologi informasi [10], [17]. Oleh karena itu, peningkatan peran TI menuju posisi yang lebih strategis memerlukan perubahan budaya organisasi serta komitmen manajemen sebagai prasyarat utama keberhasilan implementasi tata kelola TI.

Selain itu, penyesuaian manual pada BAI09 – Managed Assets sebesar –100 dengan alasan telah dilaksanakan pada periode sebelumnya menunjukkan bahwa beberapa praktik tata kelola TI sebenarnya telah berjalan pada aspek tertentu. Hal ini memperlihatkan bahwa analisis Design Factors COBIT 2019 tidak hanya menghasilkan prioritas pengembangan baru, tetapi juga mampu mengidentifikasi capaian tata kelola yang telah dimiliki organisasi sehingga sumber daya institusi dapat dialokasikan secara lebih efektif dan efisien. Pendekatan ini sesuai dengan konsep COBIT 2019 yang menekankan pentingnya penyesuaian tata kelola TI berdasarkan konteks dan kebutuhan organisasi [14], [19].

4. KESIMPULAN

Penelitian ini telah merancang sistem tata kelola TI dan menentukan prioritas governance and management objectives beserta target capability level-nya di Poltekkes Kemenkes Bengkulu melalui analisis sepuluh Design Factors COBIT 2019, dengan APO13 – Managed Security sebagai objective fokus studi kasus. Strategi institusi yang berorientasi pada Cost Leadership dan Client Service/Stability secara konsisten memengaruhi prioritas objectives di seluruh domain COBIT 2019, terutama yang berkaitan dengan efisiensi biaya dan kualitas layanan TI. Profil risiko TI institusi didominasi oleh tiga risiko sangat tinggi, yaitu IT Cost & Oversight dengan rating 25, Logical Attacks dengan rating 20, dan IT Investment Decision Making dengan rating 16, yang menjadi pendorong utama tingginya prioritas objectives keamanan dan konfigurasi.

Dari 40 governance and management objectives COBIT 2019, terdapat sembilan objectives dengan target capability level 4 dengan kategori Kritis yang perlu menjadi prioritas utama penguatan tata kelola, dipimpin oleh BAI10, APO13, dan APO12. APO13 – Managed Security menempati posisi prioritas kedua tertinggi dengan skor 90 dan target capability level 4, didorong secara konsisten oleh risiko logical attacks, threat landscape yang tinggi, dan kebutuhan kepatuhan terhadap regulasi Kementerian Kesehatan RI. Berdasarkan temuan tersebut, disusun tiga rekomendasi operasional yang selaras dengan praktik APO13 dalam COBIT 2019 [13]. Pertama, pada praktik APO13.01 (Establish and Maintain an ISMS), institusi perlu menyusun dan mengesahkan kebijakan keamanan informasi formal yang mencakup klasifikasi data akademik dan data kesehatan, ditetapkan oleh pimpinan dalam periode maksimal enam bulan ke depan. Kedua, pada praktik APO13.02 (Define and Manage an Information Security Risk Treatment Plan), Unit Teknologi Informasi dan Komunikasi perlu membentuk prosedur manajemen insiden keamanan yang mencakup mekanisme pelaporan, eskalasi, dan pemulihan insiden logical attacks, dilengkapi uji simulasi (tabletop exercise) minimal satu kali per tahun. Ketiga, pada praktik APO13.03 (Monitor and Review the ISMS), institusi perlu menerapkan kontrol akses berbasis peran (role-based access control) pada SIAKAD, Sistem Informasi Keuangan, dan Sistem Informasi Kepegawaian, disertai audit akses berkala setiap semester oleh Kepala Unit TIK bersama Kepala Bagian Keuangan. Ketiga langkah ini menjadi prioritas untuk meningkatkan kualitas layanan teknologi informasi institusi dan sekaligus menjadi dasar pengukuran capability level aktual pada penelitian lanjutan.

Penelitian ini memberikan kontribusi berupa metode perancangan sistem tata kelola dan prioritas objective keamanan informasi berbasis COBIT 2019 Design Factors yang dapat diadopsi oleh institusi pendidikan tinggi kesehatan sejenis untuk menentukan prioritas tata kelola TI secara kontekstual dan berbasis bukti. Keterbatasan penelitian ini terletak pada cakupannya yang berhenti pada penentuan prioritas dan target capability level, sehingga belum mengukur capability level aktual maupun gap antara kondisi saat ini dan target yang ditetapkan. Pengukuran capability level aktual dan analisis gap tersebut direncanakan menjadi agenda penelitian lanjutan pada tahap tesis penulis.

5. SARAN

Penelitian selanjutnya disarankan untuk melakukan asesmen capability level aktual menggunakan COBIT 2019 Performance Management dan COBIT 2019 Assessment Program, sehingga gap antara kondisi saat ini dan target capability level yang telah ditetapkan dapat diukur secara kuantitatif. Selain itu, penelitian lanjutan dapat memperluas objek penelitian ke beberapa Poltekkes Kemenkes lain agar diperoleh gambaran komparatif mengenai kondisi tata kelola keamanan informasi pada institusi pendidikan tinggi kesehatan di Indonesia.

6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Direktur beserta jajaran pimpinan dan staf Unit Teknologi Informasi dan Komunikasi Poltekkes Kemenkes Bengkulu atas izin, data, dan waktu yang diberikan selama pelaksanaan penelitian ini.

DAFTAR PUSTAKA

- [1] M. A. Saputra and M. R. Redo, "Penerapan framework COBIT 2019 untuk perancangan tata kelola teknologi informasi pada perguruan tinggi," *J. Sci. Soc. Res.*, vol. 4, no. 3, pp. 352–358, 2021, doi: 10.54314/jssr.v4i3.715.
- [2] A. S. Sukanto, H. Novriando, and A. Reynaldi, "Tata kelola teknologi informasi menggunakan framework COBIT 2019 (studi kasus: UPT TIK Universitas Tanjungpura Pontianak)," *JEPIN (J. Edukasi dan Penelit. Inform.)*, vol. 7, no. 2, pp. 214–220, 2021, doi: 10.26418/jp.v7i2.47859.
- [3] M. A. Algiffary, M. I. Herdiansyah, and Y. N. Kunang, "Audit keamanan sistem informasi manajemen rumah sakit dengan framework COBIT 2019 pada RSUD Palembang BARI," *J. Appl. Comput. Sci. Technol.*, vol. 4, no. 1, pp. 19–26, 2023, doi: 10.52158/jacost.v4i1.505.
- [4] R. Moryanda, "Evaluasi sistem informasi manajemen rumah sakit menggunakan framework COBIT 2019 (studi kasus: Semen Padang Hospital)," *J. Nas. Teknol. dan Sist. Inf.*, vol. 9, no. 3, pp. 299–306, 2023, doi: 10.25077/TEKNOSI.v9i3.2023.299-306.
- [5] International Organization for Standardization, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. Geneva, Switzerland: ISO/IEC, 2022.
- [6] R. Sinaga, "Pengembangan model penilaian kepatuhan salah satu perguruan tinggi terhadap standar ISO 27001:2022," *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 3, pp. 381–394, 2024, doi: 10.28932/jutisi.v9i3.6850.
- [7] H. M. Melaku, "A dynamic and adaptive cybersecurity governance framework," *J. Cybersecur. Priv.*, vol. 3, no. 3, pp. 327–350, 2023, doi: 10.3390/jcp3030017.
- [8] R. Setyadi and A. A. Rahman, "Enhancing IT governance based on risk and security analysis in a private school: a COBIT 2019 approach," *JOIV Int. J. Informatics Vis.*, vol. 9, no. 5, pp. 2148–2156, 2025, doi: 10.62527/joiv.9.5.3414.
- [9] D. Herlinudinkhaji and L. K. Ramadhani, "Tata kelola layanan teknologi informasi dengan ITIL V4 untuk estimasi layanan," *REMIK Ris. dan E-Jurnal Manaj. Inform. Komput.*,

- vol. 7, no. 1, pp. 452–457, 2023, doi: 10.33395/remik.v7i1.12058.
- [10] Y. Darmi, S. Fernandez, M. Y. Fathoni, and S. Wijayanto, “Evaluation of governance in information systems security to minimize information technology risks,” *INTENSIF J. Ilm. Penelit. dan Penerap. Tek. Sist. Inf.*, vol. 8, no. 1, pp. 41–52, 2024, doi: 10.29407/intensif.v8i1.21221.
 - [11] M. R. Katili, L. N. Amali, and S. Suhada, “Design factors in evaluating and formulating IT governance systems in public organizations,” *J. RESTI (Rekayasa Sist. dan Teknol. Inf.)*, vol. 7, no. 5, pp. 1182–1191, 2023, doi: 10.29207/resti.v7i5.4939.
 - [12] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg, IL, USA: ISACA, 2018.
 - [13] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL, USA: ISACA, 2018.
 - [14] ISACA, *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*. Schaumburg, IL, USA: ISACA, 2018.
 - [15] D. Utomo, M. Wijaya, Suzanna, Efendi, and N. T. M. Sagala, “Leveraging COBIT 2019 to implement IT governance in SME context: a case study of higher education in Campus A,” *CommIT J.*, vol. 16, no. 2, pp. 129–141, 2022, doi: 10.21512/commit.v16i2.8172.
 - [16] A. B. Sipayung, R. Yunis, and E. Elly, “Evaluation of information technology governance at Mikroskil University using COBIT 2019 framework with BAI11 domain,” *Int. J. Res. Appl. Technol.*, vol. 2, no. 2, pp. 128–143, 2022, doi: 10.34010/injuratech.v2i2.8085.
 - [17] D. Darmawan and A. F. Wijaya, “Analisis dan desain tata kelola teknologi informasi menggunakan framework COBIT 2019 pada PT XYZ,” *J. Comput. Inf. Syst. Ampera*, vol. 3, no. 1, pp. 1–17, 2022, doi: 10.51519/journalcisa.v3i1.139.
 - [18] E. Wulandari, L. H. Atrinawati, and M. G. L. Putra, “Perancangan tata kelola teknologi informasi dengan menggunakan framework COBIT 2019 pada PT XYZ Balikpapan,” *DoubleClick J. Comput. Inf. Technol.*, vol. 5, no. 2, pp. 96–104, 2022, doi: 10.25273/doubleclick.v5i2.10067.
 - [19] A. Zai, A. H. Muhammad, and A. Nasiri, “Tinjauan literatur audit teknologi informasi pada COBIT 2019 fokus domain APO14,” *JINTEKS (J. Inform. Teknol. dan Sains)*, vol. 5, no. 4, pp. 607–611, 2023, doi: 10.51401/jinteks.v5i4.3507.
 - [20] R. Prasetya, A. H. Muhammad, and A. Nasiri, “Perancangan model manajemen (tata kelola) data menggunakan domain APO14 COBIT 2019,” *JIP (J. Inform. Polinema)*, vol. 10, no. 3, pp. 389–396, 2024, doi: 10.33795/jip.v10i3.5135.
 - [21] R. N. Christiadi and R. Sutomo, “Measurement of IT security governance capabilities using COBIT 2019 at Indonesian business sector,” *G-Tech J. Teknol. Terap.*, vol. 7, no. 4, pp. 1498–1508, 2023, doi: 10.33379/gtech.v7i4.3170.
 - [22] A. Angelina and M. I. Fianty, “Capability level assessments of information security controls: an empirical analysis of practitioners assessment capabilities,” *G-Tech J. Teknol. Terap.*, vol. 8, no. 1, pp. 91–103, 2024, doi: 10.33379/gtech.v8i1.3509.