



IT Governance Design for PNUP Internet of Things Laboratory Using the COBIT 2019 Framework

Perancangan Tata Kelola TI Laboratorium Internet of Things PNUP Menggunakan Kerangka COBIT 2019

Amhar Davi Dewantara^{1*}, Iin Karmila Yusri², Budy Santoso³

^{1,2,3}Program Studi Teknik Komputer dan Jaringan, Jurusan Teknik Informatika dan Komputer,
Politeknik Negeri Ujung Pandang, Indonesia

E-Mail: ¹amhardavi@poliupg.ac.id, ²iin.yusri@poliupg.ac.id, ³budysantoso@poliupg.ac.id

Received Mar 09th 2026; Revised Apr 16th 2026; Accepted Apr 22th 2026; Available Online Apr 28th 2026

Corresponding Author: Amhar Davi Dewantara

Copyright © 2026 by Authors, Published by Institut Riset dan Publikasi Indonesia (IRPI)

Abstract

The IoT Laboratory of the Department of Informatics and Computer Engineering at Politeknik Negeri Ujung Pandang (Lab IoT PNUP) serves as both a student practicum facility and a faculty research center. Although standard operating procedures (SOPs) exist at the departmental level, they have not been formally implemented at the laboratory level, leading to inadequate asset documentation, unrecorded equipment borrowing, and weak access controls. This study designs an IT governance system for Lab Internet of Things (IoT) PNUP using the COBIT 2019 framework, guided by the four-stage Governance System Design Workflow. Eleven design factors were analyzed using the COBIT 2019 Design Toolkit to identify seven priority governance objectives: EDM03, APO12, APO13, MEA03, DSS05, DSS04, and DSS06. Capability assessment based on questionnaires from four respondents shows that all domains remain at Capability Level 1, with gaps ranging from +2 to +3 levels. Given the laboratory's small-enterprise scale, a phased improvement roadmap is proposed: short-term (0–6 months) for process formalization, medium-term (6–18 months) for strengthening security and compliance, and long-term (18–36 months) for institutionalizing risk governance. This roadmap provides a structured and prioritized approach to improving IT governance maturity at Lab IoT PNUP.

Keywords: *Capability Level, COBIT 2019, Design Factors, Internet of Things Laboratory, IT Governance.*

Abstrak

Laboratorium Internet of Things, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Ujung Pandang (Lab IoT PNUP) menjalankan fungsi ganda sebagai sarana praktikum mahasiswa sekaligus pusat riset dosen. Meskipun Standar Operasional Prosedur (SOP) institusional telah tersedia di tingkat jurusan, SOP tersebut belum diadopsi secara formal di tingkat operasional laboratorium, sehingga menimbulkan permasalahan berupa dokumentasi inventaris yang tidak memadai, pencatatan peminjaman perangkat yang tidak konsisten, serta kontrol akses yang lemah. Penelitian ini merancang sistem tata kelola TI untuk Lab Internet of Things (IoT) PNUP menggunakan kerangka kerja COBIT 2019, dengan mengikuti empat tahap Governance System Design Workflow. Sebelas design factor dianalisis menggunakan COBIT 2019 Design Toolkit untuk mengidentifikasi tujuh objektif tata kelola prioritas: EDM03, APO12, APO13, MEA03, DSS05, DSS04, dan DSS06. Pengukuran kapabilitas melalui kuesioner yang diisi oleh empat responden menunjukkan bahwa seluruh domain berada pada Capability Level 1, dengan kesenjangan +2 hingga +3 level terhadap target masing-masing. Mempertimbangkan skala Lab IoT PNUP sebagai organisasi kecil, diusulkan peta jalan perbaikan bertahap dalam tiga fase: jangka pendek (0–6 bulan) berfokus pada formalisasi proses, jangka menengah (6–18 bulan) memperkuat keamanan dan kepatuhan, serta jangka panjang (18–36 bulan) menginstitutionalisasi tata kelola risiko, sebagai panduan aksi terstruktur peningkatan kematangan tata kelola TI Lab IoT PNUP.

Kata Kunci: COBIT 2019, Design Factors, Laboratorium Internet of Things, Tata Kelola TI, Tingkat Kapabilitas

1. PENDAHULUAN

Laboratorium merupakan infrastruktur akademik yang menopang Tridharma Perguruan Tinggi, berfungsi sebagai ruang praktikum sekaligus tulang punggung riset dosen dan mahasiswa [1]. Permendikbud

Nomor 3 Tahun 2020 menegaskan posisinya sebagai bagian dari standar sarana-prasarana wajib [2], sementara BAN-PT menjadikan kualitas pengelolaannya sebagai salah satu indikator akreditasi [3]. Peraturan Menteri Pendidikan Tinggi, Sains, dan Teknologi Nomor 39 Tahun 2025 tentang Penjaminan Mutu Pendidikan Tinggi mempertegas bahwa pengelolaan fasilitas laboratorium merupakan bagian integral dari sistem penjaminan mutu institusi [4].

Laboratorium berbasis *Internet of Things* (IoT) menghadirkan kompleksitas yang lebih tinggi dibandingkan laboratorium konvensional, terutama karena integrasi perangkat fisik melalui jaringan internet untuk pertukaran data otomatis [5]. Infrastruktur ini membentuk ekosistem yang saling bergantung antara perangkat keras, perangkat lunak, jaringan, dan data [6]. Sabran et al. [7] menekankan bahwa pengelolaan laboratorium IoT memerlukan prosedur operasional terencana, mulai dari kontrol akses hingga pengelolaan aset secara *real-time*, mengingat setiap perangkat berpotensi menjadi titik kerentanan yang membutuhkan pengawasan terstruktur [8].

Laboratorium *Internet of Things* (IoT), Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Ujung Pandang (Lab IoT PNUP) menjalankan fungsi ganda sebagai sarana praktikum mahasiswa sekaligus pusat riset dosen. Berdasarkan observasi dan wawancara dengan kepala laboratorium, pengelolaan TI di laboratorium ini belum terstandar secara optimal. PNUP sesungguhnya telah memiliki SOP institusional di tingkat jurusan dan regulasi Tata Usaha Barang Milik Negara (BMN) yang mengatur pemeliharaan hingga pelaporan aset, namun SOP tersebut belum diadopsi di tingkat operasional laboratorium. Kondisi ini berdampak pada dokumentasi inventaris yang tidak memadai, ketiadaan mekanisme pencatatan peminjaman, serta kontrol akses yang lemah, sehingga akuntabilitas aset laboratorium menjadi rentan.

Kondisi tersebut memerlukan implementasi tata kelola TI yang sistematis. Tata kelola TI berfungsi sebagai kerangka pengambilan keputusan yang akuntabel agar pemanfaatan teknologi informasi selaras dengan visi dan strategi organisasi [9, 10, 11]. COBIT 2019 dipilih sebagai kerangka kerja utama karena fleksibilitasnya yang relevan bagi organisasi skala kecil hingga entitas besar [12], menyediakan skala *capability level* 0–5 yang terstandarisasi [13], serta mekanisme *design factors* dengan perangkat pengukuran bawaan untuk pemilihan proses secara kontekstual sesuai kebutuhan spesifik laboratorium [14].

Beberapa penelitian terdahulu telah mengkaji relevansi COBIT dalam tata kelola laboratorium pendidikan. Studi oleh Adikara [15], Afni et al. [16], dan Rosyidah & Kurniawati [17] menerapkan COBIT 5 pada skala universitas, namun temuan mereka cenderung generik karena belum mengintegrasikan mekanisme *design factors* dan tidak menyoroti unit laboratorium secara spesifik. Nasution [18] merekomendasikan model desentralistik berbasis penjaminan mutu internal untuk Laboratorium Terpadu UIN Sunan Kalijaga, namun tidak mengukur kapabilitas menggunakan standar yang terstandarisasi. Afdhani dan Soewito [19], Sopacua dan Haryani [20] serta Rasmila et al. [21] membuktikan bahwa penggunaan *design factors* COBIT 2019 mampu meningkatkan relevansi rekomendasi, namun penerapannya terbatas pada institusi pemerintahan dan organisasi umum, bukan pada laboratorium berbasis IoT dalam konteks pendidikan tinggi vokasi yang memiliki profil risiko dan skala organisasi yang berbeda. Hingga saat ini, belum tersedia kajian yang secara khusus mengintegrasikan mekanisme *design factors* COBIT 2019 untuk menghasilkan peta jalan implementasi yang konkret bagi laboratorium IoT di perguruan tinggi vokasi.

Berdasarkan penelusuran literatur tersebut, penelitian ini hadir untuk mengisi celah tersebut dengan tiga kontribusi yang membedakannya dari studi sebelumnya: (1) menggunakan COBIT 2019 dengan mekanisme *design factors* yang kontekstual sesuai karakteristik laboratorium IoT; (2) menyoroti unit laboratorium spesifik berbasis IoT dalam ekosistem pendidikan tinggi vokasi, bukan institusi secara umum; dan (3) menghasilkan peta jalan implementasi bertahap (*phased roadmap*) yang terukur dan langsung dapat dioperasionalkan, dengan mempertimbangkan keterbatasan skala *small enterprise*. Secara operasional, penelitian ini mengukur tingkat kapabilitas (*capability level*) kondisi saat ini (*as-is*) pada Lab IoT PNUP, mengidentifikasi kesenjangan (*gap*) terhadap target yang diharapkan (*to-be*), serta merancang rekomendasi strategis menggunakan COBIT 2019 Design Toolkit sebagai acuan operasional yang konkret.

2. METODOLOGI PENELITIAN

Penelitian ini dirancang menggunakan pendekatan kualitatif deskriptif dengan studi kasus tunggal pada Lab IoT PNUP. Data primer dikumpulkan melalui observasi langsung dan wawancara mendalam, sementara data sekunder diperoleh melalui studi literatur untuk mendukung analisis kontekstual. Secara prosedural, penelitian ini mengadopsi empat tahap *Governance System Design Workflow* yang bersumber dari COBIT 2019 Design Guide [14]. Gambar 1 menunjukkan alur desain sistem tata kelola yang terdiri dari empat tahap berurutan: dimulai dari pemahaman konteks organisasi, penetapan ruang lingkup awal, penyempurnaan ruang lingkup, hingga pengambilan keputusan akhir desain sistem tata kelola.

2.1. Tinjauan Literatur

COBIT 2019 merupakan kerangka kerja tata kelola TI yang dikembangkan oleh ISACA sebagai pembaruan dari COBIT 5, dengan penyempurnaan utama berupa penambahan mekanisme *design factors* dan *focus areas* yang memungkinkan organisasi merancang sistem tata kelola secara kontekstual sesuai

karakteristik spesifiknya [12, 23]. Kerangka ini mendefinisikan 40 *governance and management objectives* yang terorganisasi dalam lima domain: EDM, APO, BAI, DSS, dan MEA [12]. Salah satu keunggulan COBIT 2019 dibandingkan versi sebelumnya adalah tersedianya *Design Toolkit* berbasis *spreadsheet* yang memfasilitasi kalkulasi skor kepentingan relatif setiap *objective* berdasarkan sebelas *design factors*, sehingga rekomendasi yang dihasilkan lebih relevan dan terukur [14]. Skala *capability level* 0–5 yang terstandardisasi dalam COBIT 2019 juga memungkinkan pengukuran kondisi *as-is* dan penetapan target *to-be* secara sistematis [13].



Gambar 1. *Governance System Design Workflow*

Sejumlah penelitian telah mengkaji penerapan kerangka COBIT dalam konteks tata kelola laboratorium di institusi pendidikan tinggi. Adikara [15] menerapkan COBIT 5 pada Laboratorium Rekayasa Perangkat Lunak Universitas Esa Unggul dan menemukan bahwa tata kelola TI laboratorium memerlukan pendekatan yang berbeda dari institusi secara keseluruhan. Afni et al. [16] menggunakan COBIT 5 untuk meningkatkan strategi tata kelola TI laboratorium di Universitas XYZ, sementara Rosyidah dan Kurniawati [17] mengukur *capability level* tata kelola IT di laboratorium Teknik Informatika menggunakan COBIT 5 dan menemukan kesenjangan signifikan antara kondisi aktual dengan target yang diharapkan. Meski demikian, ketiga studi tersebut menggunakan COBIT 5 yang belum dilengkapi dengan mekanisme *design factors*, sehingga rekomendasi yang dihasilkan cenderung generik dan kurang mencerminkan kebutuhan spesifik unit laboratorium yang diteliti.

Pemanfaatan mekanisme *design factors* COBIT 2019 telah dibuktikan dapat meningkatkan relevansi rekomendasi tata kelola dalam berbagai konteks organisasi. Afdhani dan Soewito [19] menerapkan COBIT 2019 dengan *design factors* pada Pusat Data dan Informasi Kementerian dan menghasilkan prioritas *objectives* yang lebih kontekstual dibandingkan dengan pendekatan generik. Sopacua dan Haryani [20] menerapkan COBIT 2019 pada evaluasi tata kelola TI di yayasan pendidikan, sedangkan Rasmila et al. [21] mendemonstrasikan efektivitas *design factors* COBIT 2019 dalam merancang tata kelola TI pada perusahaan skala kecil. Namun demikian, seluruh penelitian tersebut dilakukan pada lingkup organisasi pemerintahan, kementerian, atau perusahaan, bukan pada unit laboratorium berbasis IoT dalam ekosistem pendidikan tinggi vokasi yang memiliki profil risiko, skala organisasi, dan kompleksitas infrastruktur yang berbeda.

Laboratorium berbasis IoT menghadirkan tantangan tata kelola yang unik akibat integrasi perangkat fisik melalui jaringan internet untuk pertukaran data otomatis [5], membentuk ekosistem yang saling bergantung antara perangkat keras, perangkat lunak, jaringan, dan data [6]. Roman et al. [8] menegaskan bahwa setiap perangkat IoT berpotensi menjadi titik kerentanan yang membutuhkan pengawasan dan pengendalian terstruktur. Sabran et al. [7] menunjukkan bahwa pengelolaan laboratorium IoT memerlukan prosedur operasional terencana, mulai dari kontrol akses hingga pengelolaan aset secara *real-time*. Nasution [18] merekomendasikan model desentralistik berbasis penjaminan mutu internal untuk laboratorium terpadu, namun tidak mengukur kapabilitas menggunakan standar yang terstandardisasi dan tidak mempertimbangkan karakteristik infrastruktur IoT secara spesifik. Hingga saat ini, belum tersedia kajian yang secara khusus mengintegrasikan mekanisme *design factors* COBIT 2019 untuk menghasilkan peta jalan implementasi yang konkret bagi laboratorium IoT di perguruan tinggi vokasi.

Berdasarkan tinjauan literatur di atas, terdapat tiga celah penelitian yang belum terjawab. Pertama, studi-studi berbasis COBIT di laboratorium pendidikan [15][16][17] masih menggunakan COBIT 5 tanpa mekanisme *design factors*, sehingga rekomendasinya kurang kontekstual. Kedua, penelitian yang telah memanfaatkan *design factors* COBIT 2019 [19][20][21] tidak menyoroti laboratorium berbasis IoT dalam ekosistem pendidikan tinggi vokasi. Ketiga, belum ada penelitian yang menghasilkan peta jalan implementasi bertahap (*phased roadmap*) yang terukur dan langsung dapat dioperasionalkan untuk laboratorium IoT berskala kecil. Penelitian ini hadir untuk mengisi tiga penelitian yang belum terjawab melalui tiga kontribusi utama: (1) menerapkan mekanisme *design factors* COBIT 2019 secara penuh pada unit laboratorium IoT spesifik; (2) menghasilkan pengukuran *capability level* berbasis standar ISACA pada konteks pendidikan tinggi vokasi; dan (3) menyusun *phased roadmap* yang mempertimbangkan keterbatasan skala *small enterprise* sebagai panduan aksi yang langsung dapat dioperasionalkan.

2.2. Tahap 1: Memahami Konteks dan Strategi Organisasi (*Understand the Enterprise Context and Strategy*)

Tahap pertama bertujuan untuk membangun pemahaman menyeluruh tentang konteks organisasi sebelum merancang sistem tata kelola TI [12]. Menurut ISACA [12], pemahaman konteks organisasi

merupakan prasyarat utama agar desain sistem tata kelola tidak bersifat generik, melainkan relevan secara spesifik terhadap kebutuhan dan kondisi nyata organisasi. Pada tahap ini, data primer dikumpulkan melalui dua instrumen utama: (1) observasi langsung terhadap kondisi operasional Lab IoT PNUP, mencakup tata letak fisik, infrastruktur perangkat keras dan lunak, serta alur aktivitas harian laboratorium; dan (2) wawancara mendalam dengan kepala laboratorium untuk menggali permasalahan TI yang dihadapi, strategi pengelolaan yang berjalan, serta ekspektasi terhadap tata kelola yang ideal. Informasi yang diperoleh mencakup profil organisasi, visi dan misi laboratorium, struktur pengelolaan, serta permasalahan operasional yang menjadi latar belakang penelitian. Output dari tahap ini berupa gambaran komprehensif tentang kondisi as-is organisasi yang menjadi landasan bagi seluruh tahap analisis berikutnya [14].

2.3. Tahap 2: Penentuan Ruang Lingkup Awal Sistem Tata Kelola (*Determine the Initial Scope of the Governance System*)

Tahap kedua bertujuan menetapkan ruang lingkup awal sistem tata kelola melalui analisis *Design Factor* 1–4, yaitu variabel-variabel kontekstual yang secara langsung memengaruhi prioritas *governance and management objectives* dalam COBIT 2019 [12]. Keempat *design factor* yang dianalisis pada tahap ini adalah: (1) *Enterprise Strategy* (DF1), yang mengidentifikasi orientasi strategis organisasi dari empat pilihan yang tersedia, yaitu *Growth/Acquisition*, *Innovation/Differentiation*, *Cost Leadership*, dan *Client Service/Stability*; (2) *Enterprise Goals* (DF2), yang menilai sejauh mana 13 *enterprise goals* COBIT 2019 relevan bagi organisasi menggunakan skala *Not Important* hingga *Primary*; (3) *IT Risk Profile* (DF3), yang mengukur tingkat keparahan 19 kategori risiko TI berdasarkan kondisi aktual organisasi menggunakan skala 0–25; serta (4) *I&T Related Issues* (DF4), yang mengidentifikasi isu-isu TI yang sedang dihadapi organisasi dari daftar 24 permasalahan umum yang disediakan COBIT 2019 [14]. Data untuk keempat *design factor* ini diperoleh melalui wawancara mendalam bersama *stakeholder* kunci laboratorium. Hasil penilaian setiap *design factor* kemudian dimasukkan ke dalam COBIT 2019 Design Toolkit sebagai perangkat kalkulasi berbasis *spreadsheet* yang disediakan ISACA untuk menghasilkan skor kepentingan relatif awal bagi setiap *governance objective* [12].

2.4. Tahap 3: Penyempurnaan Ruang Lingkup Sistem Tata Kelola (*Refine the Scope of the Governance System*)

Tahap ketiga bertujuan menyempurnakan ruang lingkup yang telah ditetapkan pada Tahap 2 dengan mempertimbangkan tujuh *design factor* tambahan (DF5–DF11) yang bersifat lebih operasional dan kontekstual [12]. Ketujuh *design factor* tersebut adalah: (5) *Threat Landscape* (DF5), yang menilai tingkat ancaman eksternal yang dihadapi organisasi dalam skala *Normal*, *High*, atau *Very High*; (6) *Compliance Requirements* (DF6), yang menilai bobot persyaratan kepatuhan regulasi yang berlaku, mulai dari *Low* hingga *Very High*; (7) *Role of IT* (DF7), yang menentukan posisi strategis TI dalam organisasi dari empat peran: *Support*, *Factory*, *Turnaround*, dan *Strategic* dengan skala 1–5; (8) *IT Sourcing Model* (DF8), yang menggambarkan komposisi model pengadaan TI antara *Insourced*, *Outsourced*, dan *Cloud* dalam persentase total 100%; (9) *IT Implementation Methods* (DF9), yang mencerminkan metode implementasi TI yang dominan digunakan, yaitu *Traditional*, *Agile*, dan *DevOps*; (10) *Technology Adoption Strategy* (DF10), yang mengklasifikasikan posisi adopsi teknologi organisasi antara *First Mover*, *Follower*, dan *Slow Adopter*; serta (11) *Enterprise Size* (DF11), yang mengklasifikasikan skala organisasi antara *Small*, *Medium*, atau *Large Enterprise* [14]. Setiap *design factor* dinilai melalui wawancara dan dikonfirmasi melalui observasi, kemudian seluruh nilai diinputkan kembali ke dalam COBIT 2019 Design Toolkit untuk memperbarui dan mempertajam skor kepentingan relatif masing-masing *objective* [12].

2.5. Tahap 4: Menyimpulkan Rancangan Sistem Tata Kelola (*Resolve Conflicts and Conclude the Governance System Design*)

Tahap keempat merupakan tahap sintesis akhir yang bertujuan mengonsolidasikan seluruh hasil penilaian 11 *design factor* menjadi keputusan akhir tentang prioritas *governance and management objectives* yang akan menjadi fokus tata kelola [12, 24]. Pada tahap ini, COBIT 2019 Design Toolkit menghasilkan skor kepentingan relatif untuk setiap *objective* dalam skala -100 hingga +100, di mana skor positif menunjukkan tingkat relevansi dan urgensi yang lebih tinggi bagi organisasi [14]. Berdasarkan panduan ISACA [12], penetapan target *capability level* ditentukan berdasarkan besaran skor: *objective* dengan skor ≥ 75 ditetapkan memiliki target *Capability Level* 4, sementara skor 50–74 ditetapkan sebagai target *Capability Level* 3. Hanya *objective* dengan skor minimal 50 yang dimasukkan sebagai prioritas utama kajian ini. Apabila terdapat konflik antardesign factor, misalnya satu faktor mendorong prioritas tinggi sementara faktor lain menekan, maka resolusi dilakukan dengan mempertimbangkan relevansi kontekstual organisasi secara holistik [12]. Output akhir dari tahap ini berupa daftar *priority objectives* beserta target kapabilitas yang menjadi acuan pengukuran *capability level* dan penyusunan rekomendasi perbaikan pada tahap analisis selanjutnya.

3. HASIL DAN PEMBAHASAN

3.1. Melakukan pemetaan COBIT Core Model 2019

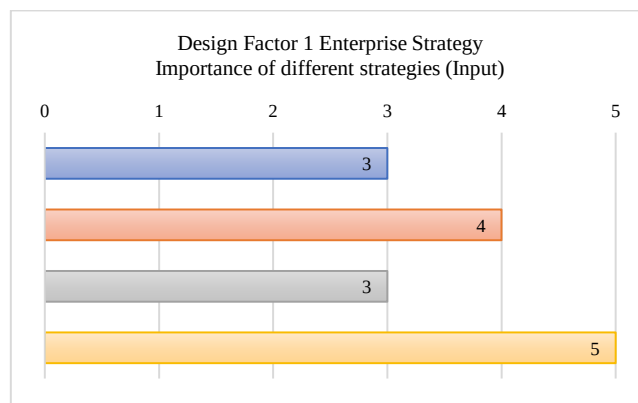
3.1.1 Tahap 1: Memahami Konteks dan Strategi Organisasi (*Understand the Enterprise Context and Strategy*)

Lab IoT PNUP berfungsi sebagai unit pelaksana teknis yang menyediakan layanan infrastruktur TI bagi praktikum mahasiswa dan riset dosen, dengan strategi berfokus pada pemenuhan layanan akademis dan inovasi berkelanjutan.

3.1.2 Tahap 2: Penentuan Ruang Lingkup Awal Sistem Tata Kelola (*Determine the Initial Scope of the Governance System*)

Lab IoT PNUP berfungsi sebagai unit pelaksana teknis yang menyediakan layanan infrastruktur TI bagi praktikum mahasiswa dan riset dosen, dengan strategi berfokus pada pemenuhan layanan akademis dan inovasi berkelanjutan.

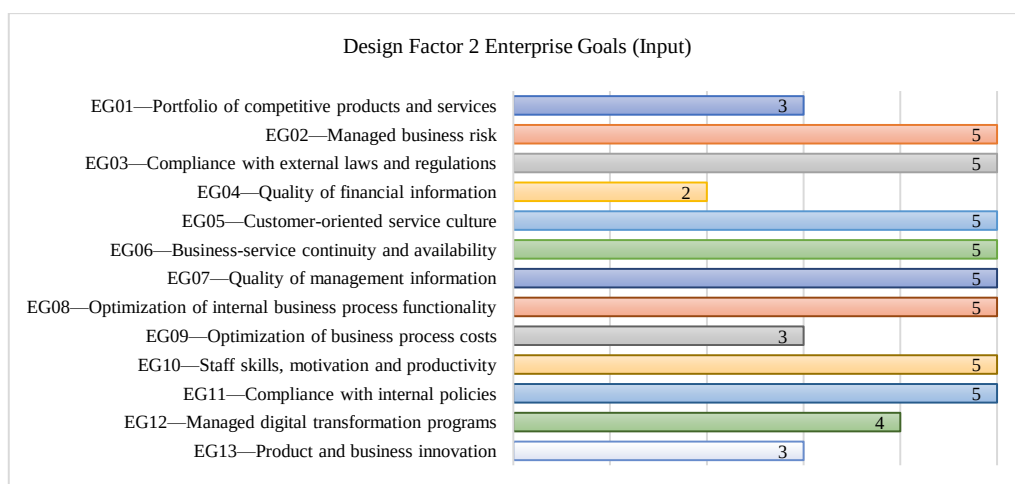
1. Design Factor 1: Enterprise Strategy



Gambar 2. Design Factor 1 - Enterprise Strategy

Gambar 2 merupakan hasil analisis strategi pada Lab IoT PNUP, dengan nilai *Client Service/Stability* tertinggi. Hal ini menunjukkan bahwa layanan Lab IoT PNUP berperan sangat kritis karena ketersediaan dan keandalan layanan laboratorium menjadi syarat mutlak bagi keberlangsungan praktikum mahasiswa. *Innovation/Differentiation* memiliki nilai empat mengingat fungsi laboratorium sebagai pusat riset dosen yang menuntut inovasi berkelanjutan dalam pemanfaatan teknologi IoT.

2. Design Factor 2 – Enterprise Goals (lihat Gambar 3)

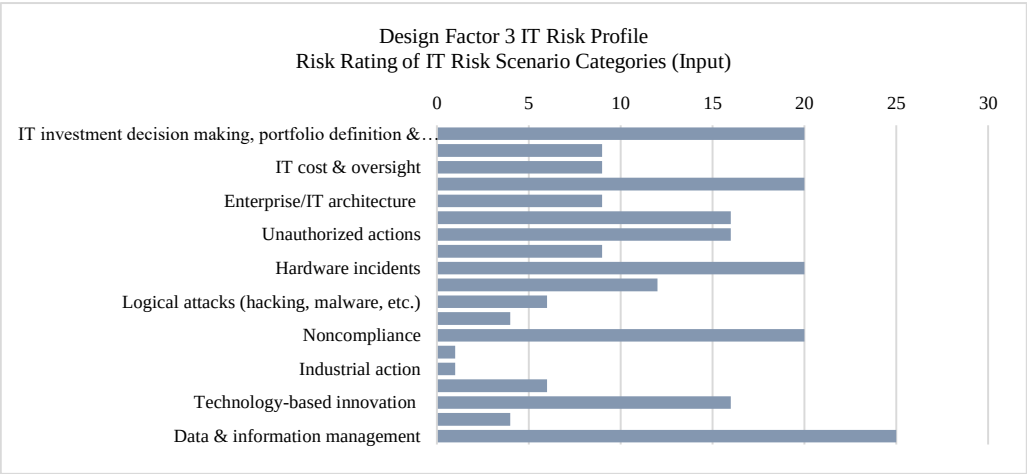


Gambar 3. Design Factor 2 – Enterprise Goals

Penilaian untuk Lab IoT PNUP menunjukkan bahwa delapan dari tiga belas *enterprise goals* mendapatkan nilai tertinggi (5), yaitu: pengelolaan risiko bisnis (EG02), kepatuhan terhadap regulasi eksternal (EG03), budaya layanan berorientasi pelanggan (EG05), keberlangsungan dan ketersediaan layanan (EG06), kualitas informasi manajemen (EG07), optimasi fungsionalitas proses internal (EG08), serta

keterampilan dan produktivitas staf (EG10) dan kepatuhan terhadap kebijakan internal (EG11). Konsentrasi nilai tinggi pada *goals* yang berkaitan dengan risiko, kepatuhan, dan kualitas layanan ini mencerminkan urgensi permasalahan tata kelola yang dihadapi laboratorium.

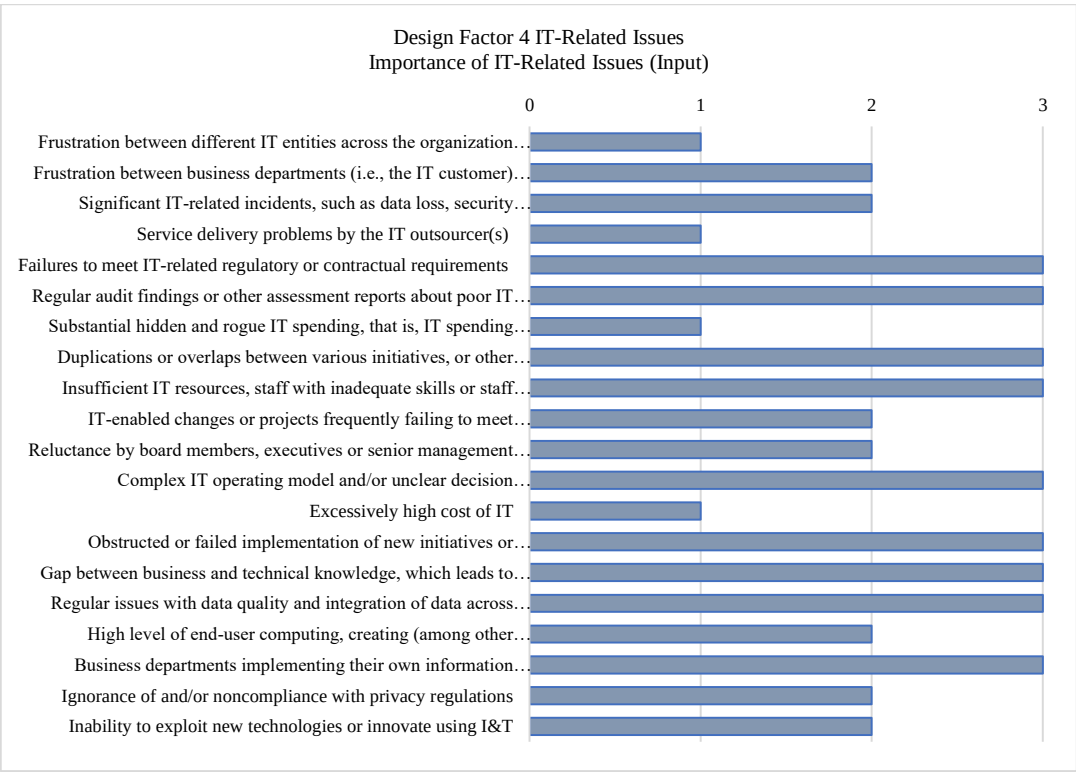
3. *Design Factor 3 – IT Risk Profile* (lihat Gambar 4)



Gambar 4. *Design Factor 3 – IT Risk Profile*

Profil risiko Lab IoT PNUP menunjukkan bahwa terdapat lima kategori dengan *risk rating* tertinggi yang masing-masing berada pada level kritis atau sangat tinggi. Risiko terkait pengelolaan data dan informasi (*Data & Information Management*) mencapai rating tertinggi (25), mengingat tidak adanya mekanisme pencatatan inventaris yang memadai. Menyusul empat kategori lain dengan rating 20, yaitu: *IT investment decision making* yang berkaitan dengan lemahnya basis data untuk pengambilan keputusan aset; *IT expertise, skills & behavior* yang mencerminkan terbatasnya kompetensi pengelola; *hardware incidents* sebagai konsekuensi intensitas penggunaan perangkat IoT; serta *noncompliance* yang bersumber dari belum diadopsinya SOP institusional.

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



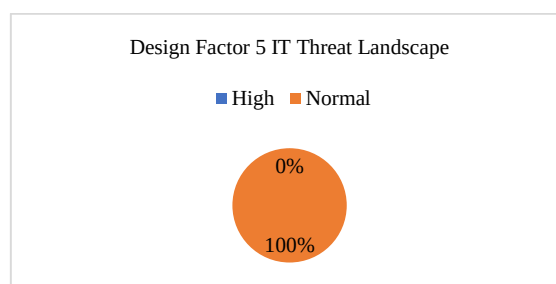
Gambar 5. *Design Factor 4 – I&T Related Issues*

Hasil penilaian DF4 untuk Lab IoT PNUP mengidentifikasi sepuluh isu yang tergolong serius (nilai 3), di antaranya: belum diadopsinya SOP institusional di tingkat laboratorium meskipun telah tersedia di tingkat Jurusan dan TU BMN; dokumentasi inventaris aset yang tidak memadai; mekanisme pencatatan peminjaman perangkat yang tidak ada; kontrol akses fisik laboratorium yang lemah; kinerja TI yang tidak terpantau secara periodik; serta ketiadaan prosedur penanganan insiden dan keberlangsungan layanan.

Kesenjangan regulasi ini memicu masalah operasional yang nyata di lapangan, seperti dokumentasi inventaris aset yang tidak terdata dengan baik serta aktivitas peminjaman alat yang sering kali tidak tercatat secara formal. Selain itu, aspek keamanan fisik dan akses laboratorium yang belum terkontrol secara sistematis menambah risiko terhadap keamanan aset-aset riset. Tanpa adanya sinkronisasi dengan kebijakan institusi yang sudah ada, Lab IoT PNUP sulit untuk menjamin akuntabilitas dan efisiensi dalam pengelolaan layanan akademiknya. Temuan ini memperkuat gambaran kondisi laboratorium yang memerlukan intervensi tata kelola yang komprehensif.

3.1.3 Tahap 3: Penyempurnaan Ruang Lingkup Sistem Tata Kelola (*Refine the Scope of the Governance System*)

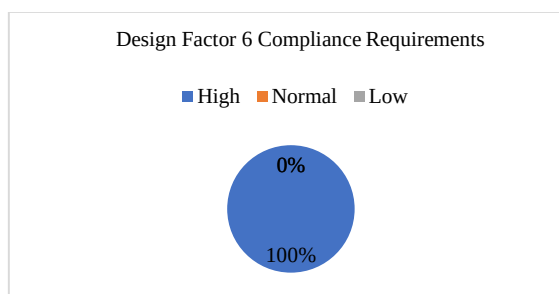
1. Design Factor 5 – Threat Landscape (lihat Gambar 6)



Gambar 6. Design Factor 5 – Threat Landscape

Lab IoT PNUP dinilai berada pada lanskap ancaman Normal (nilai 1.0). Penilaian ini didasarkan pada fakta bahwa infrastruktur jaringan laboratorium bersifat relatif tertutup dan terbatas pada lingkungan kampus, sehingga tidak terekspos pada ancaman siber tingkat tinggi yang umumnya dihadapi oleh organisasi komersial atau infrastruktur publik. Meskipun demikian, ancaman internal seperti penggunaan perangkat tanpa otorisasi tetap diperhitungkan dalam penilaian profil risiko pada DF3.

2. Design Factor 6 – Compliance Requirement (lihat Gambar 7)



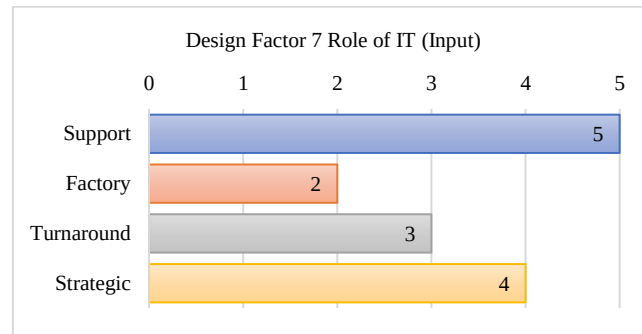
Gambar 7. Design Factor 6 – Compliance Requirement

Lab IoT PNUP dikategorikan pada tingkat kepatuhan Tinggi (*High*, nilai 1.0). Penetapan ini didasarkan pada dua regulasi utama yang mengikat operasional laboratorium: pertama, SOP institusional tingkat jurusan yang mengatur standar operasional pelaksanaan praktikum; dan kedua, regulasi Tata Usaha Barang Milik Negara (BMN) yang mengatur secara ketat pencatatan, pemeliharaan, dan pelaporan aset negara yang digunakan dalam laboratorium. Tingginya tingkat persyaratan kepatuhan ini menjadi salah satu justifikasi utama untuk memprioritaskan *objectives* yang berkaitan dengan kepatuhan dan pengendalian internal.

3. Design Factor 7 – Role of IT (lihat Gambar 8)

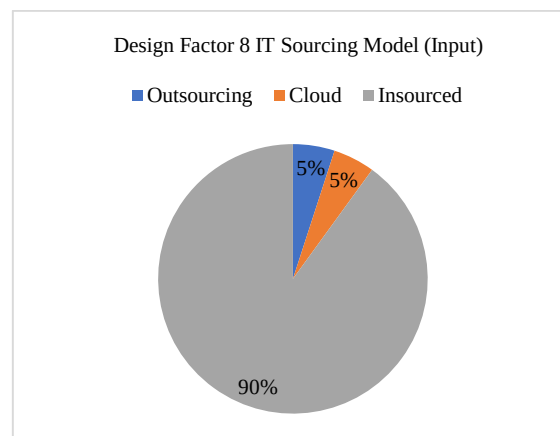
Dalam konteks Lab IoT PNUP, TI memegang peran *Support* yang sangat kritis (nilai 5) karena keseluruhan aktivitas praktikum mahasiswa bergantung pada ketersediaan dan keandalan infrastruktur TI laboratorium. Secara bersamaan, TI juga berperan *Strategic* (nilai 4) mengingat laboratorium berfungsi

sebagai pusat riset yang memanfaatkan TI sebagai *enabler* inovasi penelitian. Peran *Turnaround* dinilai 3, mencerminkan adanya upaya bertahap menuju standarisasi pengelolaan, sementara peran *Factory* dinilai 2 karena laboratorium tidak beroperasi dalam mode produksi kontinu layaknya lingkungan industri.



Gambar 8. Design Factor 7 – Role of IT

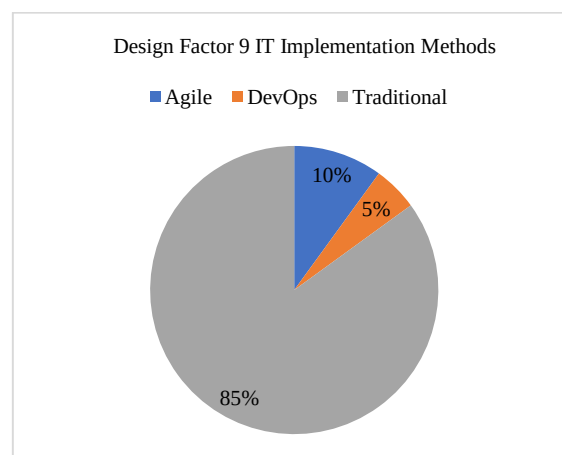
4. Design Factor 8 – IT Sourcing Model (lihat Gambar 9)



Gambar 9. Design Factor 8 – IT Sourcing Model

Lab IoT PNUP secara dominan menggunakan model *Insourced* (90%), di mana pengelolaan infrastruktur, perangkat keras, dan perangkat lunak laboratorium dilakukan secara mandiri oleh teknisi dan pengelola internal jurusan. Sebagian kecil dari layanan memanfaatkan *Cloud* (5%) dan *Outsourcing* (5%), terutama untuk layanan berbasis internet dan beberapa lisensi perangkat lunak tertentu. Dominasi model *insourced* ini membawa implikasi pada pentingnya pengembangan kompetensi internal dan standarisasi prosedur operasional.

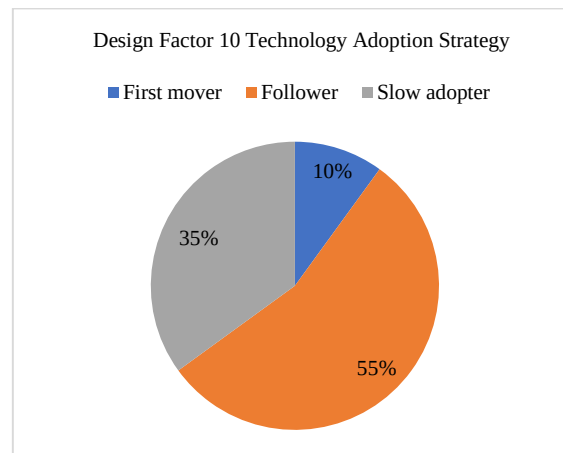
5. Design Factor 9 - IT Implementation Methods (lihat Gambar 10)



Gambar 10. Design Factor 9 : IT Implementation Methods

Lab IoT PNUP didominasi oleh metode *Traditional* (85%), yang mengacu pada pendekatan pengelolaan terstruktur dan formal dengan siklus perencanaan, implementasi, dan evaluasi yang bersifat linier. Proporsi *Agile* sebesar 10% mencerminkan fleksibilitas yang kadang diterapkan dalam pengembangan modul praktikum atau proyek riset yang memiliki iterasi cepat. DevOps hanya memiliki proporsi 5%, mengingat belum terintegrasinya *pipeline* pengembangan dan operasional secara otomatis di lingkungan laboratorium.

6. Design Factor 10 - Technology Adoption Strategy (lihat Gambar 11)



Gambar 11. Design Factor 10 - Technology Adoption Strategy

Lab IoT PNUP diklasifikasikan sebagai *Follower* (55%), yang berarti laboratorium cenderung mengadopsi teknologi setelah teknologi tersebut terbukti matang dan mendapat dukungan komunitas yang memadai. Posisi ini cukup umum di lingkungan akademik yang dibatasi oleh siklus anggaran dan kebutuhan kestabilan untuk keperluan praktikum. *Slow Adopter* (35%) mencerminkan proporsi teknologi lama yang masih dipertahankan demi keberlangsungan kurikulum yang ada, sementara *First Mover* (10%) merepresentasikan inisiatif riset terdepan yang dijalankan oleh beberapa dosen dalam kelompok riset IoT.

7. Design Factor 11 – Enterprise Size

Berdasarkan analisis terhadap struktur internal, Lab IoT PNUP diklasifikasikan sebagai unit laboratorium skala kecil atau small. Meskipun memiliki peran strategis yang besar, operasional harian laboratorium ini dikelola oleh tim yang kecil. Identifikasi ukuran organisasi ini sangat penting dalam perancangan tata kelola, karena akan memengaruhi kompleksitas struktur kontrol dan jumlah sumber daya yang perlu dialokasikan agar tetap efisien namun tetap akuntabel.

3.1.4 Tahap 4: Menyimpulkan Rancangan Sistem Tata Kelola (*Resolve Conflicts and Conclude the Governance System Design*)

Dari pengolahan 11 *design factor* menggunakan COBIT 2019 Design Toolkit diperoleh skor kepentingan relatif untuk seluruh 40 *governance and management objectives*. Terdapat 12 *objectives* dengan skor positif; tujuh di antaranya dengan skor ≥ 50 (EDM03, APO12, APO13, MEA03, DSS05, DSS04, DSS06) ditetapkan sebagai prioritas utama dan diukur kapabilitasnya. Hasil selengkapnya ditunjukkan pada Gambar 12.

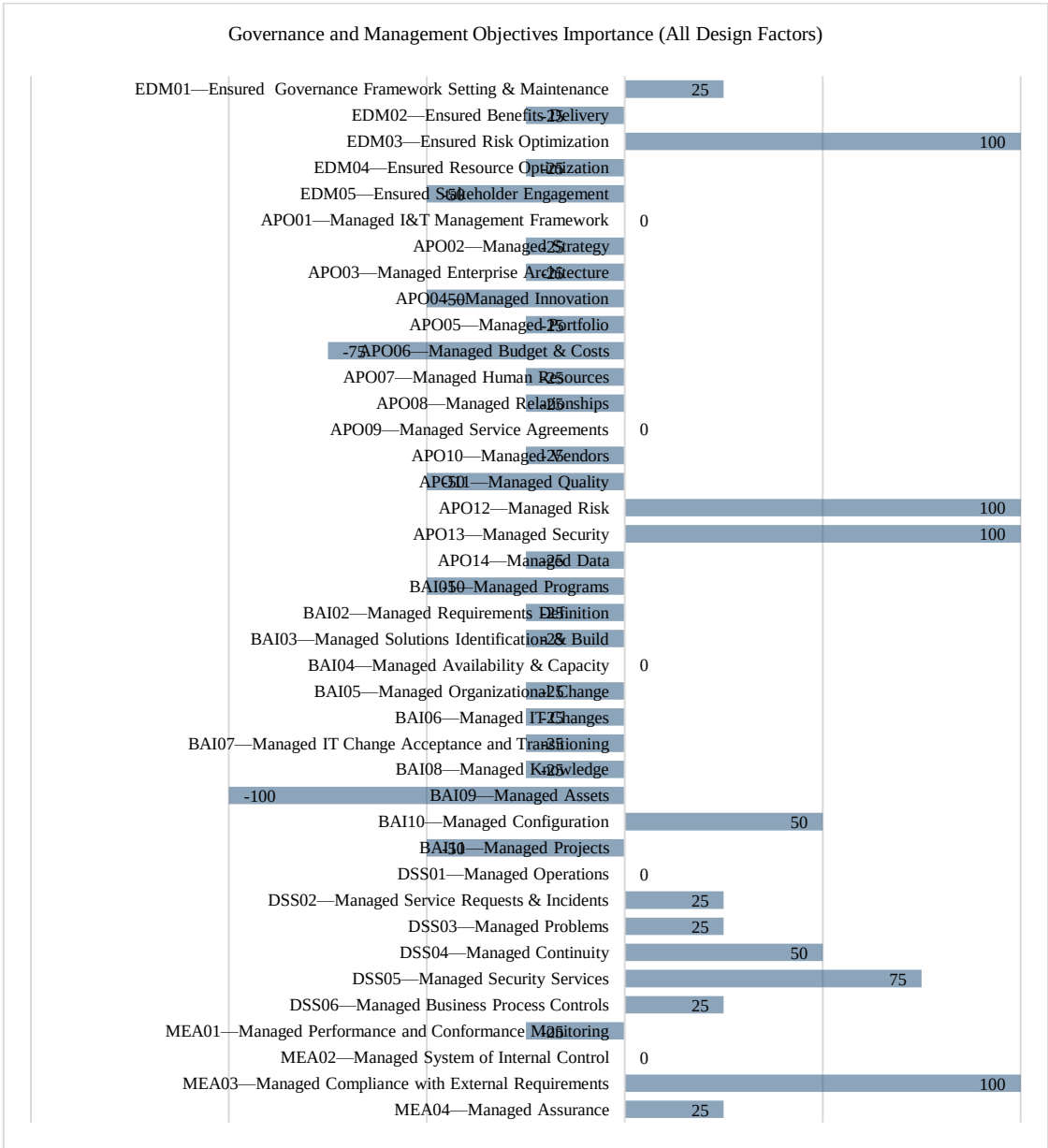
Prioritas utama (skor 100, target Level 4): EDM03, APO12, APO13, dan MEA03 mencerminkan urgensi pengendalian risiko, keamanan, dan kepatuhan regulasi di Lab IoT PNUP. DSS05 (skor 75, target Level 4) membentuk kelompok pendukung bersama DSS04 dan DSS06 (skor 50, target Level 3), sementara DSS02, DSS03, dan MEA04 (skor 25, target Level 2) merepresentasikan fondasi operasional yang perlu dibangun secara paralel.

3.2. Pengukuran Tingkat Kapabilitas

Langkah berikutnya setelah menyimpulkan 7 domain yang akan dievaluasi kedalam titik kritis adalah mengukur tingkat kompetensi/kapabilitas di setiap bidang utama. Responden berjumlah 4 orang yang terdiri dari 1 pengelola Lab IoT dan 3 Dosen pengampu rumpun mata kuliah IoT. Pemilihan keempat responden ini menggunakan pendekatan *total sampling* karena seluruh personel yang memiliki akses langsung dan kewenangan terhadap operasional Lab IoT PNUP hanya berjumlah 4 orang, sehingga seluruh populasi diikutsertakan sebagai responden. Pendekatan ini selaras dengan prinsip *purposive expert sampling* yang

lazim diterapkan pada unit organisasi berskala kecil, di mana kualitas penilaian ditentukan oleh relevansi kompetensi responden terhadap domain yang dinilai, bukan semata-mata kuantitas sampel [22].

Keempat responden dipilih karena merupakan seluruh pihak yang secara langsung terlibat dalam pengelolaan operasional dan akademik laboratorium, sehingga representasi populasi bersifat lengkap (100%). Keempat responden diharuskan mengisi pernyataan-pernyataan pada kuesioner yang telah dibagikan sebelumnya pada masing-masing domain dengan memilih Ya (Y), jika aktivitas telah dilakukan, dan Tidak (T), jika aktivitas belum dilakukan oleh Lab IoT PNUP. Skala penilaian: *Fully* (F) >85%, *Largely* (L) 50–85%, *Partially* (P) 15–50%, *Not* (N) <15%. Domain dapat naik ke level berikutnya hanya jika mencapai *Fully*; jika *Largely*, *Partially*, atau *Not*, penilaian berhenti pada level tersebut [11]. Hasil pengukuran tingkat kapabilitas saat ini dapat dilihat pada Tabel 1.



Gambar 12. Kesimpulan Seluruh Design Factor

Tabel 1. Hasil Pengukuran Tingkat Kapabilitas Saat Ini

No	Domain (Proses)	Skor Design Toolkit	Capability Level Saat Ini	Kategori
1	EDM03 – Ensured Risk Optimization	100	Level 1	Largely (68,75%)
2	APO12 – Managed Risk	100	Level 1	Largely (75%)
3	APO13 – Managed Security	100	Level 1	Partially (25%)
4	MEA03 – Managed Compliance with External Requirements	100	Level 1	Partially (18,75%)

No	Domain (Proses)	Skor Design Toolkit	Capability Level Saat Ini	Kategori
5	DSS05 – <i>Managed Security Services</i>	75	Level 1	<i>Partially</i> (20%)
6	DSS04 – <i>Managed Continuity</i>	50	Level 1	<i>Partially</i> (25%)
7	DSS06 – <i>Managed Business Process Controls</i>	50	Level 1	<i>Not</i> (6,25%)

Seluruh 7 domain berada pada *Capability Level* 1 dengan kategori bervariasi dari *Largely* hingga *Not* yang menandakan bahwa aktivitas selanjutnya tidak dapat diukur karena berada dibawah standar nilai 85%. Sehingga dapat disimpulkan bahwa domain proses EDM03, APO12, APO13, MEA03, DSS05, DSS04, dan DSS06 hanya mencapai tingkat kapabilitas level 1 (*Performed*), menunjukkan bahwa tata kelola TI Lab IoT PNUP masih berada pada tahap awal dan membutuhkan intervensi yang komprehensif dan menyeluruh

3.3. Analisis Kesenjangan

Analisis kesenjangan dilakukan untuk mengidentifikasi rekomendasi tata kelola TI yang paling sesuai bagi organisasi, dengan membandingkan kondisi saat ini dan kondisi yang diharapkan. Pada penelitian ini, tujuh domain yang dianalisis pada Laboratorium IoT PNUP, yaitu EDM03, APO12, APO13, MEA03, DSS05, DSS04, dan DSS06, telah diukur tingkat kapabilitasnya. Selanjutnya dilakukan analisis kesenjangan (*gap*) dari *capability level* masing-masing domain. Hasil analisis kesenjangan ditunjukkan pada Tabel 2.

Tabel 2. Hasil Analisis Kesenjangan (*Gap Analysis*) Tingkat Kapabilitas Lab IoT PNUP

No	Domain (Proses)	Capability Level Saat Ini (As-Is)	Target Capability Level (To-Be)	Gap	Prioritas
1	EDM03 – <i>Ensured Risk Optimization</i>	Level 1 (<i>Largely</i> , 68,75%)	Level 4	+3	Sangat Tinggi
2	APO12 – <i>Managed Risk</i>	Level 1 (<i>Largely</i> , 75%)	Level 4	+3	Sangat Tinggi
3	APO13 – <i>Managed Security</i>	Level 1 (<i>Partially</i> , 25%)	Level 4	+3	Sangat Tinggi
4	MEA03 – <i>Managed Compliance with External Requirements</i>	Level 1 (<i>Partially</i> , 18,75%)	Level 4	+3	Sangat Tinggi
5	DSS05 – <i>Managed Security Services</i>	Level 1 (<i>Partially</i> , 20%)	Level 4	+3	Tinggi
6	DSS04 – <i>Managed Continuity</i>	Level 1 (<i>Partially</i> , 25%)	Level 3	+2	Tinggi
7	DSS06 – <i>Managed Business Process Controls</i>	Level 1 (<i>Not</i> , 6,25%)	Level 3	+2	Tinggi

Berdasarkan Tabel 2, seluruh tujuh domain yang dievaluasi menunjukkan kesenjangan yang signifikan antara kondisi saat ini (*as-is*) dan target yang ditetapkan (*to-be*). Kelima domain dengan target *Capability Level* 4 (EDM03, APO12, APO13, MEA03, dan DSS05) memiliki kesenjangan sebesar +3 level, sedangkan dua domain dengan target Level 3 (DSS04 dan DSS06) memiliki kesenjangan sebesar +2 level. Tidak ada satu pun domain yang telah memenuhi target yang ditetapkan, yang mengindikasikan bahwa tata kelola TI Lab IoT PNUP secara keseluruhan masih berada pada tahap awal dan memerlukan intervensi yang terstruktur dan menyeluruh.

Mengingat besarnya kesenjangan yang ada serta keterbatasan skala Lab IoT PNUP sebagai organisasi kecil (*small enterprise*), pencapaian target tersebut direkomendasikan dilakukan secara bertahap (*phased approach*). Pada jangka pendek, prioritas utama adalah memastikan seluruh domain mencapai Level 2 dengan membangun prosedur dan dokumentasi dasar yang konsisten. Selanjutnya, pada jangka menengah, domain-domain dengan target Level 3 dan 4 dapat ditingkatkan secara bertahap seiring dengan penguatan kapasitas sumber daya manusia dan sistem pemantauan internal laboratorium.

Dua domain dengan kategori *Largely*, yaitu EDM03 (68,75%) dan APO12 (75%), menunjukkan bahwa kesadaran terhadap risiko sudah mulai terbentuk, meskipun masih bersifat informal dan belum didukung oleh mekanisme yang terdokumentasi. Sementara itu, domain keamanan APO13 (25%) dan DSS05 (20%) mencerminkan lemahnya kontrol akses serta pengendalian keamanan informasi. Kondisi ini menunjukkan tingkat risiko yang cukup tinggi, mengingat karakteristik infrastruktur IoT yang cenderung rentan. MEA03 (18,75%) mengindikasikan belum diadopsinya SOP dan regulasi BMN di tingkat operasional laboratorium, yang berpotensi memengaruhi akreditasi BAN-PT. DSS06 (6,25%, *Not*) merupakan kondisi paling kritis karena hampir tidak terdapat pengendalian proses bisnis formal, termasuk pencatatan peminjaman alat. DSS04 (25%) menunjukkan bahwa prosedur keberlangsungan layanan belum terdefinisi dengan baik. Oleh karena itu, peningkatan pada DSS06 dan DSS04 menjadi prioritas utama sebagai fondasi untuk pengembangan domain lainnya secara sistematis.

3.4. Rekomendasi

Berdasarkan hasil analisis kesenjangan pada Tabel 2, seluruh tujuh domain berada pada *Capability Level* 1 dengan kesenjangan +2 hingga +3 level terhadap target masing-masing. Mengingat skala Lab IoT PNUP sebagai organisasi kecil (*small enterprise*) dengan sumber daya yang terbatas, rekomendasi disusun menggunakan *phased approach* yang terbagi ke dalam tiga fase implementasi. Peta jalan implementasi rekomendasi disajikan pada Tabel 3.

Berdasarkan peta jalan pada Tabel 3, berikut dijabarkan rekomendasi perbaikan per domain secara bertahap. Setiap domain diuraikan dari *Capability Level* 1 menuju target yang ditetapkan, dengan output konkret pada tiap level.

1. DSS06 – Managed Business Process Controls (Target: Level 3)

DSS06 menjadi domain paling kritis dengan capaian hanya 6,25%, yang berarti hampir tidak ada pengendalian proses bisnis formal yang berjalan di laboratorium saat ini. Untuk mencapai Level 2, langkah pertama yang perlu dilakukan adalah memformalkan log peminjaman perangkat IoT dan mengadopsi SOP jurusan ke dalam operasional harian, sekaligus menetapkan siapa yang bertanggung jawab atas setiap proses. Keluaran konkret dari tahap ini berupa dokumen log peminjaman dan SOP yang telah diadopsi secara resmi. Setelah fondasi tersebut terbentuk, peningkatan menuju Level 3 dapat dicapai dengan menjalankan verifikasi penggunaan perangkat secara berkala, mengevaluasi kepatuhan SOP, dan mengintegrasikan hasilnya ke dalam laporan periodik laboratorium sehingga rekam jejak pengendalian proses menjadi terdokumentasi dengan baik

Tabel 3. Peta Jalan Implementasi Rekomendasi Tata Kelola TI Lab IoT PNUP

Fase	Jangka Waktu	Domain	Target Level	Aktivitas Utama
Fase 1	0–6 bulan	DSS06, DSS04	Level 2–3	Formalisasi pencatatan aktivitas, adopsi SOP, pendefinisian prosedur penanganan gangguan layanan
Fase 2	6–18 bulan	AP013, MEA03, DSS05	Level 3–4	Pengendalian akses fisik dan logis, inventarisasi perangkat IoT, sinkronisasi kepatuhan regulasi BMN dan SOP
Fase 3	18–36 bulan	EDM03, AP012	Level 4	Institusionalisasi manajemen risiko, penetapan toleransi risiko, integrasi evaluasi risiko ke siklus operasional

2. DSS04 – Managed Continuity (Target: Level 3)

Dengan capaian 25%, DSS04 mencerminkan kondisi di mana laboratorium belum memiliki prosedur yang jelas untuk menghadapi gangguan layanan. Menuju Level 2, prioritasnya adalah mendokumentasikan prosedur penanganan gangguan seperti kerusakan perangkat atau kegagalan jaringan, sekaligus menetapkan siapa yang bertanggung jawab untuk tiap jenis gangguan tersebut. Dokumen prosedur penanganan gangguan menjadi keluaran utama tahap ini. Selanjutnya, untuk mencapai Level 3, laboratorium perlu menyusun rencana keberlangsungan layanan yang mencakup skenario pemulihan darurat praktikum, melakukan simulasi minimal sekali per semester, dan mendokumentasikan setiap insiden yang terjadi agar pola permasalahan dapat dianalisis secara sistematis. Keluaran akhirnya berupa dokumen *continuity plan* dan rekam jejak simulasi pemulihan.

3. AP013 – Managed Security (Target: Level 4)

AP013 berada di posisi *Partially* dengan capaian 25%, menandakan bahwa kebijakan keamanan informasi di laboratorium masih bersifat *ad hoc*. Perjalanan menuju Level 2 dimulai dengan menginventarisasi perangkat IoT berdasarkan potensi kerentanannya, menerapkan autentikasi untuk akses laboratorium, dan menetapkan kebijakan keamanan jaringan yang paling mendasar. Di Level 3, kebijakan-kebijakan tersebut dibakukan, dilengkapi dengan *program security awareness* bagi pengelola dan prosedur pelaporan insiden yang terstruktur. Selanjutnya, pada Level 4, pengelolaan keamanan ditingkatkan melalui audit berkala, pembaruan kebijakan berbasis riwayat insiden, serta penguatan kompetensi pengelola di bidang keamanan IoT. Keluaran yang dihasilkan mencakup inventaris risiko, kebijakan keamanan terdokumentasi, dan laporan audit berkala.

4. DSS05 – Managed Security Services (Target: Level 4)

DSS05 ditingkatkan secara paralel bersama AP013, karena keduanya saling melengkapi dalam memperkuat keamanan laboratorium. Peningkatan menuju Level 2 berfokus pada kontrol akses fisik ke Lab IoT (ruang server dan perangkat IoT), pengelolaan hak akses, serta pencatatan insiden layanan secara konsisten. Di Level 3, pemantauan keamanan jaringan dilakukan secara berkala, prosedur penanganan insiden distandarisasi, dan hak akses ditinjau secara rutin dengan prinsip *least privilege* sebagai acuan. Level

4 dicapai ketika kontrol keamanan terus disempurnakan berdasarkan pola insiden historis dan pengujian penetrasi dilakukan secara berkala sebagai mekanisme verifikasi. Seluruh proses ini menghasilkan prosedur kontrol akses, laporan pemantauan jaringan, dan laporan pengujian keamanan yang dapat dijadikan referensi audit.

5. MEA03 – Managed Compliance with External Requirements (Target: Level 4)

MEA03 mencatat capaian terendah di antara domain dengan target Level 4, hanya 18,75%. Kondisi ini menunjukkan belum terintegrasinya kewajiban regulasi eksternal, termasuk SOP jurusan dan regulasi BMN, ke dalam praktik operasional laboratorium sehari-hari. Untuk mencapai Level 2, langkah awal mengidentifikasi dan mendokumentasikan seluruh regulasi yang berlaku, menyusun matriks kepatuhan, dan menetapkan prosedur pelaporan aset yang jelas. Pada Level 3, pemantauan kepatuhan dilakukan secara berkala dan hasilnya diintegrasikan ke dalam laporan pengelolaan jurusan, disertai sosialisasi kepada seluruh pengelola. Level 4 dicapai ketika laboratorium mampu mendeteksi potensi pelanggaran, menganalisis tren ketidakpatuhan berbasis data historis, serta meningkatkan kapasitas SDM dalam pengelolaan aset. Luaran utamanya berupa matriks kepatuhan, laporan pemantauan, dan dokumen analisis tren sebagai bukti pendukung akreditasi BAN-PT.

6. APO12 – Managed Risk (Target: Level 4)

APO12 memiliki capaian 75% (Largely), menunjukkan bahwa kesadaran risiko sudah terbentuk, namun belum terdokumentasi dengan baik. Untuk mencapai Level 2, diperlukan formalisasi melalui penyusunan *risk register* operasional serta penetapan penanggung jawab risiko. Pada Level 3, *risk register* diperbarui secara berkala, diintegrasikan ke dalam laporan, dan didukung pelatihan manajemen risiko. Selanjutnya, Level 4 dicapai dengan penetapan toleransi risiko yang terukur, pengembangan model prediktif, serta integrasi evaluasi risiko ke dalam perencanaan. Keluaran yang dihasilkan meliputi *risk register*, laporan evaluasi risiko, dan model prediktif sebagai dasar pengambilan keputusan.

7. EDM03 – Ensured Risk Optimization (Target: Level 4)

Sebagai domain tata kelola tertinggi, EDM03 memerlukan komitmen formal dari pimpinan jurusan agar implementasi dapat berkelanjutan. Dengan capaian 68,75%, fondasi sudah ada, namun masih memerlukan legitimasi kelembagaan. Untuk mencapai Level 2, diperlukan pengesahan kebijakan risiko TI, penetapan peran secara jelas, serta integrasi risiko dalam proses pengadaan. Pada Level 3, pengelolaan risiko diselaraskan dengan tujuan strategis melalui tinjauan berkala dan pelaporan kepada pimpinan. Level 4 dicapai ketika evaluasi tata kelola berbasis indikator terukur, dengan APO12 menjadi umpan balik dalam siklus peningkatan berkelanjutan. Keluaran mencakup kebijakan risiko TI, laporan tinjauan, dan dokumen *governance review*.

Hasil penelitian menunjukkan bahwa ketujuh domain prioritas: EDM03, APO12, APO13, MEA03, DSS05, DSS04, dan DSS06 berada pada Capability Level 1 dengan kesenjangan +2 hingga +3 level terhadap target masing-masing. Temuan ini sejalan dengan Adikara [15] yang menyatakan bahwa laboratorium pendidikan tinggi umumnya baru berada pada tahap awal pengelolaan TI, serta Rosyidah dan Kurniawati [17] yang menemukan kesenjangan signifikan pada laboratorium Teknik Informatika. Kesenjangan rendahnya capability level ini mengonfirmasi tantangan struktural yang sama: belum tersedianya mekanisme tata kelola TI yang terformalkan di tingkat operasional, meskipun regulasi institusional sudah tersedia di tingkat yang lebih tinggi. Keunggulan penelitian ini terletak pada penggunaan mekanisme *design factors* COBIT 2019 yang menghasilkan prioritas lebih kontekstual dan terukur dibandingkan pendekatan generik COBIT 5 pada studi-studi sebelumnya [15][16][17].

Dominasi DF1 *Client Service/Stability* dan DF6 *Compliance Requirement* secara logis menghasilkan prioritas pada domain risiko, keamanan, dan kepatuhan, selaras dengan temuan Afdhani dan Soewito [19], Sopacua dan Haryani [20], serta Rasmila et al. [21] yang membuktikan efektivitas *design factors* dalam menghasilkan rekomendasi yang lebih tepat sasaran. Penelitian ini memperluas validasi mekanisme tersebut ke konteks laboratorium IoT pendidikan tinggi vokasi yang belum pernah diteliti sebelumnya.

Rendahnya capaian APO13 (25%) dan DSS05 (20%) mencerminkan kerentanan infrastruktur IoT yang melekat, sebagaimana ditegaskan Roman et al. [8] bahwa setiap perangkat IoT berpotensi menjadi titik kerentanan, dan Gubbi et al. [6] bahwa ekosistem IoT memerlukan pendekatan keamanan yang holistik dan berlapis. Tanpa kebijakan keamanan yang terformalisasi, laboratorium rentan terhadap akses tidak sah, kehilangan data, dan gangguan layanan praktikum. Peningkatan APO13 dan DSS05 secara paralel sejalan dengan rekomendasi Sabran et al. [7] tentang pentingnya prosedur operasional terencana mulai dari kontrol akses hingga pengelolaan aset *real-time*.

Capaian MEA03 (18,75%) dan DSS06 (6,25%) mengindikasikan kesenjangan sistemik antara regulasi institusional dan praktik operasional. Nasution [18] menemukan permasalahan serupa pada Laboratorium Terpadu UIN Sunan Kalijaga akibat tata kelola terdesentralisasi tanpa standar terukur; namun berbeda dengan Nasution [18] yang hanya merekomendasikan model berbasis penjaminan mutu internal, penelitian

ini menyajikan pengukuran terstandarisasi menggunakan skala ISACA dan rekomendasi berbasis *phased roadmap* yang konkret. Kondisi DSS06 yang hampir tidak menunjukkan pengendalian proses formal berpotensi memengaruhi kepatuhan terhadap regulasi BMN dan penilaian akreditasi BAN-PT [3], sehingga penempatannya sebagai prioritas pertama Fase 1 merupakan keputusan strategis yang tepat.

Pendekatan *phased roadmap* tiga fase: formalisasi proses dasar (0–6 bulan), penguatan keamanan dan kepatuhan (6–18 bulan), serta institusionalisasi tata kelola risiko (18–36 bulan) merupakan kontribusi yang membedakan penelitian ini secara substansial dari seluruh studi terdahulu [15][16][17][19][20][21] yang tidak menghasilkan peta jalan implementasi bertahap. Pendekatan ini mencerminkan prinsip peningkatan berkelanjutan COBIT 2019 [12] dan sejalan dengan Weill dan Ross [9] bahwa tata kelola TI yang efektif dibangun secara inkremental sesuai kematangan organisasi.

4. KESIMPULAN

Penelitian ini merancang tata kelola TI untuk Laboratorium IoT PNUP menggunakan kerangka COBIT 2019 melalui empat tahap *Governance System Design Workflow*. Dari analisis sebelas *design factor*, diidentifikasi tujuh objektif prioritas, yaitu EDM03, APO12, APO13, MEA03, DSS05, DSS04, dan DSS06. Hasil pengukuran menunjukkan seluruh domain berada pada Capability Level 1 dengan capaian bervariasi, dari *Not* pada DSS06 (6,25%) hingga *Largely* pada APO12 (75%). Kesenjangan sebesar +2 hingga +3 level menunjukkan bahwa tata kelola TI masih berada pada tahap awal dan memerlukan perbaikan sistematis.

Analisis kesenjangan mengungkap dua temuan utama. Pertama, lemahnya pengendalian operasional harian (DSS06 dan DSS04) akibat belum diadopsinya SOP institusional di tingkat laboratorium. Kedua, rapuhnya keamanan informasi dan kepatuhan terhadap regulasi (APO13, DSS05, dan MEA03). Kondisi yang terakhir ini berpotensi memengaruhi akuntabilitas pengelolaan aset negara sekaligus penilaian akreditasi institusi oleh BAN-PT. Sebagai respons terhadap kondisi tersebut, penelitian ini menghasilkan rekomendasi bertahap yang terstruktur dalam tiga fase. Fase pertama (0–6 bulan) memprioritaskan formalisasi pencatatan dan adopsi SOP untuk DSS06 dan DSS04. Fase kedua (6–18 bulan) berfokus pada penguatan keamanan informasi dan kepatuhan terhadap regulasi melalui APO13, DSS05, dan MEA03. Fase ketiga (18–36 bulan) menargetkan institusionalisasi tata kelola risiko melalui APO12 dan EDM03, yang membutuhkan kematangan dari dua fase sebelumnya sebagai prasyaratnya.

Penelitian ini memberikan kontribusi berupa rancangan tata kelola TI berbasis COBIT 2019 yang spesifik untuk laboratorium IoT dalam ekosistem pendidikan tinggi vokasi. Penelitian ini memiliki keterbatasan pada jumlah responden ($n=4$) yang terbatas, sehingga generalisasi temuan ke laboratorium sejenis perlu dilakukan dengan kehati-hatian. Penelitian lanjutan dapat difokuskan pada pengukuran ulang kapabilitas pasca-implementasi untuk memverifikasi efektivitas rekomendasi yang telah dirancang, serta memperluas jumlah responden untuk meningkatkan validitas hasil.

REFERENSI

- [1] Undang-Undang Republik Indonesia Nomor 12 Tahun 2012 tentang Pendidikan Tinggi, Lembaran Negara Republik Indonesia Tahun 2012 Nomor 158, Jakarta, 2012.
- [2] Peraturan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi, Jakarta: Kemendikbud, 2020.
- [3] Badan Akreditasi Nasional Perguruan Tinggi (BAN-PT), *Instrumen Akreditasi Program Studi*, Jakarta: BAN-PT, 2019.
- [4] Peraturan Menteri Pendidikan Tinggi, Sains, dan Teknologi Republik Indonesia Nomor 39 Tahun 2025 tentang Penjaminan Mutu Pendidikan Tinggi, Jakarta: Kemdiktisaintek, 2025.
- [5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [7] Sabran, Purnamawati, and Nasruddin, "Penerapan Smart Lab Automation Berbasis IoT pada Laboratorium Digital Jurusan Pendidikan Teknik Elektronika FT-UNM," *JETC*, vol. 15, no. 2, pp. 1–9, Dec. 2020.
- [8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.
- [9] P. Weill and J. W. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Boston: Harvard Business School Press, 2004.
- [10] W. Van Grembergen, S. De Haes, and E. Guldentops, "Structures, Processes and Relational Mechanisms for IT Governance," in *Strategies for Information Technology Governance*, W. Van Grembergen, Ed. Hershey: Idea Group Publishing, 2004.
- [11] A. D. Dewantara, "Pengukuran Tingkat Kapabilitas Tata Kelola Teknologi Informasi Berdasarkan COBIT 5: Studi Kasus Pusat Data dan Informasi (PUSDATIN) Arsip Nasional Republik Indonesia

- (ANRI),” M.S. thesis, Universitas Indonesia, Jakarta, 2015
- [12] ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, Schaumburg, IL: ISACA, 2018.
 - [13] ISACA, *COBIT® 2019 Governance and Management Objectives*, Schaumburg, IL: ISACA, 2018.
 - [14] ISACA, *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, Schaumburg, IL: ISACA, 2018.
 - [15] F. S. Adikara, “Implementasi Tata Kelola Teknologi Informasi Perguruan Tinggi Berdasarkan COBIT 5 pada Laboratorium Rekayasa Perangkat Lunak Universitas Esa Unggul,” *Seminar Nasional Sistem Informasi Indonesia*, pp. 1–6, 2013.
 - [16] S. V. N. Afni, A. Widaksono, and T. Hardiani, “Tata Kelola Teknologi Informasi Menggunakan COBIT 5 untuk Peningkatan Strategi pada Laboratorium Universitas XYZ,” *Prosiding Seminar Nasional Penelitian dan Pengabdian Kepada Masyarakat LPPM Universitas 'Aisyiyah Yogyakarta*, vol. 1, pp. 400–410, 2023.
 - [17] U. Rosyidah and L. S. Kurniawati, “Pengukuran dan Analisis Capability Level Tata Kelola IT di Laboratorium Teknik Informatika menggunakan COBIT 5,” *BIOS: Jurnal Teknologi Informasi dan Rekayasa Komputer*, vol. 7, no. 1, pp. 36–41, 2026.
 - [18] K. Nasution, “Pengembangan Tata Kelola Laboratorium Universitas Islam Negeri Sunan Kalijaga Yogyakarta,” *IJAR: Indonesian Journal of Action Research*, vol. 4, no. 1, pp. 33–39, 2025.
 - [19] 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 Teknologi Informasi (JTK3TI)*, vol. 10, no. 1, pp. 22–33, 2024.
 - [20] F. J. Sopacua and E. Haryani, “Penerapan Framework COBIT 2019 pada Evaluasi Tata Kelola Teknologi Informasi di Yayasan Pendidikan,” *JEPIN: Jurnal Edukasi dan Penelitian Informatika*, vol. 10, no. 2, pp. 324–332, 2024.
 - [21] Rasmila, S. Riansyah, M. I. Firnando, M. R. Wahyudi, and M. F. Anugrah, “Framework COBIT 2019: Analisis dan Desain Tata Kelola Teknologi Informasi (Studi Kasus pada CV Ifadah Daya Bersama),” *Jurnal Nasional Ilmu Komputer*, vol. 6, no. 1, pp. 6–18, 2025.
 - [22] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th ed., Thousand Oaks: Sage Publications, 2014.
 - [23] E. Amore, T. Dilger, M. Mezzenzana, C. Ploder, and R. Bernsteiner, “Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study,” *KnE Social Sciences*, vol. 8, no. 1, pp. 73–101, Feb. 2023, doi: 10.18502/kss.v8i1.12636.
 - [24] M. B. Hardjadinata, and J. Witratama, “Capability Assessment of IT Governance Using the 2019 COBIT Framework for the IT Business Consultant Industry,” *International Journal of Science, Technology & Management*, vol. 4, no. 4, pp. 1034–1039, July. 2023, doi: 10.46729/ijstm.v4i4.902