INTEGRASI COSO, ITIL, DAN COBIT 2019 UNTUK PENGUATAN TATA KELOLA PEMERIKSAAN DIGITAL: ANALISIS KOMPREHENSIF SISTEM APLIKASI PEMERIKSAAN (SIAP) BPK RI

ABSTRACT

The digital transformation of public sector auditing requires systems that integrate audit process control, information technology governance, and IT service management. The Audit Board of the Republic of Indonesia (BPK RI) has implemented the Sistem Aplikasi Pemeriksaan (SiAP) to support digital workpaper management, hierarchical validation, team coordination, and audit progress monitoring. However, its effectiveness must be evaluated against internationally recognized governance frameworks. This study employs an analytical–comparative approach to assess SiAP's alignment with COSO, COBIT 2019, and ITIL 4. The results show strong alignment with COSO, particularly in control activities and monitoring mechanisms. Conversely, notable gaps remain in COBIT 2019—especially in IT risk governance, change management, and service delivery. Key ITIL practices, such as incident management and service continuity, are also not fully implemented. This research proposes an integrated COSO–COBIT–ITIL–SiAP governance model to enhance accountability, reliability, and resilience in BPK's digital audit ecosystem, contributing to the advancement of public sector audit digitalization.

ABSTRAK

Transformasi digital pemeriksaan negara menuntut sistem yang mampu mengintegrasikan pengendalian proses audit, tata kelola teknologi informasi, dan manajemen layanan TI. Sistem Aplikasi Pemeriksaan (SiAP) BPK RI telah mendukung digitalisasi Kertas Kerja Pemeriksaan (KKP), validasi berlapis, serta monitoring kinerja tim. Namun, efektivitas SiAP perlu dinilai dari perspektif tata kelola internasional. Penelitian ini menggunakan pendekatan analitis–komparatif untuk mengevaluasi keselarasan SiAP dengan COSO, COBIT 2019, dan ITIL 4. Hasil menunjukkan bahwa SiAP sangat selaras dengan COSO, terutama dalam aktivitas pengendalian dan monitoring. Sebaliknya, terdapat kesenjangan signifikan pada aspek COBIT 2019, seperti manajemen risiko TI, siklus pengembangan, dan layanan pendukung. Praktik ITIL juga belum sepenuhnya diterapkan, khususnya terkait incident management dan service continuity. Penelitian ini mengusulkan model tata kelola terintegrasi COSO–COBIT–ITIL–SiAP untuk memperkuat akuntabilitas, keandalan, dan ketahanan sistem pemeriksaan digital BPK. Model ini menjadi langkah strategis menuju ekosistem audit digital yang lebih matang dan berkelanjutan.

I. INTRODUCTION

Transformasi digital dalam sektor pemeriksaan negara tidak hanya merupakan tren global, tetapi sebuah kebutuhan strategis untuk memastikan akuntabilitas, transparansi, dan efisiensi dalam penggunaan keuangan negara. Evolusi teknologi informasi telah menggeser paradigma pemeriksaan dari sistem berbasis dokumen fisik yang tersebar, rentan duplikasi, dan sulit ditelusuri, menuju sistem digital terintegrasi yang memungkinkan seluruh proses audit terdokumentasi secara elektronik, real-time, dan dapat diakses oleh seluruh pemangku kepentingan berwenang. Perubahan ini tidak sekadar bersifat teknis, melainkan mengubah cara pandang lembaga pemeriksa dalam memaknai governance, responsibility, dan trustworthiness di era digital.

Dalam konteks Indonesia, Badan Pemeriksa Keuangan Republik Indonesia (BPK RI) telah merespons tuntutan tersebut melalui pengembangan dan implementasi Sistem Aplikasi Pemeriksaan (SiAP)—sebuah platform digital yang memfasilitasi proses pemeriksaan secara menyeluruh. SiAP dirancang untuk mengelola Kertas Kerja Pemeriksaan (KKP), menyelaraskan pembagian tugas antaranggota tim, memfasilitasi validasi berlapis, menyimpan bukti digital, serta mendukung penyusunan Laporan Hasil Pemeriksaan (LHP). Dalam Manual SiAP Web 3 Januari 2022, BPK secara eksplisit menekankan bahwa SiAP bukan sekadar wadah penyimpanan dokumen, tetapi sistem pengendalian proses pemeriksaan yang memastikan setiap langkah kerja pemeriksa dapat dipantau, dinilai, ditelusuri, dan dipertanggungjawabkan.

Sebagai single source of truth, SiAP memainkan peran yang jauh lebih penting daripada hanya sebagai aplikasi kerja; ia menjadi infrastruktur inti pemeriksaan negara. Struktur peran dalam SiAP memungkinkan interaksi terkoordiansi antara Tortama/Kalan, Pengendali Teknis, Ketua Tim, dan Anggota Tim. Interaksi ini tidak hanya mengalir secara administratif, tetapi dikawal melalui mekanisme kontrol berlapis yang memastikan kualitas, konsistensi, dan integritas pemeriksaan. Dengan kata lain, SiAP menghadirkan ekosistem digital yang memperkuat prinsip segregation of duties dan chain of accountability yang telah lama menjadi fondasi sistem pemeriksaan BPK.

Namun, modernisasi proses pemeriksaan melalui sistem digital seperti SiAP juga membawa tantangan baru yang tidak dapat diabaikan. Kompleksitas sistem digital memunculkan potensi risiko yang bersifat multidimensi: risiko teknologi (gangguan sinkronisasi, system downtime, kelemahan keamanan), risiko operasional (kesalahan input, ketidaksesuaian versi dokumen), hingga risiko manajemen layanan (insiden yang tidak tertangani, lambatnya respon dukungan teknis, kurangnya dokumentasi perubahan). Dengan demikian, keberhasilan SiAP tidak hanya ditentukan oleh kecanggihan fitur auditnya, tetapi sangat dipengaruhi oleh kesiapan tata kelola internal kontrol, tata kelola TI, dan manajemen layanan TI yang mengelilinginya.

Pada titik inilah integrasi antara ilmu pemeriksaan dan manajemen TI menjadi krusial. Tata kelola pemeriksaan digital tidak dapat berdiri sendiri tanpa kerangka kerja yang diakui secara internasional. Tiga kerangka global menjadi pilar penting yang dapat digunakan sebagai referensi untuk mengevaluasi dan memperkuat SiAP:

COSO Internal Control – Integrated Framework, yang memberikan struktur pengendalian internal komprehensif untuk menjamin bahwa proses organisasi berjalan secara terkendali, terdokumentasi, dan terukur. Kerangka ini menekankan pentingnya lingkungan pengendalian, penilaian risiko, aktivitas pengendalian, komunikasi informasi, dan monitoring berkelanjutan.

COBIT 2019, sebagai standar emas dalam tata kelola teknologi informasi, menyediakan prinsip-prinsip menyeluruh untuk menilai apakah TI telah dikelola secara efektif, aman, dan sejalan dengan tujuan organisasi. COBIT fokus pada pengelolaan risiko TI, perencanaan strategis, pengembangan sistem, manajemen layanan, dan mekanisme evaluasi TI.

ITIL 4, yang memberikan pendekatan sistematis dalam manajemen layanan TI, meliputi pengelolaan insiden, penanganan masalah, perubahan sistem, kontinuitas layanan, dan perbaikan berkelanjutan. ITIL memastikan bahwa sistem seperti SiAP tidak hanya berjalan baik, tetapi didukung oleh layanan TI yang responsif dan stabil.

Ketiga kerangka tersebut memiliki titik temu yang sangat kuat: semuanya bertujuan memastikan bahwa proses pemeriksaan digital berjalan dengan tingkat kendali, keandalan, dan kualitas yang maksimal. Karena itu, penelitian ini berupaya mengkaji SiAP dari tiga perspektif sekaligus, menganalisis tingkat kesesuaiannya, mengidentifikasi kesenjangan, serta menyusun model integratif yang dapat dijadikan acuan BPK RI untuk memperkuat tata kelola pemeriksaan digital secara menyeluruh.

Pendekatan integratif ini penting karena pemeriksaan masa depan membutuhkan bukan hanya sistem yang berfungsi, tetapi sistem yang dikelola, diawasi, dan dilayani secara profesional. Dengan menggabungkan COSO, COBIT 2019, dan ITIL, penelitian ini berkontribusi pada upaya BPK untuk membangun ekosistem pemeriksaan negara yang adaptif, akuntabel, dan berketahanan tinggi terhadap tantangan digital yang terus berkembang.

II. RELATED WORK

Kajian mengenai tata kelola pemeriksaan digital dan kerangka pengendalian internal telah berkembang pesat seiring meningkatnya digitalisasi proses pemeriksaan di berbagai negara. Perpaduan antara pengendalian internal, tata kelola TI, dan manajemen layanan TI menjadi semakin penting, terutama ketika lembaga pemeriksa negara mulai mengandalkan sistem aplikasi terintegrasi seperti Sistem Aplikasi Pemeriksaan (SiAP). Bagian ini mengulas studi-studi relevan terkait COSO, COBIT 2019, dan ITIL 4, serta mengidentifikasi kekosongan penelitian yang melandasi urgensi penelitian ini..

A. COSO

Kerangka COSO Internal Control – Integrated Framework banyak digunakan dalam organisasi sektor publik dan lembaga pemeriksa negara untuk menilai efektivitas pengendalian internal. COSO berfokus pada lima komponen utama, yaitu:

a. Lingkungan Pengendalian,
b. Penilaian Risiko,
c. Aktivitas Pengendalian,
d. Informasi dan Komunikasi,
e. Kegiatan Monitoring.

Literatur menunjukkan bahwa COSO telah digunakan secara luas dalam audit pemerintahan untuk meningkatkan integritas proses pemeriksaan, memperbaiki kualitas dokumentasi, dan memastikan konsistensi antara prosedur pemeriksaan dan implementasinya di lapangan. COSO juga dianggap efektif dalam memperkuat akuntabilitas karena menekankan dokumentasi yang jelas dan standar pengendalian proses yang ketat.

Dalam konteks SiAP, COSO sangat relevan karena platform ini dirancang sebagai sistem dokumentasi dan pengendalian proses pemeriksaan yang memerlukan kepastian bahwa setiap langkah audit terdokumentasi, tervalidasi, dan dapat ditelusuri. Dengan kata lain, COSO memberikan fondasi yang kuat bagi aspek audit process governance yang dilakukan melalui SiAP..

B. COBIT

COBIT 2019 merupakan kerangka yang banyak digunakan untuk tata kelola dan manajemen teknologi informasi. COBIT memberikan struktur dan pedoman yang komprehensif bagi organisasi untuk memastikan bahwa teknologi mendukung tujuan organisasi secara efektif dan aman. Berbagai penelitian menunjukkan bahwa penerapan COBIT dapat:

a. meningkatkan keselarasan antara tujuan TI dan tujuan strategis organisasi,
b. memperkuat pengelolaan risiko TI,
c. meningkatkan kualitas layanan TI melalui mekanisme kontrol yang jelas,
d. memperbaiki integritas dan keamanan sistem digital, termasuk sistem audit.

COBIT 2019 terdiri atas lima domain:

a. EDM (Evaluate, Direct and Monitor),
b. APO (Align, Plan and Organize),
c. BAI (Build, Acquire and Implement),
d. DSS (Deliver, Service and Support),
e. MEA (Monitor, Evaluate and Assess).

Kelima domain ini memiliki relevansi yang tinggi untuk SiAP, terutama mengingat karakter SiAP sebagai aplikasi audit yang membutuhkan pengelolaan risiko TI, pengembangan sistem yang berkelanjutan, mekanisme layanan TI yang kuat, serta

pengawasan terhadap kinerja aplikasi secara rutin. Oleh karena itu, COBIT memberikan kerangka logis untuk mengevaluasi bagaimana SiAP dikelola dari sisi tata kelola teknologi..

C. ITIL

ITIL 4 (Information Technology Infrastructure Library) merupakan standar global yang digunakan dalam pengelolaan layanan TI (IT Service Management). Literatur menunjukkan bahwa ITIL mampu meningkatkan kualitas layanan TI melalui fokus pada stabilitas operasional, respons terhadap insiden, perubahan yang terkontrol, dan peningkatan berkelanjutan. ITIL 4 memberikan pendekatan praktis bagi organisasi untuk memastikan bahwa sistem TI:

- tetap tersedia (availability),
- dapat diandalkan (reliability),
- pulih dengan cepat dari gangguan (resilience),
- dan mendukung tujuan organisasi melalui layanan yang stabil.

Praktik-praktik ITIL yang paling relevan berdampak langsung pada efektivitas SiAP antara lain:

a. Incident Management, untuk memastikan gangguan SiAP dapat ditangani cepat;
b. Problem Management, untuk mengidentifikasi akar penyebab gangguan;
c. Change Enablement, untuk memastikan pembaruan SiAP tidak menimbulkan risiko baru;
d. Service Continuity, untuk menjamin keberlangsungan layanan SiAP;
e. Service Desk, untuk menyediakan dukungan teknis bagi pemeriksa;
f. Continual Improvement, untuk menyempurnakan SiAP secara berkelanjutan.

Tanpa penerapan ITIL, sistem seperti SiAP rentan terhadap gangguan teknis dan keterlambatan penanganan masalah, yang berdampak langsung pada kualitas pemeriksaan..

D. Gap Literatur

Walaupun COSO, COBIT 2019, dan ITIL telah banyak dibahas dalam literatur, terdapat kekosongan signifikan dalam penelitian yang menggabungkan ketiganya secara komprehensif pada konteks sistem pemeriksaan di lembaga pemeriksa negara.

Studi terdahulu umumnya hanya berfokus pada:

a. COSO untuk pengendalian internal audit, atau
b. COBIT untuk tata kelola TI, atau
c. ITIL untuk layanan TI.

Sangat sedikit penelitian yang mengkaji hubungan langsung antara pengendalian internal, tata kelola TI, dan manajemen layanan TI dalam sistem audit pemerintahan seperti SiAP. Padahal, pemeriksaan digital modern memerlukan ketiga aspek tersebut bekerja secara simultan.

Oleh karena itu, penelitian ini hadir untuk mengisi kesenjangan literatur tersebut dengan:

- menganalisis SiAP berdasarkan COSO, COBIT, dan ITIL,
- menilai tingkat keselarasan dan kesenjangan yang ada,
- serta mengusulkan model tata kelola pemeriksaan digital terintegrasi yang menyatukan ketiga kerangka kerja tersebut.

Model semacam ini belum banyak ditemukan dalam publikasi ilmiah sebelumnya, sehingga memberikan kontribusi baru bagi pengembangan ilmu audit digital, tata kelola sistem pemerintahan, serta pelayanan TI dalam lembaga pemeriksa negara..

III. METHODOLOGY

Penelitian ini menggunakan pendekatan analitis–komparatif untuk menilai kesesuaian Sistem Aplikasi Pemeriksaan (SiAP) dengan tiga kerangka internasional: COSO, COBIT 2019, dan ITIL 4. Pendekatan ini dipilih karena memungkinkan peneliti melakukan eksplorasi mendalam atas hubungan antara proses pemeriksaan, tata kelola teknologi informasi, dan manajemen layanan TI dalam satu sistem digital terintegrasi. Secara keseluruhan, metodologi penelitian terdiri dari empat tahapan utama sebagai berikut.:

1. Analisis Dokumen

Tahap pertama dilakukan melalui telaah komprehensif terhadap berbagai dokumen teknis dan pedoman internasional yang menjadi sumber utama dalam penelitian ini. Analisis dokumen memberikan fondasi teoritis dan operasional untuk memahami:

- struktur dan komponen pengendalian internal menurut COSO Internal Control Framework,
- domain tata kelola TI menurut COBIT 2019 Governance & Management Objectives,
- praktik manajemen layanan TI menurut ITIL 4 Service Value System,
- struktur peran pemeriksa, alur kerja pemeriksaan, validasi KKP, serta mekanisme sinkronisasi data berdasarkan Manual SiAP Bagian 1–4 dan Panduan SiAP Web 2022.

Langkah ini memastikan bahwa seluruh kerangka dikaji berdasarkan sumber rujukan resmi, sehingga pemetaan dan analisis dapat dilakukan secara objektif, konsisten, dan metodologis.

2. Conceptual Mapping

Tahap kedua dilakukan melalui proses pemetaan sistematis untuk menghubungkan konsep dari ketiga kerangka global dengan fitur dan alur kerja dalam SiAP. Pemetaan ini mencocokkan:

a. Komponen COSO, seperti lingkungan pengendalian, aktivitas pengendalian, serta monitoring,

b. Domain COBIT 2019, seperti EDM, APO, BAI, DSS, dan MEA,

c. Praktik ITIL, seperti incident management, service desk, change enablement, dan service continuity,

dengan fitur operasional SiAP, termasuk:

- penyusunan dan penyimpanan Kertas Kerja Pemeriksaan (KKP),
- penyusunan Program Kerja Pemeriksaan (PKP),
- workflow validasi berlapis (Anggota Tim → Ketua Tim → Pengendali Teknis),
- manajemen tim pemeriksaan dan pembagian tugas,
- mekanisme sinkronisasi data antara SiAP Web dan SiAP Desktop,
- monitoring progres pemeriksaan, dashboard, dan audit trail.

Melalui metode pemetaan ini, peneliti dapat mengidentifikasi kesesuaian langsung, kesesuaian parsial, atau ketidaksesuaian antara praktik ideal dalam standar internasional dan implementasi nyata SiAP..

3. Gap Analysis

Tahap ketiga adalah evaluasi kesenjangan (gap analysis) yang bertujuan mengukur tingkat keselarasan dan kekurangan SiAP dibandingkan dengan ketiga kerangka internasional. Analisis ini menilai:

a. sejauh mana SiAP memenuhi prinsip pengendalian internal versi COSO,

b. sejauh mana SiAP selaras dengan tata kelola TI versi COBIT 2019,

c. dan sejauh mana layanan TI SiAP dikelola berdasarkan praktik ITIL 4.

Untuk memberikan struktur penilaian yang jelas dan dapat direplikasi, kesenjangan dikategorikan menjadi tiga tingkatan:

- Rendah – apabila SiAP hampir sepenuhnya memenuhi standar, hanya terdapat kekurangan minor.
- Sedang – apabila terdapat beberapa elemen yang terpenuhi, tetapi masih ada aspek yang perlu diperbaiki.
- Tinggi – apabila standar tidak terpenuhi, atau belum ada mekanisme yang seharusnya tersedia dalam sistem.

Gap analysis ini sangat penting karena memungkinkan penelitian mengidentifikasi area yang menjadi kekuatan SiAP, sekaligus area yang memerlukan penguatan pada aspek risiko TI, layanan TI, dan pengendalian internal digital..

4. Model Integrasi

Tahap terakhir adalah perumusan model integratif COSO–COBIT–ITIL–SiAP, yang disusun sebagai kerangka konseptual tata kelola pemeriksaan digital. Model ini dikembangkan berdasarkan temuan pemetaan dan gap analysis, sehingga mampu:

- menyatukan pengendalian proses audit (COSO),
- tata kelola teknologi informasi (COBIT 2019),
- serta manajemen layanan TI (ITIL 4),

ke dalam arsitektur pemeriksaan digital SiAP.

Model integratif ini berfungsi sebagai:

a. rekomendasi akademis untuk penguatan sistem SiAP,
b. panduan praktis bagi BPK RI dalam meningkatkan maturitas tata kelola pemeriksaan digital,
c. serta rujukan konseptual untuk penelitian-penelitian lanjutan.

Melalui pendekatan empat tahap ini, penelitian menghasilkan analisis yang mendalam, terstruktur, dan mampu menggambarkan keterkaitan sistem pemeriksaan digital dengan kerangka tata kelola internasional..

IV. RESULTS AND DISCUSSION

Hasil analisis menunjukkan bahwa Sistem Aplikasi Pemeriksaan (SiAP) telah mencapai kemajuan signifikan sebagai platform pengelolaan proses pemeriksaan digital. Namun, kesesuaian SiAP terhadap tiga kerangka internasional—COSO, COBIT 2019, dan ITIL 4—menampilkan pola yang tidak merata. Secara umum, SiAP sangat kuat pada aspek pengendalian proses audit, tetapi masih memiliki kelemahan pada dimensi tata kelola TI dan manajemen layanan TI. Temuan ini dijabarkan secara sistematis sebagai berikut..

A. Keselarasan SiAP dengan COSO

Kerangka COSO sangat relevan bagi SiAP karena fokus utama COSO adalah memastikan proses organisasi berjalan secara terkendali, terdokumentasi, dan dapat diawasi. Penilaian menunjukkan:

1. Sangat kuat

SiAP menunjukkan keselarasan yang tinggi dengan komponen COSO, terutama pada:

- Aktivitas pengendalian, melalui validasi berjenjang (AT → KT → PT) yang memastikan kualitas dan akurasi KKP.
- Monitoring, melalui audit trail otomatis, riwayat revisi, dan panel monitoring yang memungkinkan pengawasan progres pemeriksaan secara real time.
- Alur validasi, yang memastikan setiap langkah pemeriksaan diawasi oleh jenjang yang lebih tinggi.

2. Cukup Baik

- Informasi & komunikasi, terutama melalui dashboard informasi yang mendukung alur komunikasi internal antaranggota tim pemeriksa.
- Notifikasi dan struktur dokumen di SiAP membantu menjaga konsistensi dan kelancaran arus informasi.

3. Lemah

- Penilaian risiko TI (IT Risk Assessment) belum tertanam dalam mekanisme SiAP.
- Budaya risiko digital (digital risk culture) belum sepenuhnya menjadi bagian dari alur kerja pemeriksaan.
- Fokus SiAP masih pada risiko pemeriksaan substantif, bukan risiko sistem atau teknologi.

SiAP telah menjadi platform yang sangat kuat dalam mendukung internal control proses audit, tetapi belum menyentuh dimensi risiko eksternal dan risiko teknologi yang kini menjadi bagian penting dari pengendalian internal modern

B. Keselarasan SiAP dengan COBIT 2019

COBIT 2019 memandang tata kelola TI secara menyeluruh mencakup strategi, risiko, layanan, dan keberlanjutan sistem. Penilaian menunjukkan:

1. Kuat pada domain APO

   a. SiAP mendukung Align, Plan, Organize dengan baik melalui struktur peran, perencanaan audit, pembagian tugas yang terkontrol, dan workflow yang jelas.

   b. Domain APO selaras dengan karakter operasional SiAP yang mengatur banyak aspek organisasi audit.

2. Sedang pada domain MEA

   c. SiAP menyediakan monitoring progres pemeriksaan yang komprehensif.

   d. Namun, MEA (Monitor, Evaluate, Assess) dalam konteks TI—misalnya monitoring performa server, keandalan layanan, atau pemenuhan SLA—belum ada.

3. Lemah pada domain EDM, BAI, dan DSS

   a. EDM (Evaluate, Direct, Monitor) – Governance Level

      - Belum memiliki SLA TI formal.
      - Arah strategis layanan TI belum terstandarisasi.
      - Tidak ada KPI layanan yang mengikat manajemen.

      Tanpa SLA, kualitas layanan TI tidak dapat diukur, tidak dapat dievaluasi, dan tidak dapat dipertanggungjawabkan.

   b. BAI (Build, Acquire, Implement) – Pengembangan Sistem

      - Tidak ada dokumentasi SDLC (System Development Life Cycle).

- Tidak ada Change Management.
- Tidak ada catatan versi, rencana rilis, atau pengujian formal.

Setiap pembaruan SiAP berpotensi menimbulkan bug, error, dan inkonsistensi karena tidak ada kontrol perubahan yang terdokumentas

c. DSS (Deliver, Service, Support) – Layanan TI

- Tidak ada ticketing system.
- Tidak ada DRP (Disaster Recovery Plan) / BCP (Business Continuity Plan).
- Tidak ada Service Desk formal.

Gangguan SiAP tidak dapat ditangani secara sistematis. Risiko kehilangan data & downtime meningkat.

SiAP berhasil mendigitalisasi proses audit, tetapi belum memiliki tata kelola TI yang matang. Penguatan EDM–BAI–DSS sangat diperlukan agar SiAP lebih andal, aman, dan berkelanjutan

C. Keselarasan SiAP dengan ITIL

Kerangka ITIL 4 menekankan pentingnya pengelolaan layanan TI (IT Service Management) yang stabil, terukur, responsif, dan berkelanjutan. ITIL tidak hanya berbicara tentang keberfungsian sistem, tetapi juga tentang bagaimana layanan TI diberikan kepada pengguna—dalam konteks BPK, pengguna tersebut adalah para pemeriksa yang mengandalkan SiAP sebagai alat utama dokumentasi dan kendali pemeriksaan.

Hasil analisis menunjukkan bahwa keselarasan SiAP dengan ITIL masih bersifat parsial dan belum mencapai tingkat maturitas yang dibutuhkan untuk mendukung ekosistem pemeriksaan digital yang kompleks

1. Aspek yang sebagian terpenuhi

SiAP telah mengimplementasikan mekanisme Single Sign-On (SSO) serta memanfaatkan VPN untuk akses jaringan internal, disertai pembatasan hak akses berdasarkan peran (Tortama/Kalan, Pengendali Teknis, Ketua Tim, Anggota Tim). Dari perspektif ITIL, hal ini mencerminkan implementasi elemen Information Security Management, yaitu pengamanan akses yang mendukung integritas dan kerahasiaan data pemeriksaan. Hal ini menunjukkan bahwa aspek keamanan akses termasuk dalam prioritas desain SiAP. Meskipun belum masuk dalam layanan TI tingkat lanjut, pengaturan akses yang kuat merupakan fondasi penting bagi keberlanjutan layanan

2. Aspek yang kurang atau belum tersedia

a. Tidak tersedia sistem ticketing insiden

SiAP belum memiliki sistem ticketing insiden TI yang terintegrasi. Pengguna yang mengalami gangguan—seperti gagal sinkronisasi, aplikasi tidak dapat dibuka, atau error saat validasi—tidak memiliki kanal resmi untuk:

- melaporkan masalah,
- mendapatkan nomor tiket,
- memantau progres penyelesaian insiden,
- atau memastikan kapan layanan kembali pulih

b. Tidak ada Disaster Recovery Plan (DRP) atau Business Continuity Plan (BCP).

   Dalam ITIL, Service Continuity Management merupakan praktik wajib bagi sistem yang mendukung proses inti organisasi. Tanpa DRP/BCP:

   - SiAP tidak memiliki rencana pemulihan layanan saat terjadi bencana,
   - tidak ada skenario failover,
   - tidak ada simulasi pemulihan layanan,
   - tidak ada dokumentasi prioritas layanan kritis.

   Ini merupakan risiko besar karena SiAP adalah sistem yang masuk kategori mission-critical.

c. Belum tersedia service desk formal yang berfungsi sebagai titik tunggal laporan masalah dan permintaan layanan TI.

Secara keseluruhan, SiAP memiliki arsitektur proses audit yang kuat, namun fondasi layanan TI-nya belum mendukung kebutuhan operasional pemeriksaan digital secara berkelanjutan. Tanpa penerapan praktik ITIL seperti incident management, service continuity, DRP/BCP, dan service desk, SiAP akan terus menghadapi risiko:

- downtime tak terduga,
- layanan tidak responsif,
- kesulitan pengendalian risiko operasional,
- dan potensi kegagalan layanan yang berdampak luas pada pekerjaan pemeriksa.

D. Interpretasi Akademis

Secara umum, temuan penelitian menunjukkan pola yang konsisten:

1. SiAP berhasil mendigitalisasi proses pemeriksaan, menjadikan proses lebih terkontrol, terdokumentasi, dan responsif terhadap kebutuhan kerja pemeriksa.
2. Namun SiAP belum sepenuhnya mendigitalkan tata kelola TI dan layanan TI.
3. Kekuatan SiAP terletak pada audit process governance (sejalan dengan COSO), tetapi kelemahannya terdapat pada IT governance (COBIT) dan IT service management (ITIL).
4. Ketidakseimbangan antara digitalisasi proses dan digitalisasi tata kelola menciptakan risiko sistemik, antara lain:
   - risiko downtime,
   - risiko kehilangan data,

- risiko sinkronisasi,
- risiko keamanan siber,
- dan risiko ketergantungan teknologi tanpa mekanisme mitigasi.

Temuan ini menunjukkan bahwa modernisasi pemeriksaan tidak cukup hanya dengan menyediakan platform digital. Tata kelola TI dan layanan TI yang kuat harus ditanamkan agar SiAP dapat berfungsi sebagai sistem pemeriksaan negara yang kuat, berkelanjutan, dan tahan risiko dalam jangka panjang..

V. PROPOSED MODEL INTEGRATIF COSO–COBIT–ITIL–SiAP

Hasil analisis menunjukkan bahwa SiAP telah berhasil menyatukan proses pemeriksaan dalam satu platform digital, namun belum memiliki struktur tata kelola TI dan layanan TI yang memadai. Untuk mengatasi ketidakseimbangan tersebut, penelitian ini mengusulkan model tata kelola pemeriksaan digital terintegrasi yang menggabungkan tiga kerangka internasional—COSO, COBIT 2019, dan ITIL 4—ke dalam arsitektur operasional SiAP.

Model ini tidak hanya berfungsi sebagai peta konseptual, tetapi juga sebagai governance blueprint yang dapat diterapkan oleh BPK RI untuk membangun ekosistem pemeriksaan digital yang andal, aman, dan berkelanjutan.

A. Prinsip Dasar Pengembangan Model

Model integratif ini dibangun berdasarkan tiga prinsip:

1. Complementarity (Saling Melengkapi)

COSO, COBIT, dan ITIL memiliki kekuatan unik:

- COSO → mengendalikan proses audit internal.
- COBIT → mengendalikan tata kelola TI dan manajemen risiko teknologi.
- ITIL → menjamin kualitas layanan TI yang mendukung aplikasi.

Karena ketiganya fokus pada aspek yang berbeda, integrasi mereka memberikan lingkup kontrol yang komprehensif.

2. Interoperability (Keterhubungan Antar-Kerangka)

Model ini memastikan bahwa komponen COSO dapat diterjemahkan ke dalam aktivitas COBIT, dan praktik ITIL dapat mendukung kebutuhan teknis SiAP.

3. Feasibility (Dapat Diimplementasikan)

Model dirancang agar realistis dan dapat diterapkan secara bertahap sesuai kapasitas organisasi BPK RI.

B. Struktur Model Tiga Lapisan (Three-Layer Architecture)

Model integratif diusulkan sebagai arsitektur tiga lapisan (three-layer governance structure), yang saling terkait namun memiliki fungsi berbeda.

1) Lapisan COSO (Process Governance Layer)

Lapisan ini berfungsi sebagai fondasi dalam mengendalikan proses pemeriksaan. COSO memberikan struktur agar aktivitas pemeriksaan berjalan secara:

- terkontrol,
- terdokumentasi,
- konsisten,
- dapat direviu.

Komponen COSO yang Dihubungkan dengan SiAP

a. Control Environment
    - Pembagian peran (Tortama/Kalan, PT, KT, AT).
    - Kebijakan integritas dan akuntabilitas digital.

b. Risk Assessment
    - Risiko pemeriksaan.
    - Perluasan ke risiko TI—yang belum tersedia di SiAP.

c. Control Activities
    - Validasi berlapis, audit trail, pembatasan akses.

d. Information & Communication
    - Dashboard, notifikasi, struktur dokumen audit.

e. Monitoring
    - Supervisi berjenjang, progres pemeriksaan, rekam jejak perubahan.

Peran COSO dalam model:

Menjamin bahwa proses pemeriksaan digital dapat dipercaya, terstandardisasi, dan memenuhi prinsip akuntabilitas publik..

2) Lapisan COBIT 2019 (IT Governance Layer)

COBIT memberikan kerangka tata kelola TI untuk memastikan bahwa sistem seperti SiAP:

- dikelola secara strategis,
- memiliki kontrol risiko TI,
- memiliki pengembangan sistem yang terstruktur,
- dan memenuhi standar keamanan modern.

Keterhubungan COBIT–SiAP

a. EDM: Pemantauan risiko TI, KPI layanan, kinerja aplikasi.

b. APO: Perencanaan TI selaras strategi pemeriksaan.

c. BAI: Pengendalian perubahan, SDLC, dokumentasi pengembangan.

d. DSS: Pengelolaan insiden, keamanan, pemulihan layanan.

e. MEA: Evaluasi performa TI, kepatuhan TI.

Peran COBIT dalam model:

Mengendalikan tulang punggung teknis SiAP agar sistem audit berjalan stabil, aman, dan strategis..

3) Lapisan ITIL 4 (IT Service Management Layer)

ITIL memperkuat kualitas operasional layanan TI yang menopang SiAP.

Komponen ITIL yang Dikaitkan dengan SiAP

a. Incident Management: Penyelesaian cepat gangguan SiAP.
b. Problem Management: Menyelesaikan akar masalah berulang.
c. Change Enablement: Pembaruan sistem yang terkontrol.
d. Service Continuity: DRP/BCP untuk menjaga keberlangsungan layanan.
e. Service Desk: Titik layanan tunggal untuk pemeriksa BPK.
f. Continual Improvement: Pembaruan berkelanjutan untuk SiAP.

Peran ITIL dalam model:

Menjamin layanan SiAP berjalan tanpa gangguan dan responsif terhadap masalah.

4) Lapisan Operasional SiAP (Application Layer)

SiAP menjadi jembatan antara tata kelola audit (COSO), tata kelola TI (COBIT), dan layanan TI (ITIL).

Model menempatkan SiAP sebagai:

- alat kontrol,
- alat dokumentasi,
- alat koordinasi,
- dan alat monitoring pemeriksaan digital.

Dengan integrasi model ini, SiAP tidak hanya menjadi aplikasi teknis, tetapi naik kelas menjadi platform governance bagi seluruh proses pemeriksaan negara.

C. Interaksi Antar-Lapisan (Interlayer Interaction)

Interaksi antar-lapisan dalam model integratif COSO–COBIT–ITIL–SiAP merupakan inti dari desain tata kelola pemeriksaan digital yang modern. Ketiga kerangka tersebut tidak berdiri sendiri, karena masing-masing memainkan peran berbeda dalam memastikan bahwa proses audit digital bukan hanya dilakukan, tetapi juga dipastikan, diawasi, dan dilayani dengan standar profesional yang tinggi.

Dalam konteks ini, SiAP menjadi titik temu (convergence point) tempat ketiga kerangka tersebut bertemu, berinteraksi, dan saling memperkuat.

1. COSO → SiAP

COSO memberikan fondasi dasar untuk mengatur bagaimana proses audit harus dijalankan. Kontribusinya terhadap SiAP bersifat sangat operasional—berada pada level aktivitas pemeriksaan sehari-hari.

a. Alur Validasi

Validasi berjenjang (Anggota Tim → Ketua Tim → Pengendali Teknis) bukan sekadar rutinitas prosedural. Dalam perspektif COSO, validasi adalah control activity, yaitu mekanisme untuk memastikan bahwa setiap langkah pemeriksaan:

- sesuai standar,
- bebas dari kesalahan yang dapat dihindari,
- melewati pengawasan struktural,
- dan dapat dipertanggungjawabkan.

Melalui SiAP, alur validasi ini tidak hanya terdokumentasi, tetapi juga tertib, terpantau, dan terjaga integritasnya.

b. Dokumentasi KKP

Dokumentasi Kertas Kerja Pemeriksaan menjadi esensi dari pemeriksaan yang akuntabel. COSO menekankan bahwa dokumentasi harus:

- lengkap,
- akurat,
- konsisten,
- dan dapat ditelusuri (traceable).

SiAP membuat hal ini menjadi mungkin dengan menghilangkan risiko kehilangan dokumen fisik, memastikan versi dokumen terkontrol, dan menyediakan audit trail otomatis. Dengan demikian, SiAP bukan hanya mencatat, tetapi juga membuktikan bahwa proses audit berlangsung sebagaimana mestinya.

c. Supervisi Berjenjang

Pengawasan oleh Ketua Tim dan Pengendali Teknis adalah manifestasi dari komponen COSO Monitoring Activities. SiAP memfasilitasi pengawasan yang:

- tidak bergantung pada pertemuan fisik,
- dapat dilihat real-time,
- tercatat dalam sistem,
- dan memiliki bukti digital yang objektif.

Interaksi COSO→SiAP menunjukkan bahwa SiAP berfungsi sebagai alat bantu disiplin proses audit yang memastikan prosedur berjalan “terlihat” dan tidak sekadar dilakukan

2. COBIT → SiAP

Jika COSO mengatur proses, COBIT mengatur sistem yang menjalankan proses tersebut. COBIT bekerja pada level strategis dan teknologi.

a. Manajemen Risiko TI

COBIT memberikan struktur agar risiko terhadap SiAP—misalnya kegagalan sinkronisasi, serangan siber, downtime, atau korupsi data—dapat:

- diidentifikasi,
- dinilai dampaknya,
- dikendalikan,
- dan dimitigasi.

Tanpa COBIT, SiAP berfungsi sebagai alat, tetapi tidak memiliki strategi perlindungan.

b. Siklus Pengembangan Sistem (SDLC)

COBIT mengatur bagaimana SiAP harus:

- dirancang,
- diuji,
- diperbarui,
- dievaluasi,
- dan dikelola secara berkelanjutan.

Dengan kata lain, COBIT menekankan bahwa aplikasi bukan barang sekali jadi. SiAP harus memiliki life cycle yang terencana, terdokumentasi, dan dapat diprediksi.

c. Keamanan Sistem TI

COBIT mendefinisikan standar keamanan untuk:

- kontrol akses,
- enkripsi data,
- pengelolaan akun pengguna,
- dan perlindungan dari ancaman eksternal.

Interaksi COBIT→SiAP memastikan bahwa platform audit digital tidak hanya berjalan, tetapi juga tangguh, aman, dan berdaya tahan terhadap risiko teknologi..

3. ITIL → SiAP

COBIT mengelola sistemnya, tetapi ITIL mengelola layanan yang disediakan sistem tersebut kepada pengguna, yaitu pemeriksa BPK. Interaksi ini terjadi pada level operasional sehari-hari—di mana kenyamanan, kecepatan, dan keterandalan layanan TI sangat menentukan kelancaran pemeriksaan.

a. Respons Insiden

ITIL memastikan bahwa ketika terjadi gangguan (error, tidak bisa login, gagal sinkron), maka:

a. ada mekanisme pelaporan,

b. ada rekaman insiden,
c. ada SLA penanganan,
d. ada analisis penyebab,
e. ada pemulihan layanan.

Tanpa ITIL, penyelesaian masalah tergantung pada improvisasi, bukan standar layanan.

b. Kontinuitas Layanan

ITIL mengatur service continuity melalui DRP (Disaster Recovery Plan) dan BCP (Business Continuity Plan).

Ini memastikan bahwa SiAP tetap dapat berfungsi saat:

a. server bermasalah,
b. ada pemadaman,
c. terjadi bencana alam,
d. gangguan pusat data.

Ini berdampak langsung pada keberlangsungan pemeriksaan negara.

c. Peningkatan Layanan (Continuous Improvement)

ITIL memberikan prinsip continual improvement yang memastikan bahwa:

a. setiap gangguan menghasilkan pelajaran,
b. setiap keluhan menghasilkan perbaikan,
c. setiap kebutuhan baru direspons dengan peningkatan layanan.

Interaksi ITIL→SiAP menjadikan aplikasi ini bukan hanya perangkat, tetapi layanan yang tumbuh bersama kebutuhan pemeriksa.

Makna Interaksi Tiga Lapisan: Harmonisasi Proses, Teknologi, dan Layanan

Ketika COSO, COBIT, dan ITIL berinteraksi melalui SiAP, sistem pemeriksaan digital menjadi:

1. terkontrol (dikawal COSO),
2. terkelola (dikendalikan COBIT),
3. terlayani dengan baik (didukung ITIL).

Dengan demikian, SiAP bukan hanya aplikasi teknis, tetapi “Platform tata kelola pemeriksaan digital yang hidup, bergerak, dan berkelanjutan.”

Interaksi antar-lapisan ini menciptakan ekosistem pemeriksaan negara yang:

- akuntabel,
- aman,
- stabil,
- adaptif,
- berorientasi pada kualitas jangka panjang.

Model ini memastikan bahwa digitalisasi pemeriksaan bukan sekadar pemindahan dokumen ke aplikasi, melainkan transformasi menyeluruh terhadap cara pemeriksaan negara dikelola dan dilayani..

VI. GAP ANALYSIS

Analisis kesenjangan (gap analysis) dilakukan untuk menilai seberapa jauh Sistem Aplikasi Pemeriksaan (SiAP) memenuhi standar internasional yang ditetapkan oleh COSO, COBIT 2019, dan ITIL 4. Gap analysis ini tidak hanya memetakan perbedaan antara kondisi saat ini dan kondisi ideal, tetapi juga menjelaskan implikasi nyata terhadap kualitas pemeriksaan dan stabilitas sistem digital BPK.

Dengan demikian, hasil analisis ini memberikan gambaran menyeluruh tentang area yang sudah kuat dan area yang perlu mendapatkan prioritas perbaikan dalam rangka memperkuat tata kelola pemeriksaan digital.

A. Gap Analysis: COSO vs SiAP

Tabel berikut menunjukkan kesenjangan antara standar COSO dan implementasi aktual dalam SiAP.

Table 1. COSO–SiAP Gap Analysis

Komponen COSO	Kondisi Ideal (COSO)	Implementasi SiAP	Kesenjangan (Gap)	Severity
Control Environment	Struktur peran, etika digital, budaya risiko	Struktur peran kuat; budaya risiko TI belum jelas	Belum ada kebijakan risiko TI & kompetensi digital	Medium
Risk Assessment	Penilaian risiko menyeluruh, termasuk risiko TI	Penilaian risiko hanya fokus pada audit substantif	Tidak ada modul penilaian risiko TI	High
Control Activities	Kontrol yang terdokumentasi dan konsisten	Validasi berlapis, audit trail, pembatasan akses	Hampir selaras	Low
Information & Communication	Informasi tepat waktu, akurat, terintegrasi	Dashboard, notifikasi tersedia	Integrasi antar-sistem pemeriksaan belum penuh	Medium

Komponen COSO	Kondisi Ideal (COSO)	Implementasi SiAP	Kesenjangan (Gap)	Severity
Monitoring Activities	Pengawasan berkelanjutan termasuk TI	Monitoring audit kuat; monitoring teknologi tidak ada	Tidak ada pemantauan performa TI	Medium

Dari perspektif COSO, SiAP memiliki core strength pada aktivitas pengendalian dan monitoring berjenjang. Ini menandakan bahwa proses pemeriksaan sudah terorganisir dengan baik dan selaras dengan prinsip-prinsip internal control.

Namun, gap terbesar berada pada Risk Assessment, khususnya risiko TI. Tanpa manajemen risiko TI, SiAP berpotensi mengalami gangguan yang dapat berdampak pada integritas proses pemeriksaan.

Gap ini penting karena dalam model COSO modern, risiko teknologi merupakan bagian yang tidak terpisahkan dari lingkungan pengendalian internal organisasi.

B. Gap Analysis: COBIT 2019 vs SiAP

Berikut hasil pemetaan kesenjangan antara COBIT 2019 dan SiAP.

Table 2. COBIT 2019–SiAP Gap Analysis

Domain COBIT	Kondisi Ideal COBIT	Implementasi SiAP	Kesenjangan (Gap)	Severity
EDM (Evaluate, Direct, Monitor)	Tata kelola risiko TI, SLA, KPI layanan	Tidak ada SLA, KPI TI, atau risk governance TI	Governance TI belum formal	High
APO (Align, Plan, Organize)	Strategi dan perencanaan TI selaras tujuan organisasi	Perencanaan pemeriksaan kuat; perencanaan TI tidak terlihat	TI belum sepenuhnya terintegrasi strategi	Medium
BAI (Build, Acquire, Implement)	SDLC terdokumentasi, kontrol perubahan	Tidak ada dokumentasi perubahan atau SDLC	Manajemen perubahan belum ada	High
DSS (Deliver, Service, Support)	Insiden, keamanan, layanan pengguna	Akses aman; tidak ada insiden formal atau DRP	Layanan TI belum terstruktur	High

Domain COBIT	Kondisi Ideal COBIT	Implementasi SiAP	Kesenjangan (Gap)	Severity
MEA (Monitor, Evaluate, Assess)	Evaluasi kinerja TI dan kepatuhan	Monitoring audit ada, monitoring TI tidak	Tidak ada evaluasi performa TI	Medium

COBIT mengevaluasi SiAP dari perspektif TI. Hasilnya jelas:

SiAP unggul sebagai aplikasi pemeriksaan, tetapi belum memenuhi tata kelola TI modern.

Gap paling signifikan berada pada:

a. EDM (risk governance TI) → sistem tidak memiliki pengelolaan risiko TI.
b. BAI (manajemen perubahan) → tidak ada mekanisme kontrol pembaruan.
c. DSS (layanan TI) → belum ada insiden, DRP, BCP, atau helpdesk resmi.

Tanpa unsur COBIT ini, SiAP rentan terhadap risiko operasional seperti:

- kegagalan sinkronisasi,
- downtime,
- ketidaksesuaian versi sistem,
- ancaman keamanan siber.

Dalam konteks lembaga pemeriksa negara, risiko-risiko ini dapat mengancam kredibilitas proses pemeriksaan.

C. Gap Analysis: ITIL 4 vs SiAP

Penilaian berikut menunjukkan gap antara standar ITIL 4 dan layanan TI yang mendukung SiAP.

Table 3. ITIL–SiAP Gap Analysis

Praktik ITIL	Kondisi Ideal ITIL	Implementasi SiAP	Kesenjangan (Gap)	Severity
Incident Management	Pelaporan insiden, respon cepat, SLA	Tidak ada ticketing insiden	Respons insiden tidak terstruktur	High
Problem Management	Identifikasi akar masalah, perbaikan permanen	Tidak terdokumentasi	Risiko masalah berulang tinggi	High
Change Enablement	Kontrol pembaruan sistem	Pembaruan terjadi tapi tidak transparan	Tanpa prosedur formal	Medium

Praktik ITIL	**Kondisi Ideal ITIL**	**Implementasi SiAP**	**Kesenjangan (Gap)**	**Severity**
Service Continuity	DRP/BCP tersedia dan diuji	Tidak ada dokumentasi DRP/BCP	Layanan rentan terhadap bencana	High
Service Desk	Titik layanan tunggal formal	Tidak ada service desk	Dukungan TI tidak terstandarisasi	Medium
Continual Improvement	Perbaikan berkelanjutan	Tidak terdokumentasi secara sistematis	Potensi stagnasi layanan	Medium

ITIL melihat SiAP dari kacamata kualitas layanan TI. Temuannya menunjukkan bahwa SiAP masih sangat minim dalam aspek layanan TI operasional. Padahal bagi pemeriksa, kualitas layanan TI—respons masalah, stabilitas sistem, dan kontinuitas layanan—sama pentingnya dengan fitur aplikasi itu sendiri.

Gap ITIL ini berdampak langsung pada kualitas pemeriksaan, terutama ketika tim pemeriksa menghadapi:

a. error aplikasi di lapangan,
b. sistem tidak dapat diakses,
c. sinkronisasi gagal,
d. kebutuhan dukungan teknis segera.

Tanpa ITIL, pengalaman pengguna SiAP dapat terhambat, meskipun fitur aplikasinya kuat.

D. Analisis Sintesis: Kombinasi Gap dari Tiga Kerangka

Jika ketiga gap analysis digabungkan, pola utamanya adalah:

1. Kekuatan utama SiAP berada pada pengendalian proses audit (konsep COSO).

2. Kelemahan terbesar SiAP berada pada tata kelola TI (COBIT) dan layanan TI (ITIL).

3. Ini menciptakan “asimetri tata kelola” antara proses dan teknologi.

Asimetri ini berpotensi menyebabkan:

- ketergantungan pada aplikasi tanpa mitigasi risiko TI,
- kualitas pemeriksaan yang tidak stabil saat terjadi gangguan sistem,
- ketidakseimbangan antara digitalisasi proses dan digitalisasi governance,
- risiko sistemik yang dapat merusak kredibilitas pemeriksaan.

Ini menjadi dasar urgensi penerapan model integratif COSO–COBIT–ITIL yang telah diusulkan sebelumnya.

VII. CONCLUSION

Penelitian ini menelaah secara komprehensif posisi Sistem Aplikasi Pemeriksaan (SiAP) BPK RI dalam konteks tata kelola pemeriksaan digital dengan membandingkannya terhadap tiga kerangka internasional yang saling melengkapi: COSO (pengendalian internal), COBIT 2019 (tata kelola TI), dan ITIL 4 (manajemen layanan TI).

Secara keseluruhan, hasil penelitian mengungkapkan bahwa SiAP telah mencapai tingkat digitalisasi proses pemeriksaan yang baik, namun belum mencapai tingkat kematangan tata kelola TI dan layanan TI yang dibutuhkan untuk menjamin keberlangsungan pemeriksaan digital secara menyeluruh.

A. Temuan Utama Penelitian

1. SiAP sangat kuat dalam dimensi COSO (internal control process).

   SiAP telah menerapkan prinsip-prinsip COSO secara efektif, terutama pada:

   - aktivitas pengendalian (validasi berlapis, audit trail, pembatasan akses),
   - monitoring pemeriksaan,
   - dan dokumentasi pemeriksaan (KKP, PKP, struktur folder digital).

   SiAP berhasil membuktikan bahwa digitalisasi dapat meningkatkan disiplin, keteraturan, dan akuntabilitas proses pemeriksaan. Dengan kata lain, SiAP telah menjadi tulang punggung pengendalian proses pemeriksaan yang sebelumnya tersebar dalam dokumen fisik.

2. SiAP masih lemah pada dimensi COBIT 2019 (IT governance).

   Penilaian terhadap COBIT 2019 menunjukkan bahwa SiAP masih menghadapi kelemahan struktural pada:

   a. manajemen risiko TI,

   b. manajemen perubahan dan SDLC,

   c. keamanan TI tingkat lanjut,

   d. layanan TI yang harus dimonitor secara sistemik.

   Lemahnya domain EDM, DSS, dan BAI menunjukkan bahwa SiAP belum memiliki tata kelola TI formal yang mendukung keberlanjutan operasi sistem. Ini menunjukkan bahwa digitalisasi proses audit belum dibarengi dengan digitalisasi tata kelola TI yang matang.

3. SiAP sangat minim pada dimensi ITIL 4 (service management).

   SiAP saat ini belum memiliki fondasi layanan TI modern, seperti:

a. ticketing insiden,
b. service desk formal,
c. problem management,
d. disaster recovery planning (DRP) dan business continuity planning (BCP),
e. mekanisme peningkatan layanan berkelanjutan.

Padahal, kualitas pemeriksaan digital sangat dipengaruhi oleh stabilitas dan respons layanan TI. Tanpa ITIL, pemeriksa rentan menghadapi gangguan sistem tanpa dukungan struktural yang memadai.

B. Makna Akademis dan Kontribusi Ilmiah

Penelitian ini memberikan kontribusi baru pada literatur audit digital, tata kelola TI sektor publik, dan manajemen layanan pemerintahan dengan:

1. Menghadirkan model integratif COSO–COBIT–ITIL pertama dalam konteks pemeriksaan keuangan negara.

   Model ini menempatkan SiAP dalam tiga lapisan governance:

   a. governance proses audit (COSO),
   b. governance teknologi (COBIT),
   c. governance layanan TI (ITIL).

2. Mengungkap asimetri governance antara proses audit (sudah matang) dan teknologi audit (belum matang).

   Asimetri ini merupakan temuan penting yang dapat mendorong reformasi tata kelola TI di BPK RI.

3. Menawarkan pendekatan evaluatif baru, yang menghubungkan pengendalian internal audit, pengelolaan teknologi digital, dan kualitas layanan TI dalam satu kajian terpadu.
4. Memberikan dasar terbentuknya kebijakan tata kelola pemeriksaan digital nasional, yang dapat menginspirasi Supreme Audit Institutions (SAIs) di negara lain.

C. Implikasi Praktis bagi BPK RI

Temuan penelitian menunjukkan bahwa BPK perlu:

1. Mengembangkan IT Risk Management formal.
2. Menyusun SLA, OLA, KPI untuk layanan SiAP.
3. Membangun Service Desk dan ticketing system standar.
4. Merancang SDLC yang terdokumentasi untuk setiap versi SiAP.
5. Membentuk Disaster Recovery Plan (DRP) dan Business Continuity Plan (BCP).

6. Menerapkan audit TI internal berkala terhadap SiAP.

Dengan implementasi langkah-langkah tersebut, SiAP dapat berkembang dari sistem pencatatan pemeriksaan menjadi sistem tata kelola pemeriksaan digital yang utuh dan berkelanjutan.

D. Keterbatasan Penelitian

Penelitian ini memiliki keterbatasan:

1. Belum dilakukan pengujian empiris melalui survei pengguna SiAP (auditor dan pemeriksa).
2. Analisis belum mencakup aspek arsitektur teknis SiAP karena terbatasnya dokumen publik.
3. Kajian dilakukan pada dokumentasi, sehingga belum mengevaluasi performa teknis sistem secara langsung.

Keterbatasan ini dapat dijadikan dasar penelitian lanjutan untuk memperoleh gambaran yang lebih holistik.

E. Future Work

Penelitian lanjutan dapat diarahkan pada:

1. Survei empiris pemeriksa BPK untuk mengukur usability dan efektivitas SiAP.
2. Evaluasi teknis performa SiAP (kecepatan, stabilitas, availability).
3. Integrasi SiAP dengan sistem nasional (SIPD, e-Rekon, e-LHP).
4. Pengembangan SiAP Analytics berbasis machine learning untuk deteksi anomali pemeriksaan.
5. Penerapan model integratif ini pada lembaga pemeriksa negara lainnya.
6. Penelitian mendalam tentang keamanan siber SiAP dan mitigasinya.

Dengan demikian, penelitian ini tidak hanya menawarkan rekomendasi konseptual, tetapi juga membuka ruang bagi pengembangan ekosistem

REFERENCES

[1] Monteiro, C. Cepêda, A. C. F. Da Silva, and J. Vale, “The relationship between AI adoption intensity and internal control system and accounting information quality,” Systems, vol. 11, no. 536, pp. 1–17, 2023.

[2] AXELOS, *ITIL 4 Foundation*, 2019.

[3] R. Aditya, R. Hartanto, and L. E. Nugroho, “The role of IT audit in the era of digital transformation,” IOP Conf. Series: Materials Science and Engineering, vol. 407, p. 012164, 2018.

[4] Abrams, J. Karel, B. Miller, P. Pfitzmann, and S. Ruschka-Taylor, “Optimized Enterprise Risk Management,” IBM Systems Journal, vol. 46, no. 2, pp. 219–234, 2007.
[5] COSO, *Internal Control – Integrated Framework,* 2013.
[6] Fayard and N. E. Vincent, “Assessing IT Risks,” Strategic Finance, vol. 99, no. 1, pp. 49–53, Jan. 2018.
[7] Palko et al., “Cyber security risk modeling in distributed information systems,” Applied Sciences, vol. 13, no. 4, p. 2393, 2023.
[8] K. Meçe et al., “Governing IT in HEIs: Systematic Mapping Review,” Business Systems Research, vol. 11, no. 3, pp. 93–109, 2020.
[9] Sutadji, W. N. Hidayat, S. Patmanthara, S. Sulton, N. A. M. Jabari, and M. Irsyad, “Analysis of information technology governance in the planning and organization of e-learning at Universitas Negeri Malang,” IOP Conf. Series: Materials Science and Engineering, vol. 732, 2020.
[10] A. Alali and C.-L. Yeh, “Cloud computing: Overview and risk analysis,” Journal of Information Systems, vol. 26, no. 2, pp. 13–33, 2012.
[11] Simetinger, “Audit and Assurance Specifics in Cloud-Based Industry 4.0 Environment,” Journal of Systems Integration, vol. 9, no. 3, pp. 7–18, 2018.
[12] Burstein and I. Zuckerman, “Deconstructing risk factors for predicting risk assessment in supply chains using machine learning,” Journal of Risk and Financial Management, vol. 16, no. 2, p. 97, 2023.
[13] Mateescu and M. Vlădescu, “Auditing hybrid IT environments,” International Journal of Advanced Computer Science and Applications, vol. 5, no. 3, pp. 1–7, 2014.
[14] G. S. Leite, A. B. Albuquerque, and P. R. Pinheiro, “Application of technological solutions in the fight against money laundering—A systematic literature review,” Applied Sciences, vol. 9, no. 22, p. 4800, 2019.
[15] M. Melaku, “Context-Based and Adaptive Cybersecurity Risk Management Framework,” Risks, vol. 11, no. 101, pp. 1–23, 2023.
[16] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*, 2019.
[17] B. O’Donnell and Y. Rechman, “Navigating the standards for information technology controls,” The CPA Journal, pp. 64–69, Jul. 2005.
[18] L. Rubio Sánchez, “Optimization algorithm to sequence the management processes in information technology departments,” Computation, vol. 9, no. 5, p. 60, 2021.
[19] K. AL-Dosari and N. Fetais, “Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach,” Electronics, vol. 12, no. 17, p. 3629, 2023.
[20] L. Moudoubah, A. El Yamami, M. Khalifa, and M. Qbadou, “A Critical Analysis of IS Governance Frameworks: A Metamodel of the Integrated Use of COBIT Framework,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 9, pp. 203–213, 2020.

[21] M. Krey, S. Furnell, B. Harriehausen, and M. Knoll, “Method engineering approach to the adoption of information technology governance, risk and compliance in Swiss hospitals,” in Proceedings of the European Conference on Information Systems, 2012.
[22] O. Gavilanez, G. Rodriguez, and F. Gavilanez, “Audit Analysis Models, Security Frameworks and Their Relevance for VoIP,” International Journal, pp. 143–153.
[23] O. Matrane and M. Talea, “A maturity model for information security management in small and medium-sized Moroccan enterprises: An empirical investigation,” International Journal of Advanced Research in Computer Science, vol. 5, no. 6, pp. 206–210, 2014.
[24] P. Michelberger and Á. Kemendi, “Data, information and IT security – software support for security activities,” Problems of Management in the 21st Century, vol. 15, no. 2, pp. 108–124, 2020.
[25] P. Solana-González, A. A. Vanti, M. M. García Lorenzo, and R. E. Bello Pérez, “Data mining to assess organizational transparency across technology processes: An approach from IT governance and knowledge management,” Sustainability, vol. 13, no. 18, p. 10130, 2021.
[26] S. A. A. de Freitas, E. D. Canedo, R. C. S. Felisdório, and H. A. T. Leão, “Analysis of the risk management process on the development of the public sector information technology master plan,” Information, vol. 9, no. 10, p. 248, 2018.
[27] S. Ashby, T. Buck, S. Nöth-Zahn, and T. Peisl, “Emerging IT risks: Insights from German banking,” The Geneva Papers on Risk and Insurance, vol. 43, pp. 180–207, 2018.
[28] T. W. Kwan and H. K. N. Leung, “A risk management methodology for project risk dependencies,” IEEE Transactions on Software Engineering, vol. 37, no. 5, pp. 635–648, 2011.
[29] V. Telino, R. Massa, I. Mota, A. Gomes, and F. Moreira, “A methodology for creating a macro action plan to improve IT use and its governance in organizations,” Information, vol. 11, no. 9, p. 427, 2020.
[30] Z. Korachi and B. Bounabat, “Integrated Methodological Framework for Digital Transformation Strategy Building (IMFDS),” International Journal of Advanced Computer Science and Applications, vol. 10, no. 12, pp. 242–251, 2019.