

EVALUASI PENERAPAN *IT GOVERNANCE* DENGAN MENGGUNAKAN KERANGKA KERJA COBIT 5 PADA LAYANAN PUBLIK

¹Ibrahim Ibrahim, ²Rahmat Hidayat

^{1,2}Program Studi Teknik Elektro, Fakultas Teknik, Universitas Singaperbangsa Karawang

ibrahim@ft.unsika.ac.id, rahmat.hidayat@staff.unsika.ac.id

INFO ARTIKEL

Diterima : 18 April 2021

Direvisi : 03 Juli 2021

Disetujui : 07 Juli 2021

Kata Kunci :

COBIT 5, IT Governance, Manajemen Layanan TI, Process Capability Level

ABSTRAK

Penelitian ini bertujuan melakukan evaluasi penerapan *Information Technology (IT) governance* pada institusi sektor layanan publik, dengan menggunakan kerangka kerja COBIT 5. Evaluasi dilakukan untuk memastikan kinerja implementasi layanan teknologi informasi (TI) dapat dirasakan manfaatnya oleh pemangku kepentingan dalam penyediaan informasi yang cepat, akurat, efektif dan efisien untuk mendukung pengambilan keputusan. Metode penelitian menggunakan COBIT 5 pada proses *delivery, service and support (DSS)* dan *process capability model (PCM)*. Pendekatan yang dilakukan berupa studi kasus untuk menilai efektivitas layanan TI yang dijalankan. Hasil penelitian menunjukkan bahwa nilai *process capability level* domain DSS adalah 3,3 (*established*), yakni DSS1=4, DSS2=4, DSS3=4, DSS4=3, DSS5=3 dan DSS6=2. Proses DSS01, DSS02, DSS03 dan DSS04 telah memenuhi target kinerja. Sedangkan proses DSS04, DSS05 dan DSS06 masih dibawah target kinerja sehingga perlu dilakukan perbaikan. Rekomendasi perbaikan secara umum meliputi penyusunan dokumen BCP dan DRP, pengendalian informasi dan data bisnis, audit dan sertifikasi berdasarkan standar sistem manajemen keamanan informasi.

I. PENDAHULUAN

Kinerja Teknologi Informasi (TI) pada sebuah institusi menjadi aspek penting untuk dilakukan dievaluasi dan diukur seiring dengan semakin banyaknya penggunaan dan pemanfaatan TI dalam menjalankan aktivitas bisnis. Kinerja layanan TI akan berdampak langsung pada kinerja kinerja institusi, artinya jika kinerja TI yang digunakan baik maka tentu akan berdampak pada perbaikan kinerja institusi [1].

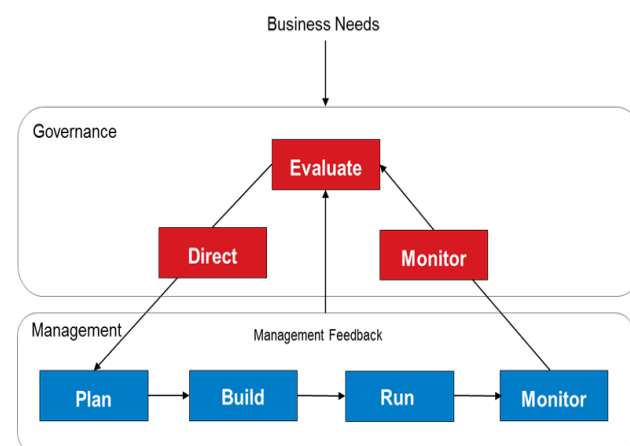
Hal lain yang tak kalah pentingnya untuk dievaluasi dan dimonitor adalah bagaimana memastikan layanan TI lebih baik dan selaras dengan tujuan bisnis [2]. Keselarasan antara layanan TI dengan tujuan bisnis terkadang menjadi masalah dalam investasi TI. Peningkatan investasi TI pada sebuah institusi terkadang tidak berdampak pada meningkatkan kualitas layanan TI [3]. Untuk itu diperlukan pengelolaan TI yang baik untuk memastikan investasi TI berdampak pada meningkatnya kualitas layanan TI yang dihasilkan atau biasa disebut Tata Kelola Teknologi Informasi (*IT Governance*). *IT governance* adalah bagian dari Tata Kelola Perusahaan [4]. Salah satu upaya untuk pengelolaan layanan TI yang baik adalah dengan cara melakukan evaluasi, pengukuran dan pengendalian terhadap proses-proses TI. Penelitian ini difokuskan pada aspek tata kelola atau manajemen layanan TI yang mencakup pengukuran dan pengendalian proses TI sehingga kinerja setiap proses TI terukur dan terkendali baik prosesnya maupun luaran serta dampak yang dihasilkan. Dengan demikian maka layanan TI dapat diprediksi hasil dan dampaknya bagi institusi [5].

A. *IT Governance*

Keberhasilan implemtnasi *IT governance* yang efektif pada sebuah organisasi sangat dipengaruhi oleh sejauhmana organisasi tersebut dapat fokus pengelolaan kerjanya. Sementara kinerja organisasi juga dipengaruhi oleh sejauhmana penerapan TI pada organisasi tersebut. Sedangkan kinerja TI sangat dipengaruhi oleh sejauhmana penerapan tata kelola TI yang baik. Dengan demikian

kinerja organisasi sangat dipengaruhi dan ditunjang oleh sebaikmana penerapan tata kelola TI atau *IT governance* [6]. Tata Kelola TI merupakan tanggung jawab eksekutif dan dewan direksi, dan terdiri dari kepemimpinan, struktur organisasi, dan proses-proses yang memastikan bahwa TI perusahaan menopang dan meningkatkan strategi dan tujuan organisasi [7].

Menurut *IT Governance Institute (ITGI)*, bahwa *IT governance* dapat diterapkan di hampir semua jenis organisasi, tak terkecuali layanan publik. Fokus utama tata kelola TI adalah bagaimana menyelaraskan strategi TI dengan strategi organisasi [8]. Demikian pula dengan pengalokasian sumber daya TI yang efisien dapat membantu organisasi untuk mencapai tujuannya dan organisasi itu dapat melakukan pengukuran kinerja untuk mendapatkan gambaran umum dan menilai sejauh mana organisasi telah mencapai tujuannya [9]. Arsitektur Tata Kelola TI COBIT 5 seperti diperlihatkan pada Gambar 1.



Gambar 1 Arsitektur tata kelola TI COBIT 5 [9]

Berdasarkan definisi diatas maka Komponen utama Tata Kelola TI terdiri dari Struktur Kepemimpinan TI dalam perusahaan, Struktur Organisasi TI serta Proses-

proses TI. Secara ringkas komponen tata kelola diuraikan sebagai berikut.

- a. *Business Needs*, merupakan kebutuhan bisnis sebagai faktor pendorong utama disusunnya tata kelola TI. Pada bagian ini diidentifikasi daftar kebutuhan bisnis yang mencakup visi, misi, tujuan dan sasaran bisnis. Kebutuhan bisnis tersebut kemudian dipetakan atau diterjemahkan kedalam kebutuhan TI atau disebut tujuan TI.
- b. Proses TI, merupakan proses-proses TI yang harus dijalankan untuk mendukung pencapaian tujuan TI yang telah diidentifikasi sebelumnya berdasarkan tujuan bisnis. Proses-proses TI terdiri dari 2 (dua) area yakni area *Governance* dan Manajemen. Area *governance* merupakan domain pimpinan atau kebijakan yang mencakup *evaluate*, *direct* dan *monitor*. Sedangkan domain manajemen merupakan proses-proses pengelolaan yang terdiri dari *plan*, *build*, *run* and *monitor*.

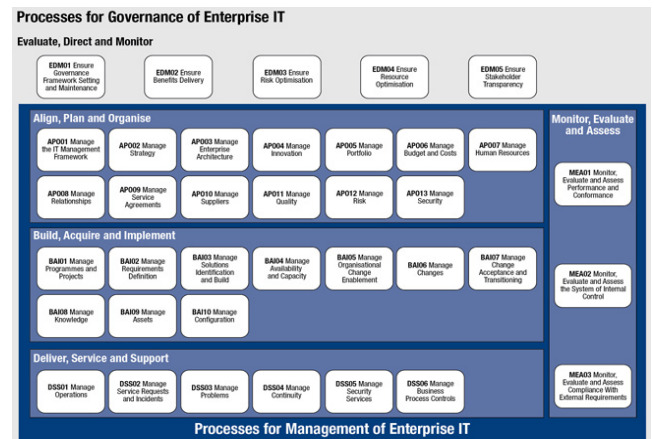
Kerangka kerja *IT Governance* disusun berdasarkan standar ISO 38500 merupakan dasar bagi pengembangan model tata kelola sebagai penjematan untuk menterjemahkan visi, misi, tujuan dan sasaran serta kebijakan organisasi kedalam operasional bisnis yang dapat diukur melalui panduan COBIT 5 yakni proses *Plan, Built, Run, and Monitor* [10].

B. Framework COBIT 5

COBIT (Control Objective for Information and related Technology) merupakan sebuah *framework* yang dikeluarkan oleh *IT Governance Institute* sebagai bagian dari *ISACA (Information Systems Audit and Control Association)*. COBIT 5 merupakan versi terbaru yang diluncurkan sebagai revisi dari edisi sebelumnya. Hal baru yang terdapat pada COBIT 5 yakni mengatur tentang informasi dan teknologi di dalam institusi. Pengaturan terhadap teknologi dan informasi dilakukan secara keseluruhan serta menjabarkan bisnis secara *end-to-end* berdasarkan fungsi dan tanggung jawab dari tata kelola TI dalam menciptakan nilai tambah bagi perusahaan. COBIT 5 juga menyediakan prinsip, praktek, dan *tools* analisis untuk meningkatkan nilai tambah dari TI [11].

Hal lain yang terdapat dalam COBIT 5 selain sebagai kerangka tata kelola dan manajemen TI, juga merupakan kumpulan instrumen yang dapat mendukung dan menjembatani jarak (*gap*) antara kebutuhan pengendalian (*control requirements*), masalah-masalah teknis (*technical issues*) dan resiko bisnis (*business risk*). Selain itu pada COBIT 5 juga dengan tegas dilakukan pemisahan yang sangat jelas antara area *governance* dengan area manajemen. Area *governance* merupakan proses-proses terkait dengan kebijakan-kebijakan, terdiri dari *Evaluate, Direct and Monitor (EDM)*. Sedangkan area manajemen merupakan proses-proses terkait dengan pengelolaan yang terdiri dari domain *Align, Plan and Organize (APO)*, domain *Build, Acquire and Implement (BAI)*, domain *Deliver, Service and Support (DSS)*, dan domain *Monitor, Evaluate and Assess (MEA)*. Secara keseluruhan COBIT 5 terdiri dari 37 proses.

Proses *referensi models* yang terdapat pada COBIT 5 seperti diperlihatkan pada Gambar 2.

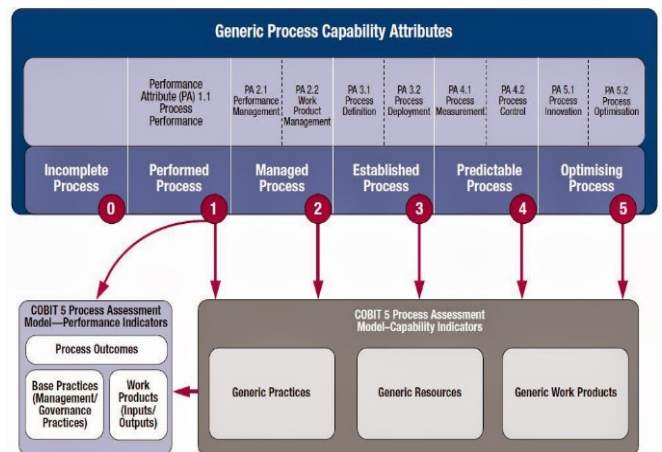


Gambar 2 COBIT 5 process reference models [11]

Kerangka kerja COBIT 5 merupakan sekumpulan dokumen dan panduan untuk implementasi *IT governance* [12]. COBIT 5 membantu para auditor, manajemen dan pengguna dalam menjembatani kesenjangan antara risiko bisnis, kebutuhan dan pengendalian [13].

C. Process Capability Model

Pendekatan yang digunakan pada COBIT 5 dalam pengukuran tingkat kematangan proses TI menggunakan *Process Capability Model* yang diadopsi dari ISO 15504. Model tersebut seperti diperlihatkan pada Gambar 3.



Gambar 3 COBIT 5 process capability models [14]

Deskripsi model *Process Capability Level* COBIT 5 diperlihatkan pada Tabel I.

II. METODE PENELITIAN

A. Pendekatan Penelitian

Pada penelitian ini digunakan pendekatan kualitatif dengan metode studi kasus institusi layanan publik yakni Badan Aksesibilitas Telekomunikasi dan Informasi (BAKTI) Kementerian Komunikasi dan Informatika. Pendekatan ini dimaksudkan untuk mendapatkan pemahaman tentang fenomena penyelenggaraan tata kelola TI melalui kajian,

wawancara dan observasi sesuai kerangka kerja seperti diperlihatkan pada Gambar 4.

TABEL I
MODEL PROCESS CAPABILITY LEVEL COBIT 5 [12]

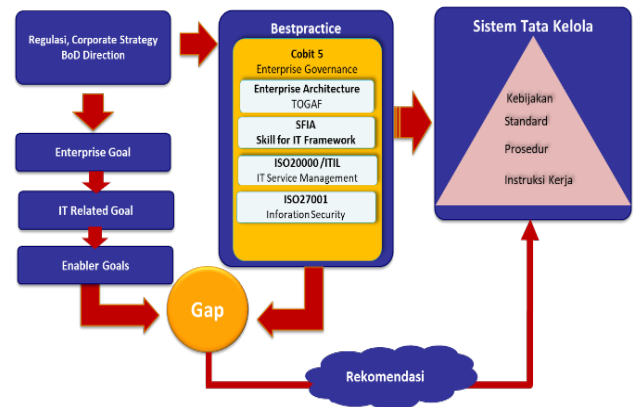
Level	Nilai	Deskripsi
<i>Incomplete</i>	0	Level prosesnya tidak diimplementasikan atau gagal mencapai tujuannya. Pada level ini terdapat sedikit atau tidak ada bukti sistematis pencapaian tujuan dari proses yang dijalankan.
<i>Performed</i>	1	Level proses sudah ada dan diterapkan serta telah menunjukkan tujuan telah tercapai. Proses ini memiliki satu proses atribut yaitu <i>process performance</i> .
<i>Performed</i>	2	Level proses yang dilakukan sekarang telah diimplementasikan dan dikelola (direncanakan, dimonitor dan disesuaikan). Proses ini memiliki dua atribut proses yaitu <i>performance management</i> dan <i>work product management</i> .
<i>Established</i>	3	Level proses telah dikelola, proses diterapkan dan proses dapat dipastikan dapat mencapai <i>outcome</i> . Proses ini memiliki dua atribut proses yaitu <i>process definition</i> dan <i>process deployment</i> .
<i>Predictable</i>	4	Level proses yang ditetapkan telah beroperasi saat ini dipastikan dapat mencapai tujuan dalam jumlah tertentu dan dapat diprediksi. Proses ini memiliki dua atribut proses yaitu <i>process management</i> dan <i>process control</i> .
<i>Optimizing</i>	5	Level proses dapat diprediksi dan dapat dilakukan perbaikan berkelanjutan secara terus menerus untuk memenuhi tujuan bisnis saat ini dan dapat diproyeksikan. Proses ini memiliki dua atribut proses yaitu <i>process innovation</i> dan <i>process optimization</i> .

Pendekatan penyusunan tata kelola TI pada Gambar 4 diuraikan sebagai berikut.

- Kajian regulasi, strategi organisasi dan arahan manajemen. Kegiatan ini dimaksudkan untuk mendapatkan pemahaman tentang aspek regulasi yang harus dipatuhi terkait dengan penyelenggaraan tata kelola TI. Selain itu diperlukan pula pemahaman terhadap strategi organisasi yang mencakup visi, misi tujuan, sasaran, dan indikator kinerja organisasi serta kebijakan-kebijakan yang ada, sebagai dasar dalam penetapan tujuan TI. Demikian pula dengan arahan manajemen atau direksi perlu dipahami sehingga dapat diselaraskan dengan arah pengembangan dan pengelolaan TI.
- Mengidentifikasi *enterprise goals*; kegiatan yang dilakukan pada tahap ini adalah mengidentifikasi seluruh tujuan organisasi berdasarkan regulasi, strategi organisasi menjadi daftar *enterprise goals*. Kegiatan ini dimaksudkan untuk memahami dan menterjemahkan strategi dan kebijakan organisasi

kedalam tujuan yang dapat diimplementasikan dan dicapai.

- Menetapkan *IT related goal*; pada tahap ini dilakukan pendefinisian tujuan TI yang relevan dengan tujuan bisnis yang telah diidentifikasi sebelumnya. Pada bagian ini akan didapatkan daftar tujuan TI yang harus diimplementasikan dan dicapai.

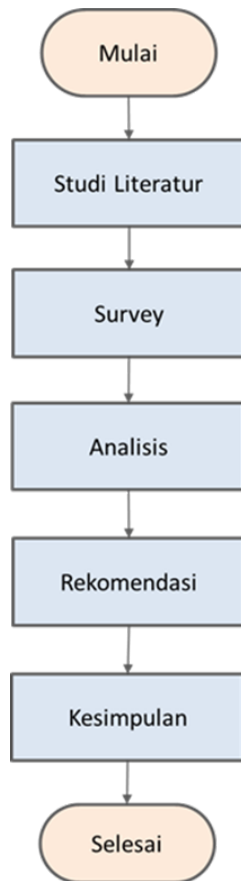


Gambar 4 Pendekatan penyusunan tata kelola TI

- Enabler goal*; pada tahap ini akan diidentifikasi factor penggerak (*enabler*) untuk mencapai tujuan TI. Untuk dapat melaksanakan fungsinya dengan benar, pada COBIT 5 terdapat 7 faktor penggerak, yaitu *Principles, Policies and Framework, Process, struktur organisasi, Culture, Ethics, Behavior, Information, Services, Dan People, Skills, dan Competencies*.
- Melakukan kajian dan mengadopsi *bestpractices* yang relevan dengan topik yang dikaji dalam rangka penyusunan tata kelola TI, antara lain COBIT 5 sebagai *framework* utama, *enterprise architecture*, berbasis TOGAF (*The Open Group Architecture Framework*), SFIA (*Skills Framework for the Information Age*), ISO 20000 (*IT Service Management*), ISO 27001 (*Information Security Management System*). *Framework* tersebut dijadikan sebagai pedukung dalam menyusun dan implementasi tata kelola TI.
- Melakukan analisis kesenjangan (*gap analysis*) antara kondisi penyelenggaraan tata kelola TI saat ini dengan *bestpractice* serta proses-proses TI yang sesuai dengan kebutuhan bisnis untuk diterapkan. Tentu tidak semua *bestpractice* diadopsi namun hanya disesuaikan dengan kebutuhan dan keunikan sebuah organisasi.
- Menyusun sistem tata kelola sebagai kerangka kerja tata kelola untuk diimplementasikan pada organisasi tersebut. Pada kerangka tata kelola ini akan dituangkan dalam bentuk kebijakan, standar, prosedur hingga instruksi kerja, sebagai panduan dalam penyelenggaraan TI.

B. Metode Penelitian

Metode penelitian merupakan alur pikir kegiatan yang dilaksanakan untuk mencapai hasil. Adapun alur kegiatan yang dilakukan pada penelitian ini seperti diperlihatkan pada Gambar 5.



Gambar 5 Alur penelitian

Berdasarkan Gambar 5, alur penelitian diuraikan sebagai berikut.

- Studi literatur, yakni melakukan kajian teoritis terhadap literatur yang mendasari penelitian, baik berupa *text book*, penelitian terdahulu, dokumen bisnis, termasuk hasil audit atau kajian sebelumnya, maupun referensi khususnya terkait dengan tata kelola TI.
- Melakukan *survey* dan wawancara untuk mendapatkan pemahaman kondisi lingkungan bisnis organisasi studi kasus penelitian. Survei mencakup strategi dan tujuan bisnis; kajian terhadap aspek bisnis mulai dari visi, misi, tujuan bisnis dan usaha yang dijalankan. Kegiatan dilakukan dengan cara studi dokumen dan wawancara dengan manajemen institusi, wawancara dengan personil kunci bisnis serta personil TI.
- Melakukan analisis terhadap hasil *survey*. Analisis dilakukan untuk mendapatkan gambaran kondisi penyelenggaraan tata kelola TI yang sedang berjalan saat ini. Selanjutnya dilakukan pengukuran tingkat kematangan atau *process capability* proses-proses TI yang diteliti

dengan menggunakan *COBIT framework*. Selanjutnya hasil analisis dituangkan dalam bentuk potret kondisi saat ini, permasalahan dan kendalanya. Setelah itu dilakukan *setting target* tentang kondisi yang diinginkan oleh institusi. Sumber data yang lain adalah berupa dokumen-dokumen bisnis, dokumen TI serta hasil evaluasi atau audit sebelumnya sebagai bahan perbandingan untuk memperdalam kajian. Instrumen pengukuran yang digunakan berupa kuesioner mengacu pada COBIT 5, *Process Capability Model*. Penilaian *process capability level* dilakukan melalui perhitungan nilai *process capability level* TI dengan menggunakan *tools* yang terdapat pada PCM.

- Menetapkan target yang ingin dicapai berikut rekomendasi langkah perbaikan proses-proses TI yang diperlukan dalam rangka peningkatan nilai *process capability level* proses TI yang diharapkan ke depan. Rekomendasi perbaikan meliputi target nilai *process capability* yang diharapkan untuk dicapai, dan kegiatan-kegiatan yang diperlukan untuk mencapai target tersebut, serta cara mencapainya termasuk teknik pengukuran dan *monitoring* pencapaian.
- Merumuskan kesimpulan hasil penelitian sesuai dengan permasalahan penelitian tujuan dan hasil pengukuran atau pengamatan, yang menggambarkan kondisi penyelenggaraan tata kelola TI saat ini, target pencapaian dan kegiatan perbaikan ke depan.

III. HASIL DAN PEMBAHASAN

Pada bagian ini akan diuraikan mengenai Data hasil dan analisis nilai *process capability* Domain DSS.

A. Nilai *Process Capability* Domain DSS

Hasil pengukuran nilai *process capability level* domain DSS adalah 3,3 (*established*). Hal ini menunjukkan bahwa secara umum proses TI pada domain DSS telah didefinisikan dan dikelola termasuk target pencapaiannya. Secara detail nilai setiap proses diperlihatkan pada Tabel II.

TABEL II
NILAI PROCESS CAPABILITY DOMAIN DSS

Proses	Nilai	Nilai Target	Gap
	Sekarang		
DSS1	4	4	0
DSS2	4	4	0
DSS3	4	4	0
DSS4	3	4	1
DSS5	3	4	1
DSS6	2	4	2

Tabel II menunjukkan bahwa nilai *process capability level* domain DSS adalah 3,3 (*established*), yang terdiri dari DSS1=4, DSS2=4, DSS3=4, DSS4=3, DSS5=3 dan DSS6=2. Hal ini berarti bahwa proses DSS1, DSS2, DSS3 telah memiliki *process capability* yang terukur dan terkendali. Sedangkan DSS4 dan DSS5 memiliki tingkat *process capability* yang telah didefinisikan dan dikelola sesuai standar baku walaupun belum dilakukan pengukuran

DENGAN MENGGUNAKAN KERANGKA KERJA COBIT 5 PADA LAYANAN PUBLIK

dan pengendalian. Sedangkan DSS6 memiliki tingkat *process capability* yang masih rendah, proses sudah ada dan telah memiliki luaran yang dikelola. Secara detail setiap proses akan diuraikan sebagai berikut.

1. DSS01 Manage Operations

Hasil pengukuran dan analisis data pada proses DSS01 diperlihatkan pada Tabel III.

TABEL III
HASIL PENGUKURAN PROCESS CAPABILITY DOMAIN DSS01

	Nilai Sekarang	<i>Process Capability Level</i>
Hasil Pengamatan	4	<i>Predictable</i>
Target	4	<i>Predictable</i>
Gap	0	

Proses *Manage Operations* bertujuan memastikan seluruh kegiatan operasional layanan TI berjalan sesuai dengan jadwal yang telah ditetapkan, dipantau, terukur dan dilaporkan secara rutin. Hasil pengamatan pengelolaan operasi layanan TI menunjukkan proses telah berjalan sesuai jadwal petugas pelayanan operasional TI. Pemantauan operasional layanan TI juga telah dilakukan termasuk yang dioperasikan oleh penyedia jasa dari pihak ketiga. Telah ditetapkan pula *service level agreement* (SLA) untuk penyedia jasa pihak ketiga termasuk pencapaiannya. Sedangkan untuk layanan TI internal belum dilakukan perhitungan SLA secara keseluruhan pada semua jenis layanan. Kondisi target yang diinginkan ke depannya adalah terdefinisinya SLA pada seluruh layanan yang disediakan, dimonitor dan dikendalikan pencapaian SLA-nya.

Untuk mencapai target tersebut maka direkomendasikan perbaikan pada proses ini adalah pada setiap layanan TI dibuat katalog layanan yang lebih lengkap, didalamnya telah didefinisikan SLA, penanggung jawab, pencapaian SLA dipantau, terukur dan dilaporkan pencapaiannya secara rutin setiap bulan terkait dengan hasil monitoring pencapaian SLA. Demikian pula dengan faktor-faktor kendala yang ada harus didefinisikan dan dipantau dan dikendalikan.

2. DSS02 Manage Service Requests and Incidents

Hasil pengukuran dan analisis data pada proses DSS02 diperlihatkan pada Tabel IV.

TABEL IV
HASIL PENGUKURAN PROCESS CAPABILITY DOMAIN DSS02

	Nilai Sekarang	<i>Process Capability Level</i>
Hasil Pengamatan	4	<i>predictable</i>
Target	4	<i>predictable</i>
Gap	0	

Proses *Manage Service Requests and Incidents* bertujuan memastikan seluruh permintaan layanan TI dan insiden layanan TI dapat dikendalikan sesuai target *service level agreement* (SLA) yang telah ditetapkan. Permintaan layanan sifatnya permohonan baru dan harus dipenuhi sesuai prosedur dan SLA permintaan layanan baru. Sedangkan pengelolaan insiden merupakan penanganan terhadap gangguan atau kondisi tidak terhadap normal layanan TI.

Hasil pengamatan menunjukkan bahwa terdapat proses untuk penanganan permintaan layanan dan insiden (*helpdesk*). Permintaan layanan sesuai dengan prosedur permintaan dan pemenuhan layanan dan telah dijalankan dengan baik dan konsisten. Penanganan insiden juga telah dilakukan sesuai prosedur pengelolaan insiden telah dilaksanakan secara konsisten. Setiap penanganan insiden dimonitor dan dilaksanakan sesuai SLA layanan yang telah ditetapkan. Analisis terhadap *trend* insiden saat ini belum dilakukan baik berupa laporan harian, mingguan maupun bulanan.

Untuk pengembangan ke depan maka diperlukan penanganan insiden, analisis tren insiden dilakukan untuk keperluan penanganan yang lebih cepat dan terukur. Untuk itu rekomendasi perbaikan ke depan adalah menetapkan SLA penanganan insiden untuk seluruh layanan TI, melakukan evaluasi penanganan insiden dalam bentuk laporan harian, mingguan, bulanan termasuk analisis tren insiden, sebagai dasar untuk melakukan perbaikan menyeluruh dan peningkatan efektifitas layanan.

3. DSS03 Manage Problem

Hasil pengukuran dan analisis data pada proses DSS03 diperlihatkan pada Tabel V.

TABEL V
HASIL PENGUKURAN PROCESS CAPABILITY DOMAIN DSS03

	Nilai Sekarang	<i>Process Capability Level</i>
Hasil Pengamatan	4	<i>Predictable</i>
Target	4	<i>Predictable</i>
Gap	0	

Tujuan dari proses *Problem Management* adalah memastikan permasalahan yang terjadi pada layanan TI dapat diidentifikasi, diklasifikasikan dan dicari akar masalah (*root cause*) penyebab terjadinya serta menemukan resolusi dengan tepat waktu dan mencegah kejadian berulang. Perbedaan insiden dengan *problem* terletak pada karakteristik insiden dan penyebabnya. Insiden yang terjadi secara berulang, meskipun telah dilakukan penanganan namun terjadi lagi dengan insiden yang sama, maka disebut *problem*, artinya ada sesuatu penyebab yang belum ditemukan solusi permanennya. Jika hal ini terjadi pada sebuah layanan maka segera dimasukkan sebagai kategori *problem*.

Pada penelitian kali ini, hasil pengamatan menunjukkan bahwa telah terdapat prosedur penanganan masalah (*problem*), implementasi penanganan masalah dijalankan sesuai prosedur yang telah ditetapkan. Penanganan masalah juga telah dilakukan sesuai SLA, namun evaluasi tren masalah yang terjadi belum dilakukan. Untuk mencapai target perbaikan yang diinginkan maka kondisi yang diharapkan adalah selain pengelolaan masalah yang terukur, juga perlu dilakukan evaluasi kejadian masalah, baik secara harian, mingguan dan bulanan, sehingga dapat diketahui tren masalah yang sering terjadi. Setiap jenis masalah pada layanan perlu didefinisikan SLA penanganan masalah layanan TI (dapat diintegrasikan dalam katalog layanan). Untuk mencapai target tersebut maka rekomendasi perbaikan kedepan adalah proses insiden dan *problem* agar dipisahkan (dibedakan), melakukan evaluasi

penanganan masalah dalam bentuk laporan harian, mingguan, bulanan termasuk analisis tren yang masalah terjadi.

4. DSS04 Manage Continuity

Hasil pengukuran dan analisis data pada proses DSS04 diperlihatkan pada Tabel VI.

TABEL VI
HASIL PENGUKURAN PROCESS CAPABILITY DOMAIN DSS04

	Nilai Sekarang	Process Capability Level
Hasil Pengamatan	3	Established
Target	4	Predictable
Gap	1	

Tujuan proses *Manage Continuity* adalah memastikan keberlangsungan layanan TI yang sifatnya kritis dapat disediakan dengan tingkat layanan minimum sesuai kebutuhan bisnis. Dalam pengelolaan layanan TI, jika terjadi kondisi darurat tidak mesti seluruh layanan TI harus berjalan, tetapi dipilih layanan TI yang mendukung bisnis yang sifatnya vital. Layanan TI yang mendukung layanan vital inilah yang disebut layanan TI kritis.

Hasil pengamatan penelitian menunjukkan bahwa institusi telah memiliki *backup* data dan aplikasi dilakukan ke *disaster recovery center* (DRC) secara *mirroring* untuk aplikasi kritis seperti SAP. Prosedur *backup* data dan aplikasi juga telah disusun dan dilaksanakan. Meskipun demikian dokumen formal *Business Continuity Plan* (BCP) belum disusun dan ditetapkan sebagai dasar strategi dan prosedur *backup* DRC. Kondisi yang diharapkan ke depan adalah seluruh proses-proses bisnis vital diidentifikasi, layanan TI baik aplikasi maupun infrastrukturnya juga diidentifikasi sesuai kebutuhan bisnis dan data. *Recovery time objective* (RTO) dan *recovery point objective* (RPO) harus didefinisikan sehingga dapat diketahui toleransi kehilangan data jika terjadi bencana dapat didefinisikan. Demikian pula dengan periode *backup* dapat ditetapkan berdasarkan RPO dan RTO tersebut. Untuk rekomendasi perbaikan kedepan perlu disusun dokumen BCP dan DRP yang lengkap, ditetapkan dan diimplementasikan sebagai dasar penetapan strategi *backup* dan pembuatan DRC.

5. DSS05 Manage Security Services

Hasil pengukuran dan analisis data pada proses DSS05 diperlihatkan pada Tabel VII.

TABEL VII
HASIL PENGUKURAN PROCESS CAPABILITY DOMAIN DSS05

	Nilai Sekarang	Process Capability Level
Hasil Pengamatan	3	established
Target	4	predictable
Gap	1	

Tujuan proses *Manage Security Services* adalah memastikan bahwa penyelenggaraan layanan TI memenuhi persyaratan keamanan informasi. Persyaratan keamanan informasi disusun secara terencana, dikomunikasikan dan diimplementasikan serta dioperasikan konsisten di seluruh lingkungan organisasi. Keamanan informasi tidak hanya keamanan fisik tetapi juga keamanan logik. Keamanan fisik meliputi ruangan, gedung, tempat kerja, dokumen fisik serta

keamanan manusia. Keamanan logik mencakup keamanan jaringan, aplikasi, data, dan aset lainnya.

Hasil pengamatan penelitian menunjukkan bahwa sistem manajemen keamanan informasi telah diterapkan berupa Kebijakan Pengamanan Informasi, standar dan prosedur keamanan informasi. Kebijakan, standar dan prosedur tersebut disusun sesuai kebutuhan. Sedangkan evaluasi atau pengujian pengamanan informasi yang dilakukan selama ini melalui *Vulnerability Assessment* (VA) dan *Penetration Testing* secara internal.

Pengelolaan keamanan informasi belum menerapkan standar berupa sistem manajemen keamanan informasi baik aspek penyusunan sistem manajemen keamanannya maupun auditnya. Kondisi yang diharapkan ke depan adalah pengelolaan keamanan informasi mengacu pada *bestpractice* seperti ISO 27001: *information security management system* (ISMS). Untuk rekomendasi perbaikan ke depan adalah menerapkan standar ISMS dalam penyusunan sistem manajemen keamanan informasi, audit dan sertifikasi sistem manajemen keamanan informasi (ISMS) standar internasional seperti ISO/IEC 27001:2017, atau dapat menggunakan *bestpractice* internasional lainnya.

6. DSS06 Manage Business Process Controls

Hasil pengukuran dan analisis data pada proses DSS06 diperlihatkan pada Tabel VIII.

TABEL VIII
HASIL PENGUKURAN PROCESS CAPABILITY DOMAIN DSS06

	Nilai Sekarang	Process Capability Level
Hasil Pengamatan	2	managed
Target	4	predictable
Gap	2	

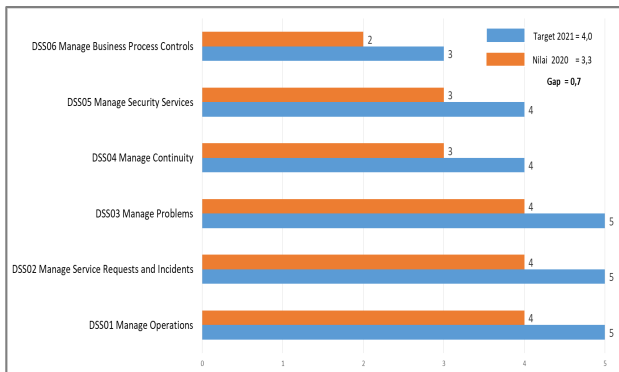
Tujuan proses *Manage Business Process Controls* difokuskan pada bagaimana memastikan transaksi bisnis, pertukaran data bisnis antar unit kerja, individu maupun lintas institusi dilakukan pengendalian sesuai standar keamanan informasi. Pertukaran informasi yang dimaksud dapat dilakukan melalui sistem atau layanan TI maupun yang dilakukan secara manual.

Hasil pengamatan menunjukkan bahwa pengendalian dokumen informasi bisnis maupun data transaksi bisnis telah dilakukan, namun belum didasarkan pada klasifikasi tingkat keamanan. Klasifikasi data berdasarkan tingkat keamanan belum dibuat kategori, misalnya sangat rahasia, rahasia, internal, dan umum. Kategorisasi data bisnis belum didefinisikan sesuai tingkat kritikalitasnya. Kondisi yang diharapkan ke depan adalah melakukan pendefinisian kategorisasi data bisnis berdasarkan tingkat kritikalitasnya. Seluruh data bisnis harus dilakukan pemetaan sehingga dapat ditentukan masuk kategori mana dari aspek klasifikasi keamanan data.

Untuk rekomendasi perbaikan ke depan, perlu membuat standar kategori data bisnis berdasarkan kerahasiaan atau keamanan informasi. Membuat standar dan prosedur pengelolaan dan pengendalian keamanan data bisnis berdasarkan tingkat kerahasiaan datanya. Melakukan audit pengelolaan dan penerapan standar dan prosedur keamanan data bisnis secara rutin, dan dapat dilakukan berdasarkan sistem manajemen keamanan informasi (ISMS)

DENGAN MENGGUNAKAN KERANGKA KERJA COBIT 5 PADA LAYANAN PUBLIK

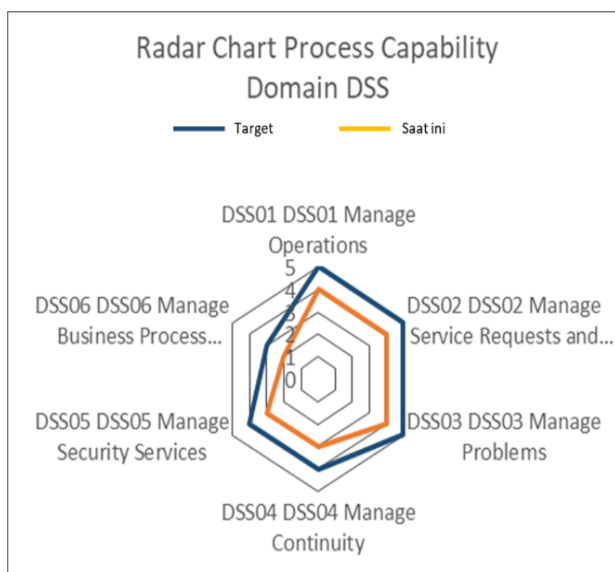
standar internasional seperti ISO/IEC 27001:2017. Hasil pengukuran nilai *process capability* domain DSS seperti diperlihatkan pada Gambar 6.



Gambar 6 Nilai process capability saat ini dan target process capability domain DSS

Berdasarkan Gambar 6, nilai *process capability level* domain DSS adalah 3,3 (*established*). Nilai target yang diinginkan adalah 4,0 (*predictable*), dan masih terdapat *gap* atau kesenjangan yang harus dipenuhi sebesar 0,7 nilai. Hal ini berarti bahwa secara keseluruhan proses TI pada domain DSS telah didefinisikan dan dikelola termasuk target pencapaiannya. Proses yang masih belum memenuhi target yakni DSS05 dan DSS06 sehingga perlu perbaikan. Sementara proses DSS01, DSS02, DSS03 dan DSS04 telah memenuhi target yang diharapkan sehingga perlu dipertahankan.

Dalam bentuk *radar chart* hasil pengamatan *process capability level* domain DSS saat ini dan target perbaikan yang direkomendasikan dalam penelitian ini seperti diperlihatkan pada Gambar 7.



Gambar 7 Radar chart kinerja saat ini dan target process capability domain DSS

IV. KESIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa tata kelola TI atau *IT Governance* pada layanan publik BAKTI telah diimplementasikan namun belum sepenuhnya

memenuhi target yang diinginkan. Hasil penelitian menunjukkan bahwa nilai *process capability level* domain DSS adalah 3,3 (*established*), yang terdiri dari DSS1=4, DSS2=4, DSS3=4, DSS4=3, DSS5=3 dan DSS6=2. Tiga proses telah memenuhi target kinerja yakni DSS01, DSS02, DSS03 dan DSS04. Sedangkan tiga proses lainnya masih dibawah target kinerja yakni DSS04, DSS05 dan DSS06, sehingga perlu dilakukan perbaikan.

Target kinerja yang diharapkan adalah *predictable* atau berada pada nilai *process capability* 4,0, sehingga masih terdapat kesenjangan yang harus diupayakan pemenuhannya. Untuk proses DSS04 direkomendasikan untuk dilakukan penyusunan dokumen BCP dan DRP sebagai dasar penetapan strategi *backup* dan pembuatan DRC. Sedangkan DSS05 direkomendasikan untuk dilakukan evaluasi, audit dan sertifikasi berdasarkan sistem manajemen keamanan informasi (ISMS) standar internasional seperti ISO/IEC 27001:2017. Demikian pula untuk DSS06 direkomendasikan pengendalian informasi dan data bisnis sesuai standar sistem manajemen keamanan informasi (ISMS).

DAFTAR RUJUKAN

- [1] Peterson, R. R., *Integration Strategies and Tactics for Information Technology Governance*, London, 2000.
- [2] Van Grembergen, W., De Haes, S., & Guldentops, E., *Structures, Processes and Relational Mechanisms for IT Governance*, Belgium, Idea Group, 2004
- [3] D. H. Steven and V. G. Wim, *Enterprise Governance of Information Technology: Achieving Alignment and Value Featuring COBIT 5*, Springer, 2015.
- [4] Nugroho, Heru, Proposed IT Governance at Hospital Based on COBIT 5 Framework, *International Journal of Applied IT* Vol. 01 No. 02, pp 54-58, 2017.
- [5] Castillo, F., & Stanojevic, P. *An Assessment Of The IT Governance Maturity At Stockhols Lokaltrafik*, 2011.
- [6] Khther, R., & Othman, D., COBIT Framework As Guideline Of Effective IT Governance In Higher Education. *International Journal of Information Technology Convergence and Services (IJITCS)*, 3, 2013.
- [7] Huang, R., Zmud, R. W., & Price, R. L., Influencing the effectiveness of IT governance practices through steering committees and communication policies. *European Journal of Information Systems*, 2010.
- [8] Setiawan, K., Ari, & Andty F., Johanes F, IT Governance Evaluation Using Cobit 5 Framework On The National Library, *Journal of Information System*, Volume 15, Issue 1, pp.11-17, April 2019.
- [9] Lorences, P., & Avila, L., *The Evaluation and Improvement of IT Governance. JISTEM - Journal of Information Systems and Technology Management*, pp 219-234, 2013.
- [10] IT Governance Institute., *COBIT 4.1 Framework, Control Objectives, Management Guidelines and Maturity Models*. USA: ITGI, 2007.
- [11] COBIT 5: *A Business Framework for the Governance and Management of Enterprise IT*. ISACA, 2012.

- [12] Weill, P., & Woodham, R., *Don't Just Lead, Govern: Implementing Effective IT Governance.*, 2002.
- [13] D. G. Stephen, *The Basics of IT Audit*, Syngress, 2013.
- [14] COBIT 2019 *Framework: Introduction & Methodology*, ISACA, 2018