Control Self-Assessment Pada *Unit* Infrastruktur Teknologi Informasi Universitas Telkom

Control Self-Assessment at Information Technology Infrastructure Unit of Telkom University

1st Nilam Eria Azzahra
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
nilameriaazzahra@student.telkomuniversity.ac.id

2nd Lukman Abdurrahman
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
abdural@telkomuniversity.ac.id

3rd Rahmat Mulyana
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
rahmatmoelyana@telkomuniversity.ac.id

Abstrak*—Perkembangan teknologi terkini, perubahan perilaku menuju digital serta akselerasi digitalisasi karena pandemi Covid-19 telah meningkatkan risiko TI dengan sangat pesat yang dapat menghambat pencapaian tujuan organisasi. Penelitian sebelumnya telah menemukan praktik yang baik dalam mengoptimalkan risiko menuju pencapaian target kinerja, yaitu melalui pendekatan Three Lines of Defense (TLOD). TLOD Line pertama adalah pengendalian risiko oleh pemilik risiko, kedua adalah manajemen risiko, dan ketiga adalah audit internal. Salah satu bentuk pengendalian risiko oleh pemilik risiko adalah dengan menerapkan Control Self-Assessment (CSA). Oleh karena itu, penelitian ini dilakukan untuk mengidentifikasi praktik CSA terkini yang sesuai dengan profil risiko organisasi. Metode yang digunakan adalah studi kasus yang dilakukan di unit infrastruktur TI pada pusat pengelolaan TI di Universitas Telkom, Indonesia. Kerangka kerja yang digunakan sebagai referensi penelitian adalah COBIT 2019 dari ISACA. Pengumpulan data dilakukan dengan wawancara staf terkait, triangulasi dokumen, dan observasi. Analisis dilakukan dengan melakukan assessment prioritas Governance & Management Objective (GMO) dan mengidentifikasi kontrol yang sesuai berdasarkan GMO terpilih dan mengidentifikasi praktik pengendalian terkait. Penelitian ini menghasilkan DSS01 dan DSS03 rekomendasi praktik CSA. Hasil penelitian berkontribusi terhadap basis keilmuan untuk menjadi acuan penelitian sejenis berikutnya, serta dapat menjadi referensi implementasi CSA, khususnya di PuTI Universitas Telkom, maupun perguruan tinggi lainnya.

***Kata Kunci*— control self-assessment, COBIT 2019, tata kelola TI.**

Abstract* — The latest technological developments, changes in behavior towards digital, and the acceleration of digitalization due to the Covid-19 pandemic have rapidly increased IT risks, which can hinder the achievement of organizational goals. Previous research has found good practices in optimizing risk towards achieving performance targets, namely through the Three Lines of Defense (TLOD). The first TLOD line is risk control by risk owners, the second is risk management, and the third is internal audit. One form of risk control by risk owners is implementing Control Self-Assessment (CSA). This research was conducted to identify current CSA practices following the organization's risk profile. The method used is a case study conducted in unit infrastructure IT at the IT management center at Telkom University, Indonesia. The framework used as a research reference is COBIT 2019 from ISACA. Data was collected by interviewing related staff, document triangulation, and observation. The analysis is carried out by assessing the Governance & Management Objective (GMO) prioritization and then identifying appropriate controls based on the selected GMOs. This study resulted in DSS01 and DSS03 recommendations for CSA practices and relevant staff roles. The results of the research contribute to the scientific basis to become a reference for the next similar research and can be a reference for the implementation of CSA, especially at PUTI Telkom University, as well as other universities.

***Keywords*— control self-assessment, COBIT 2019, IT governance**

1. PENDAHULUAN

Dewasa ini, sebagian besar perusahaan di semua sektor industri bergantung pada penerapan teknologi informasi yang diimplementasikan, termasuk sektor pendidikan yang memiliki peran penting dalam perkembangan Indonesia maka dari itu Universitas Telkom harus menyesuaikan diri dengan perkembangan yang ada khususnya pada Direktorat Pusat Teknologi Informasi (PuTI), karena itu bukanlah sebuah pilihan melainkan keharusan dan kewajiban. Salah satu upaya untuk memenuhi kebutuhan tersebut adalah mengadakan *Control Self-Assessment* (CSA) terhadap setiap proses yang ada pada unit – unit di perusahaan baik *branch* maupun *head office*. CSA dilaksanakan untuk tujuan bisnis dalam skala yang lebih luas dan mencakup maksimalisasi laba, layanan pelanggan, perbaikan produk atau proses, dan lainnya. CSA dapat dilakukan dengan berbagai macam metode, salah satunya yaitu dengan menggunakan kerangka kerja COBIT 2019 dalam pengimplementasiannya. Oleh karena itu, sangat penting dilakukannya *Control Self-Assessment* pada unit Infrastruktur Teknologi Informasi (IsTI) untuk menguji apakah kontrol tersebut sudah efisien untuk diterapkan. Berdasarkan permasalahan tersebut, penulis melakukan penelitian ini untuk menghasilkan rekomendasi *Governance Management Objective* (GMO) menggunakan COBIT 2019 yang nantinya dapat digunakan untuk mempermudah pelaksanaan *Control Self-Assessment* pada unit Infrastruktur Teknologi Informasi (IsTI) Direktorat Pusat Teknologi Informasi Universitas Telkom.

II. KAJIAN TEORI

A. Tata Kelola Teknologi Informasi

Transformasi digital memberikan keunggulan dalam tata kelola TI, dengan memberikan keselarasan antara bisnis dan teknologi informasi guna meningkatkan kinerja dalam organisasi (Mulyana dkk. 2022). Mekanisme tata kelola TI yang teridentifikasi mempengaruhi transformasi digital di berbagai organisasi serta memberikan pengaruh terhadap kinerja organisasi (Mulyana dkk. 2021). Menurut Surendro tahun 2009, tata kelola teknologi informasi adalah kemampuan organisasi untuk mengontrol perumusan dan implementasi strategi perusahaan dan mendorong manfaat daya saing perusahaan.

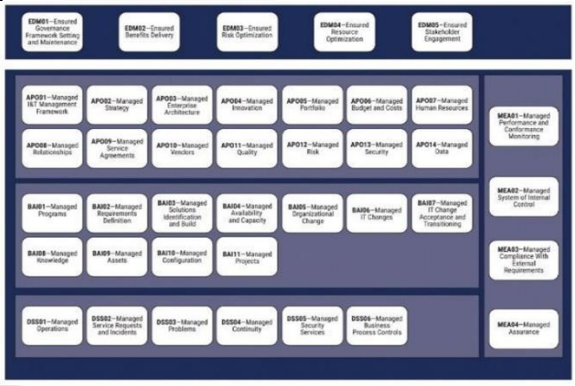
B. Control Self-Assessment

Kompetensi digital, pengetahuan, inovasi, dan manajemen perubahan selaras dengan proses tata kelola TI dari strategi digital dan manajemen arsitektur perusahaan (Mulyana dkk. 2021). Organisasi secara sistematis bersiap untuk beradaptasi secara konsisten dan bersaing secara efektif terhadap perubahan digital yang sedang berlangsung dengan membandingkan dengan organisasi ideal yang ditransformasi oleh teknologi digital (Thordsen dkk. 2020). Akhirnya, perusahaan perlu meningkatkan peluang untuk mencapai transformasi digital yang sukses dengan melakukan *agile audit and assurance management* (Mkoba dan Marnewick 2020). Audit adalah penilaian yang dilakukan oleh *auditor internal* untuk memeriksa dan mengevaluasi kegiatan organisasi, salah satu alat auditor adalah *Control Self-Assessment* untuk memperoleh gambaran pengendalian internal organisasi. Dengan memberikan rekomendasi guna meningkatkan proses tata Kelola untuk mencapai tujuan dan sasaran organisasi (Suharso, 2016).

Menurut Hubbard tahun 2000, *Control Self-Assessment* adalah CSA merupakan proses di mana manajemen dari semua tingkat secara terus menerus membangun kesadaran atas semua faktor penting yang dapat mempengaruhi pencapaian tujuan sehingga memungkinkan mereka untuk melakukan penyesuaian–penyesuaian (menciptakan kontrol) yang dibutuhkan.

C. COBIT 2019

COBIT 2019 merupakan *framework* versi terbaru untuk melakukan audit saat ini yang dikeluarkan oleh ISACA. COBIT 2019 ini merupakan evolusi dari COBIT 5 yang dikembangkan berdasarkan dua prinsip, yaitu prinsip yang menjelaskan inti dari sistem tata kelola teknologi dan informasi pada perusahaan serta prinsip kerangka kerja tata kelola yang dapat digunakan untuk membangun sistem tata kelola perusahaan.



GAMBAR 1
DOMAIN COBIT 2019

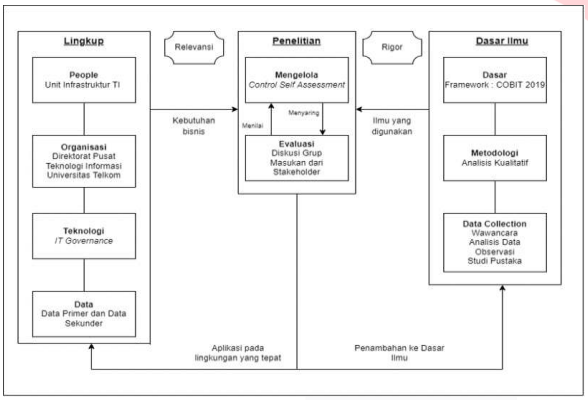
Gambar 1 mendefinisikan faktor desain yang harus dipertimbangkan perusahaan untuk membangun sistem tata kelola TI yang baik. COBIT saat ini berkembang menjadi kerangka tata kelola dan manajemen TI. *Framework* COBIT 2019 memiliki 5 domain, yaitu:

1. *Evaluate, Direct and Monitor* (EDM) membahas tentang *governance area*, mengevaluasi opsi-opsi strategis, mengarahkan manajemen senior pada

opsi-opsi strategis yang dipilih dan memantau pencapaian strategi.
2. *Align, Plan and Organize* (APO) membahas keseluruhan organisasi, strategi, dan kegiatan pendukung untuk TI.
3. *Build, Acquire and Implement* (BAI) mendefinisikan, mengakuisisi, dan implementasi solusi TI dan integrasinya dalam proses bisnis.
4. *Deliver, Service and Support* (DSS) membahas operasional dan dukungan layanan TI, termasuk keamanan.
5. *Monitor, Evaluate and Assess* (MEA) membahas pemantauan kinerja dan kesesuaian TI dengan target kinerja internal, tujuan kontrol internal, dan persyaratan eksternal

III. METODE

A. *Model Konseptual*



GAMBAR 2
METODOLOGI PENELITIAN

Gambar 2 merupakan penelitian Sistem Informasi terdiri dari lingkungan yang mencakup orang, organisasi, dan teknologi yang memenuhi kebutuhan bisnis. Pada model konseptual di atas dapat diperoleh dari hasil identifikasi lingkungan yang terkait dengan bisnis berupa orang, organisasi, dan teknologi. Bagian *People* menjelaskan tentang siapa yang menjadi subjek pada sebuah penelitian, bisa dalam bentuk peran, kemampuan, ataupun karakteristik. Dalam penelitian ini yang menjadi aspek people adalah unit Infrastruktur Teknologi Informasi (IsTI). Di bagian Organisasi menjelaskan tentang strategi, struktur dan kultur, serta proses yang ada pada organisasi. Organisasi yang akan diteliti yaitu Direktorat Pusat Teknologi Informasi (PuTI) Universitas Telkom. Di bagian Teknologi menjelaskan teknologi apa yang ada di bagian infrastruktur TI dan digunakan di organisasi tempat penelitian.

B. Sistematika Penelitian

Sistematika penelitian yang digunakan berpedoman pada siklus implementasi di dalam panduan COBIT 2019 *Implementation Guide*. Siklus implementasi yang dilakukan hanya dari fase 1 sampai fase 4. Berikut penjelasan mengenai sistematika penelitian:

1. Memahami konteks dan strategi perusahaan

Pada fase pertama, perusahaan memeriksa latar belakang, strategi, dan lingkungan bisnisnya untuk mendapatkan pemahaman yang jelas tentang empat area yang sebagian tumpang tindih, saling bergantung, dan sering kali saling melengkapi. Menguraikan sub-langkah dasar di langkah pertama yaitu strategi perusahaan, sasaran perusahaan dan sasaran penyelarasan yang dihasilkan, profil risiko TI dan masalah terkait TI saat ini.

2. Menentukan seluruh komponen pada CSA

Untuk menentukan ruang lingkup awal sistem tata kelola, fase kedua ini mempertimbangkan komponen sistem tata kelola, menentukan risiko pada unit Infrastruktur Teknologi Informasi, dan menentukan seluruh bagian *Control Self-Assessment*.

3. Menilai risiko dari seluruh bidang pada CSA

Fase ketiga menilai risiko dari seluruh bidang pada CSA, berdasarkan risiko paling tinggi pada unit Infrastruktur Teknologi Informasi yang ada pada COBIT 2019.

4. Menyimpulkan dan memberikan rekomendasi CSA

Sebagai fase terakhir dari penyelesaian masalah, fase keempat menyelesaikan rencana *Control Self-Assessment* dari fase sebelumnya dengan memberikan rekomendasi *Governance Management Objective* (GMO) COBIT 2019.

IV. PENGUMPULAN DAN ANALISIS DATA

A. Pengumpulan Data

Dalam penyusunan tugas akhir ini penulis mengambil objek penelitian pada Direktorat Pusat Teknologi Informasi Universitas Telkom yang bertempat di Jalan Telekomunikasi No.1 Bandung. Pengumpulan data dalam penelitian ini menggunakan 2 cara berikut merupakan uraian yang digunakan:

1. Observasi

Suatu metode pengumpulan data yang dilakukan dengan mengamati langsung, melihat dan mengambil suatu data yang dibutuhkan (Sudaryono, 2011). Observasi juga bisa diartikan sebagai proses yang kompleks. Pengumpulan data yang dilakukan di unit Infrastruktur Teknologi Informasi (IsTI).

2. Wawancara

Wawancara merupakan salah satu teknik pengumpulan data yang dilakukan melalui tatap muka langsung dengan narasumber dengan cara tanya jawab langsung (Jogiyanto, 2008). Wawancara dilakukan dengan perwakilan unit Infrastruktur Teknologi

Informasi (IsTI) yang berhubungan dengan data yang terkait. Informasi yang diperoleh antara lain:

a) Struktur organisasi PuTI
b) Aktivitas bisnis PuTI
c) Pemodelan proses bisnis PuTI
d) Penerapan *Control Self-Assessment*
e) Risk Scenario Category
f) Peta Risiko masing – masing Unit PuTI
g) Bukti Tindakan Mitigasi dan Evaluasi risiko masing – masing unit Direktorat Pusat Teknologi Informasi
h) Proses bisnis dari masing – masing risiko unit Direktorat Pusat Teknologi Informasi
i) Konfirmasi terkait bukti Tindakan Mitigasi dan Evaluasi risiko masing – masing unit Direktorat Pusat Teknologi Informasi

3. Studi Pustaka

Menurut Rahardjo (2011) studi pustaka adalah teknik pengumpulan data yang dilakukan dengan menganalisis karya ilmiah atau jurnal terdahulu yang memiliki kaitan dengan penelitian ini. Studi pustaka yang digunakan dalam penelitian ini adalah karya ilmiah yang berkaitan dengan *Control Self-Assessment* menggunakan kerangka kerja COBIT 2019.

B. Analisa Data

Analisis ini dilakukan dengan cara menganalisis kondisi perusahaan di Direktorat Teknologi Informasi Universitas Telkom saat ini dengan kondisi yang diinginkan oleh perusahaan, sehingga dihasilkan rekomendasi *Governance Management Objective* (GMO) berdasarkan COBIT 2019.

1. Memahami Proses Bisnis unit Infrastruktur TI

Proses bisnis adalah serangkaian aktivitas yang dilakukan oleh sebuah organisasi, seperti memulai *input*, mengubah informasi, dan menghasilkan *output*. Hasilnya tidak hanya berharga bagi pelanggan, perusahaan, tetapi juga dalam organisasi. Sebuah proses bisnis dapat dibagi menjadi beberapa sub-proses yang membantu mencapai tujuan dari proses induk. Sub-proses dapat dibagi lagi menjadi aktivitas yang terdiri dari satu atau lebih yang harus disertakan dalam proses bisnis (Harmon, 2003).

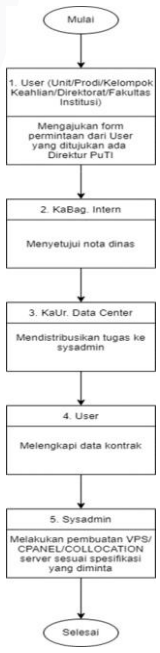
a. Proses Bisnis Keberfungsian Layanan TI

Gambar 3 merupakan proses bisnis keberfungsian layanan TI, di mana Ka Bag INTEN berkoordinasi dengan jajaran dibawah-Nya untuk melakukan *monitoring* keberfungsian layanan TI yang dijaminkan selama jam operasional. *Monitoring* Keberfungsian Layanan TI dilakukan menggunakan bantuan aplikasi

GAMBAR 3
PROSES BISNIS KEBERFUNGSIAN LAYANAN TI

b. Proses Bisnis Permintaan Data Layanan *Center*

Gambar 4 merupakan proses bisnis data layanan *center*, *Data Center* menerima permintaan melalui aplikasi nota dinas *official* Universitas Telkom yang dikirimkan oleh *user* (Unit/Prodi/Kelompok Keahlian/Direktorat/Fakultas/Institusi) dan ditujukan kepada Direktur Sisfo untuk permintaan layanan VPS/CPANEL/COLLECTION. Kabag. Intern menyetujui nota dinas dan mendistribusikan tugas kepada Kaur. *Data Center*. Kaur. *Data Center* melakukan pendistribusian tugas kepada bagian *sysadmin* (Staf *Data Center* yang melakukan eksekusi untuk permintaan layanan VPS, CPanel, dan *Collaction*) *User* melengkapi kontrak yang meliputi deskripsi kebutuhan dan kontak PIC.



GAMBAR 4
PROSES BISNIS DATA LAYANAN *CENTER*

2. Memahami Profil Risiko Perusahaan

TABEL 1
KATEGORI KE TERJADIAN RISIKO

Ke terjadian	
Level kemungkinan (L)	Kriteria
1 (Hampir Tidak Terjadi)	1 kejadian dalam 1 semester
2 (Jarang Terjadi)	>1 – 3 kejadian dalam 1 semester
3 (Kadang Terjadi)	>3 – 5 kejadian dalam 1 semester
4 (Sering Terjadi)	>5 – 10 kejadian dalam 1 semester
5 (Selalu Terjadi)	>10 kejadian dalam 1 semester

Tabel 1 merupakan kategori ke terjadian risiko dengan level kemungkinan dan kriteria yang berbeda. Mulai dari level kemungkinan yang terendah (hampir tidak terjadi) sampai yang tertinggi (selalu terjadi), dengan kriteria kejadian dalam satu semester.

Tabel 2 merupakan peta penilaian risiko yang menunjukkan tingkat risiko terendah sampai tertinggi dengan skala tidak signifikan, minor (kecil), moderat (sedang), signifikan, serta ekstrem. Dengan penilaian matriks risiko 1 (hampir tidak terjadi), 2 (jarang terjadi), 3 (kadang terjadi), 4 (sering terjadi), dan 5 (selalu terjadi).

TABEL 2
PETA PENILAIAN RISIKO

Risk Matrix Grading					
Scale	1 Hampir Tidak Terjadi	2 Jarang Terjadi	3 Kadang Terjadi	4 Sering Terjadi	5 Selalu Terjadi
(1) Tidak Signifikan	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
(2) Minor	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
(3) Moderat	MEDIUM	MEDIUM	MEDIUM	HIGH	DANGER
(4) Signifikan	MEDIUM	MEDIUM	HIGH	DANGER	DANGER
(5) Ekstrem	MEDIUM	HIGH	DANGER	DANGER	DANGER

Peta risiko terbagi menjadi lima bagian antara lain:

a. Tidak signifikan artinya terjadi dampak kecil berupa kerugian non finansial pada area dampak risiko di mana kejadian masih dapat ditangani melalui prosedur dan proses kerja yang berlaku.
b. Minor artinya terjadi dampak kecil pada area dampak risiko di mana kejadian masih dapat ditangani melalui prosedur dan proses kerja yang berlaku.
c. Moderat artinya terjadi dampak yang signifikan pada area dampak risiko tetapi dapat ditangani melalui prosedur dan proses kerja yang berlaku.
d. Signifikan artinya terjadi dampak signifikan dan berpotensi sistematik pada area dampak risiko yang perlu ditangani secara cepat dan tepat.
e. Ekstrem atau sangat signifikan artinya terjadi dampak membahayakan dan sistematik pada area dampak risiko yang perlu ditangani secara cepat dan tepat.

3. Memahami Kontrol terhadap Risiko unit Infrastruktur TI

Berikut merupakan kontrol yang terdapat pada unit Infrastruktur Teknologi informasi (IsTI) dengan *risk value medium* hingga *high. Risk value* digunakan untuk menentukan risiko kerugian yang terjadi pada unit Infrastruktur Teknologi Informasi (IsTI) dengan menggunakan risiko skala menengah hingga risiko tinggi. Dengan menilai kontrol tersebut baik secara rancangan dan operasional, secara rancangan kontrol tersebut dilakukan oleh siapa saja atau orang yang terlibat dalam proses tersebut. Secara operasional, kontrol tersebut dilakukan berapa kali dalam kurun waktu satu tahun dengan pembuktian adanya dokumen yang ditandatangani oleh pihak terkait. Dengan melakukan pengujian kontrol, apakah termasuk efisien atau defisien untuk dijalankan dalam proses bisnis unit Infrastruktur Teknologi Informasi (IsTI). Kontrol tersebut dikatakan efisien, jika memenuhi kriteria secara rancangan dan operasional atau salah satu dari kedua pengujian kontrol tersebut. Di mana kontrol tersebut digunakan untuk menguji risiko, risiko merupakan suatu kejadian yang berkaitan dengan kondisi yang dapat menghambat jalannya proses bisnis unit Infrastruktur Teknologi Informasi (IsTI).

TABEL 3
KONTROL EFISIEN DAN DEFISIEN

Bagian 1		
Proses Bisnis	:	Permintaan Data Layanan *Center*
Risiko	:	Ancaman terhadap keamanan informasi, karena terdeteksi celah keamanan data pada perangkat *Data Base* akademik dan non-akademik
Kemungkinan	:	1
Dampak	:	5
Risk Value	:	*Medium*
Tindakan Mitigasi	:	Melakukan *backup image*
Efisien/Defisien	:	Efisien
Bagian 2		
Proses Bisnis	:	Permintaan Data Layanan *Center*
Risiko	:	Pengaruh terhadap jaringan, listrik, AC, akses kontrol, kebakaran,

		karena pengajuan di luar standar IsTI
Kemungkinan	:	1
Dampak	:	5
Risk Value	:	*Medium*
Tindakan Mitigasi	:	Melakukan konfirmasi sesuai standar IsTI
Efisien/Defisien	:	Efisien
Bagian 3		
Proses Bisnis	:	Permintaan Data Layanan *Center*
Risiko	:	Tidak dapat mengakses layanan internet
Kemungkinan	:	1
Dampak	:	3
Risk Value	:	*Medium*
Tindakan Mitigasi	:	Melakukan konfigurasi sesuai standar IsTI
Efisien/Defisien	:	Defisien
Bagian 4		
Proses Bisnis	:	Keberfungsian Layanan Teknologi Informasi
Risiko	:	Akses Internet dan Intranet mati, karena *fiber optik* putus
Kemungkinan	:	1
Dampak	:	3
Risk Value	:	*Medium*
Tindakan Mitigasi	:	Menutup pintu atau celah *rack* agar tikus tidak bisa masuk
Efisien/Defisien	:	Efisien
Bagian 5		
Proses Bisnis	:	Keberfungsian Layanan Teknologi Informasi
Risiko	:	Akses internet dan intranet mati karena tidak bisa log in (*tune*)
Kemungkinan	:	1
Dampak	:	3
Risk Value	:	*Medium*
Tindakan Mitigasi	:	Melakukan *monitoring system health* secara berkala
Efisien/Defisien	:	Efisien
Bagian 6		
Proses Bisnis	:	Keberfungsian Layanan Teknologi Informasi
Risiko	:	Akses internet dan intranet area *data center* tidak berfungsi (mati)
Kemungkinan	:	1
Dampak	:	5
Risk Value	:	*Medium*
Tindakan Mitigasi	:	Melakukan konfirmasi sesuai standar IsTI
Efisien/Defisien	:	Efisien

V. REKOMENDASI

Berdasarkan pengujian dari masing – masing kontrol terhadap risiko unit Infrastruktur Teknologi Informasi (IsTI) terdapat satu kontrol yang defisien yaitu kontrol pada bagian 3 yang defisien, yang perlu dilakukan perbaikan dari segi efisiensi rancangan dan operasioanal di mana setelah dilakukan analisis dengan membandingkan profil risiko kontrol tersebut tidak berjalan dengan baik.

Setelah melakukan penilaian kontrol berdasarkan risiko yang terjadi pada unit Infrastruktur Teknologi Informasi (IsTI) pada PuTI Universitas Telkom. Pada bagian ini, peneliti akan menentukan *Governance Management Objective* (GMO) prioritas yang relevan dalam mendukung berjalannya aktivitas proses bisnis pada unit Infrastruktur TI. Berikut Tabel 4 merupakan rekomendasi *Governance Management Objective* (GMO) yang di dalamnya terdapat kontrol terhadap risiko yang defisien.

Tabel 4 menunjukkan manajemen objektif mana yang akan berpotensi dilakukannya CSA pada unit Infrastruktur TI Direktorat PuTI Universitas Telkom sesuai dengan hasil skor pada *assessment* penelitian sebelumnya.

TABEL 4
FOKUS UTAMA UNIT IsTI

No.	*Business Unit*	*Management Objective*
1	IsTI	APO11 – *Managed quality*
2	IsTI	APO12 – *Managed risk*
3	IsTI	BAI08 – *Managed knowledge*
4	IsTI	DSS05 – *Managed security services*

Hasil ini didasarkan pada lampiran B dengan mengacu pada penelitian yang dilakukan oleh Ruri Fadhilah (2021) dengan judul "Pengembangan Rencana Audit Teknologi Informasi Pada Unit Infrastruktur Teknologi Informasi Direktorat Pusat Teknologi Informasi Universitas Telkom Menggunakan COBIT 2019". Di mana pada penelitian tersebut telah didapatkan fokus utama pada unit Infrastruktur Teknologi Informasi (IsTI), dilihat berdasarkan skor tertinggi serta yang relevan pada unit Infrastruktur Teknologi Informasi Direktorat PuTI Universitas Telkom yaitu pada APO11 (*Align, Plan and Organize*) yaitu *Manage quality*, APO12 (*Align, Plan and Organize*) yaitu *Manage risk*, BAI08 (*Build, Acquire and Implement*) yaitu *Managed knowledge* dan DSS05 (*Deliver, Service, and Support*) yaitu *Managed security services.*

Tabel 5 merupakan analisis kesenjangan proses bisnis, risiko dan rekomendasi pada unit Infrastruktur TI, penentuan dilakukan dengan melakukan analisis terhadap *management practice* yang telah didapatkan. Setelah itu, setiap risiko yang terdapat pada unit Infrastruktur TI disesuaikan dengan *key management practice* yang relevan. Hal ini dilakukan untuk mempermudah pihak unit Infrastruktur Teknologi Informasi melihat secara keseluruhan potensi bahaya yang terdapat pada unit Infrastruktur TI, serta mempermudah dalam menentukan prioritas kontrol risiko yang harus dilakukan terlebih dahulu.

TABEL 5
REKOMENDASI UNIT IsTI

No.	*Management Practice*	Rekomendasi
1	APO11.01	Penambahan aktivitas dalam pengelolaan mutu internal IsTI sehingga dapat mengidentifikasi

		persyaratan dan kriteria terkait kontrol TI dan proses bisnis
2	APO11.03	Mengintegrasikan manajemen mutu yang diperlukan dalam unit IsTI serta mengkomunikasikan pendekatan manajemen mutu tersebut secara efektif, misalnya berupa program pelatihan sebagai solusi utama di seluruh organisasi
3	APO11.04	Melakukan peninjauan secara teratur terhadap kualitas kinerja manajemen dengan menganalisis hasil kinerja manajemen mutu secara keseluruhan
4	APO11.05	Mengkomunikasikan secara teratur atau terjadwal mengenai rencana kualitas keseluruhan sistem manajemen mutu
5	APO12.02	Membangun upaya analisis risiko dengan mempertimbangkan segala kemungkinan risiko yang dapat terjadi pada unit IsTI
6	APO12.03	Melakukan serangkaian rencana tindakan pengawasan terhadap *risk profile* mengenai sumber daya dan infrastruktur TI yang menopang operasi bisnis proses
7	APO12.04	Melaporkan hasil analisis secara cepat dan tepat kepada setiap stakeholder
8	APO12.05	Mengidentifikasi dan mengelola risiko dalam portofolio yang difokuskan pada peristiwa yang dapat berdampak negatif pada pencapaian tujuan strategis
9	APO12.06	Menerapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.
10	BAI08.01	Meningkatkan ke hati – hatian pada setiap staf yang bertugas atau terhadap para pengguna TI
11	BAI08.02	Melakukan pelatihan agar dapat meningkatkan keterampilan karyawan sesuai dengan perubahan teknologi
12	BAI08.03	Terdapat kategori informasi berdasarkan kebutuhan stakeholder yang berbeda-beda, misalkan informasi tersebut berguna untuk *problem solving,* pembelajaran, atau untuk pengambilan keputusan. Semua itu diatur di dalam *knowledge user database.*
13	BAI08.04	Mengevaluasi dan memperbarui informasi secara lebih kritis dengan menyesuaikan kebutuhan organisasi

Pada tabel 5 merupakan tabel rekomendasi unit Infrastruktur Teknologi Informasi (IsTI), dengan analisis kesenjangan proses bisnis dengan *existing* pada unit Infrastruktur TI, kesenjangan ini dilakukan dengan melakukan analisis terhadap *management practice* yang telah didapatkan. Setelah itu, setiap proses bisnis *existing* yang terdapat pada unit Infrastruktur TI disesuaikan dengan *key management practice* yang relevan terhadap proses bisnis tersebut. Apakah dalam proses bisnis tersebut terdapat aktivitas yang relevan terhadap *management practice,* dibuktikan dengan adanya dokumen *evidence* yang memperkuat bahwa aktivitas tersebut telah dilakukan pada unit Infrastruktur TI. Sebaliknya, jika aktivitas tersebut tidak terdapat pada proses bisnis, maka terdapat gap atau kesenjangan baik secara rancangan maupun operasional. Hal tersebut dapat memunculkan risiko baru pada unit IsTI, dengan justifikasi pada level risiko tersebut serta memberikan rekomendasi agar risiko tersebut tidak terulang kembali pada unit Infrastruktur Teknologi Informasi.

Unit Infrastruktur Teknologi Informasi (IsTI) pada PuTI Universitas Telkom terdapat 22 *management practice* atau fokus utama unit Infrastruktur TI yaitu pada *Governance Management Objective* APO11, APO12, BAI08, dan DSS05. Terdapat 9 *management practice* yang terdapat pada unit Infrastruktur TI antara lain APO11.02, APO12.01, DSS05.01, DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06, dan DSS05.07 dengan mengacu pada kerangka kerja COBIT 2019 yang relevan dalam mendukung berjalannya aktivitas proses bisnis permintaan data layanan Center dan proses bisnis keberfungsian layanan TI pada unit Infrastruktur TI. Dibuktikan dengan adanya *evidence* yang dapat memperkuat hubungan antara *management practice* dengan proses bisnis tersebut. Dengan 13 *management practice* yang tidak terdapat pada unit Infrastruktur TI yaitu APO11.01, APO11.03, APO11.04, APO11.05, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, BAI08.01, BAI08.02, BAI08.03, dan BAI08.04 yang tidak terdapat dalam unit Infrastruktur TI.

VI. KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan analisis yang telah dilakukan dalam penelitian ini, yaitu:

1. Penerapan *Control Self-Assessment* pada unit Infrastruktur Teknologi Informasi (IsTI) untuk mengidentifikasi praktik CSA terkini yang sesuai dengan profil risiko organisasi. Penerapan CSA berfokus pada kontrol terhadap masing – masing risiko unit Infrastruktur Teknologi Informasi (IsTI) dengan mengevaluasi tindakan mitigasi atau evaluasi masing – masing kontrol baik secara desain maupun operasional, kontrol berdasarkan desain dilakukan oleh siapa atau semua orang yang terlibat dalam proses. Secara operasional, pengawasan dilakukan beberapa kali dalam setahun, membuktikan dengan adanya dokumen yang ditandatangani oleh pihak-pihak terkait.

2. Pengujian pada kontrol menunjukkan bahwa kontrol bagian 3 dengan tindakan mitigasi melakukan *backup image*, yang perlu dilakukan perbaikan oleh unit Infrastruktur Teknologi Informasi (IsTI) berdasarkan hasil penilaian secara rancangan dan operasional dengan tidak adanya bukti yang menunjukkan bahwa tindakan mitigasi tersebut telah dilakukan oleh pihak unit Infrastruktur Teknologi Informasi (IsTI).
3. Penentuan rekomendasi dilakukan dengan menganalisis *assessment* prioritas *Governance & Management Objective* (GMO) dan mengidentifikasi kontrol yang sesuai berdasarkan GMO terpilih. Penelitian ini menghasilkan APO11.01, APO11.03, APO11.04, APO11.05, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, BAI08.01, BAI08.02, BAI08.03, dan BAI08.04 rekomendasi praktik CSA berdasarkan panduan kerangka kerja COBIT 2019 yang dapat dijalankan atau diimplementasikan pada unit Infrastruktur Teknologi Informasi (IsTI) Direktorat Pusat Teknologi Informasi (PuTI) Universitas Telkom dengan menyesuaikan dari proses bisnis maupun kebutuhan TI organisasi.

REFERENSI

[1] Agus. (2017, 12 01). Control Self Assessment. Retrieved from BAB-10-INTERNAL-AUDIT-FIX: https://123dok.com/document/qoo6edmq-makalah-control-self-assessment.html

[2] B, A., S, I., & A, L. (2021, Desember). Rencana Audit Teknologi Informasi Menggunakan COBIT 2019 Pada Unit RiYanTI Universitas Telkom, 06, 336-347. Retrieved from openlibrary.telkomuniversity.ac.id

[3] Davies, H., & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? Global Policy, 9, 34-42.

[4] F, R., S, I., & A, L. (2021). Pengembangan Rencana Audit Teknologi Informasi pada Unit Infrastruktur Teknologi Informasi Direktorat Pusat Teknologi Informasi Universitas Telkom Menggunakan COBIT 2019. Retrieved from openlibrary.telkomuniversity.ac.id

[5] ISACA. (2018). COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY. Schaumburg, USA: ISACA.

[6] ISACA. (2018). COBIT 2019 IMPLEMENTATION GUIDE. Schaumburg, USA: ISACA.

[7] ISACA. (2018). COBIT2019 FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES. Schaumburg, USA: ISACA.

[8] Lawrence, S. G., & Theresa. (2019). Control Self-Assessment and Costs of Compliance. Journal of Management Accounting Research, 16-20.

[9] Mulyana, R., Rusu, L., & Perjons, E. (2021). IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review. In Twenty-Seventh Americas' Conference on Information Systems (AMCIS), Digital Innovation and Entrepreneurship, Virtual Conference, August 9-13, 2021. (pp. 1-10).

[10] Mulyana, R., Rusu, L., & Perjons, E. (2022). IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry. In Pacific Asia Conference on Information Systems (PACIS), AI-IS-ASIA (Artificial Intelligence, Information Systems, in Pacific Asia), Virtual Conference, July 5-9, 2022. Association for Information Systems (AIS).

[11] R, R. N., S, I., & A, L. (2021). Pengembangan Rencana Audit Teknologi Informasi Menggunakan COBIT 2019 Pada Unit Pengembangan Produk Teknologi Informasi Universitas Telkom. Retrieved from openlibrary.telkomuniversity.ac.id

[12] Soto-Acosta, P. 2020. "COVID-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear," Information Systems Management (37:4), pp. 260-266.

[13] Suharso. (2016, April 09). Konsep Dasar Control Self-Assessment. Retrieved from Memahami Konsep Dasar Control Self-Assessment (CSA): https://www.klikharso.com/2016/09/konsep-dasar-control-self-assessment-csa.html

[14] Wisnu, Pradipha Wibisono. (2014, Februari 15). Control Self-Assessment Dalam Pengauditan Internal. Retrieved from 123dok: https://123dok.com/document/qoo6edmq-makalah-control-self-assessment.html