Audit Teknologi Informasi Pada Unit Nits Pt Telkom Indonesia Tbk Menggunakan Framework Cobit 2019

1st Luthfi Rahmansyah Nandika
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
luthfirn@student.telkomuniversity.ac.id

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

3rd Ryan Adhitya Nugraha
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
ranugraha@telkomuniversity.ac.id

***Abstrak* — PT Telkom Indonesia, sebagai salah satu perusahaan TI terkemuka di Indonesia, memiliki tanggung jawab yang besar dalam menjaga keamanan dan keandalan sistem TI mereka, tetapi berdasarkan hasil pengambilan data yang dilakukan terdapat risiko yang sudah memiliki kontrol namun belum dapat mengurangi level dari risiko tersebut sehingga perlu dilakukan audit pada kontrol risiko terkait TI demi tercapainya efektivitas dari kontrol risiko pada risiko risiko terkait. Dalam konteks ini, penelitian berfokus pada audit kontrol risiko menggunakan COBIT 2019 pada PT. Telkom Indonesia. Penelitian ini menguji bagaimana rancangan kontrol risiko berdasarkan kriteria yang sudah dirancang, operasional kontrol risiko berdasarkan aktivitas kontrol risiko yang telah dilakukan, dan kontrol risiko terhadap objektif terpilih dari COBIT 2019 I&T Risk Focus Area serta menghasilkan rekomendasi sesuai kriteria dan aktivitas yang terdapat dalam objektif COBIT 2019 I&T Risk Focus Area. Penelitian ini berkontribusi terhadap pemahaman yang lebih mendalam tentang efektivitas kontrol risiko pada PT. Telkom Indonesia dalam menghadapi risiko-risiko terkait teknologi informasi.**

***Kata kunci*— COBIT 2019 I&T Risk Focus Area, Risiko IT, Kontrol Risiko, Telkom**

I. PENDAHULUAN

Perkembangan teknologi informasi (TI) yang pesat telah mengubah lanskap bisnis di berbagai sektor industri. Perusahaan saat ini sangat mengandalkan infrastruktur dan sistem TI yang handal untuk menjalankan operasi sehari-hari mereka. Namun, penggunaan TI juga membawa risiko yang signifikan. Oleh karena itu, penting bagi perusahaan untuk memastikan bahwa kontrol yang memadai telah diterapkan untuk mengelola risiko-risiko tersebut.

Perusahaan IT, termasuk PT Telkom Indonesia, berada di garis depan revolusi teknologi informasi yang terus berkembang. Dalam lingkungan yang penuh tantangan ini, penting bagi perusahaan IT untuk memastikan bahwa sistem dan infrastruktur TI mereka beroperasi dengan efisien, aman, dan sesuai dengan kebijakan yang ditetapkan. Untuk mencapai tujuan tersebut, pengelolaan risiko dan penerapan kontrol yang efektif sangatlah penting.

Salah satu kerangka kerja yang digunakan secara luas untuk mengelola risiko dan kontrol dalam lingkungan TI adalah COBIT (Control Objectives for Information and Related Technology). COBIT adalah sebuah kerangka kerja yang dikembangkan oleh Information Systems Audit and Control Association (ISACA) yang menyediakan panduan praktis bagi perusahaan dalam mengelola, mengontrol, dan mengaudit TI mereka.

COBIT telah mengalami berbagai perubahan dan penyempurnaan sejak pertama kali diperkenalkan. Pada tahun 2019, ISACA merilis versi terbaru dari COBIT, yaitu COBIT 2019. COBIT 2019 membawa perubahan signifikan dalam hal pendekatan, konsep, dan arsitektur kerangka kerja untuk memastikan kepatuhan dengan standar terbaru dan praktik terbaik dalam pengelolaan TI.

COBIT (Control Objectives for Information and Related Technology) telah menjadi salah satu kerangka kerja yang diterima secara luas dalam mengelola risiko dan kontrol dalam lingkungan TI. COBIT menyediakan pedoman praktis untuk membantu perusahaan dalam merancang, menerapkan, dan mengaudit kontrol TI yang efektif. Versi terbaru dari COBIT, yaitu COBIT 2019, menawarkan panduan yang komprehensif dan terkini dalam mengelola risiko dan pengendalian TI.

Dalam konteks audit kontrol risiko pada perusahaan IT, penggunaan COBIT 2019 dapat memberikan manfaat yang signifikan. COBIT 2019 menawarkan pendekatan yang terintegrasi dan holistik dalam mengidentifikasi, mengevaluasi, dan mengendalikan risiko-risiko yang berkaitan dengan TI perusahaan. Dengan menerapkan COBIT 2019, perusahaan dapat mengidentifikasi kontrol yang tepat untuk memitigasi risiko-risiko tersebut dan memastikan bahwa mereka sesuai dengan kebijakan, standar, dan peraturan yang berlaku.

PT Telkom Indonesia, sebagai salah satu perusahaan IT terkemuka di Indonesia, memiliki tanggung jawab yang besar dalam menjaga keamanan dan keandalan sistem TI mereka. Dalam konteks ini, audit kontrol risiko menggunakan COBIT 2019 dapat memberikan manfaat yang signifikan bagi PT Telkom Indonesia. Dengan menerapkan COBIT 2019, perusahaan dapat mengidentifikasi risiko-risiko yang ada, mengevaluasi efektivitas kontrol yang ada, dan mengambil tindakan yang tepat untuk mengurangi risiko tersebut.

Dalam konteks ini, penelitian ini akan berfokus pada audit kontrol risiko menggunakan COBIT 2019 pada PT Telkom Indonesia. Penelitian ini akan membahas implementasi

COBIT 2019 dalam pengelolaan risiko dan kontrol TI, mengidentifikasi risiko-risiko yang spesifik yang dihadapi oleh PT Telkom Indonesia, serta menganalisis keefektifan kontrol yang ada dalam mengurangi risiko-risiko tersebut. Melalui penelitian ini, diharapkan akan ditemukan temuan dan rekomendasi yang dapat membantu PT Telkom Indonesia dalam meningkatkan pengelolaan risiko dan kontrol TI mereka. Hasil penelitian ini juga dapat memberikan sumbangan pada pemahaman praktis tentang penerapan COBIT 2019 pada perusahaan IT, terutama dalam konteks industri telekomunikasi dan teknologi informasi di Indonesia.

II. KAJIAN TEORI

A. Risiko

Menurut Rejda (2008), tidak ada suatu definisi umum mengenai risiko, karena terdapat beberapa definisi yang berbeda tentang konsep risiko yang diinterpretasikan oleh berbagai profesi.

Eddie cade (2002) menyatakan bahwa definisi risiko berbedabeda, tergantung pada tujuannya. Definisi risiko yang tepat menurutnya dilihat dari sudut pandang adalah, exposure terhadap ketidakpastian pendapatan.

Menurut David MC Namee dan Georges Selim: "Risiko adalah konsep yang digunakan untuk menyatakan ketidakpastian atas kejadian dan atau akibatnya yang dapat berdampak secara material bagi tujuan organisasi".

Risiko adalah semua kemungkinan terjadinya suatu peristiwa yang bisa membuat sebuah perusahaan merugi. Meski masih berupa ketidakpastian, hendaknya perusahaan mempersiapkan solusi atau perisai serta mempertimbangkan segala kemungkinannya. Risiko adalah prospek suatu hasil yang tidak disukai (Arthur J. Keown. 2000).

B. Kontrol Risiko

Kontrol risiko, dalam konteks manajemen risiko, merujuk pada langkah-langkah atau tindakan yang diambil oleh organisasi untuk mengidentifikasi, mengevaluasi, mengurangi, atau mengelola risiko agar risiko tersebut tetap berada dalam tingkat yang dapat diterima atau sesuai dengan toleransi risiko yang ditetapkan oleh organisasi. Tujuan utama kontrol risiko adalah untuk melindungi nilai dan keberlangsungan organisasi dengan meminimalkan dampak negatif dari risiko dan memaksimalkan peluang yang positif (COSO, 2017).

C. *Risk Assesment*

Secara umum Risk Assessment berfungsi untuk mengidentifikasi risiko potensial baik yang berasal dari internal maupun eksternal organisasi, selain itu juga menilai sejauh mana dampak yang ditimbulkan oleh risiko tersebut dapat mengganggu jalannya proses bisnis dan tujuan organisasi. Besarnya dampak dapat diukur melalui penilaian Inherent Risk dan Residual Risk, serta dianalisis melalui dua perspektif antara lain Probability/Likelihood dan Impact/Consequence. (ISACA, 2012)

D. *Teknologi Informasi*

Teknologi Informasi adalah studi atau peralatan elektronika, terutama komputer, untuk menyimpan, menganalisa, dan mendistribusikan informasi apa saja, termasuk kata-kata, bilangan, dan gambar (kamus Oxford, 1995)

Menurut Haag & Keen (1996), "Teknologi Informasi adalah seperangkat alat yang membantu anda bekerja dengan informasi dan melaksanakan tugas-tugas yang berhubungan dengan pemrosesan informasi". Menurut Martin (1999), "Teknologi Informasi tidak hanya terbatas pada teknologi komputer (software & hardware) yang digunakan untuk memproses atau menyimpan informasi, melainkan juga mencakup teknologi komunikasi untuk mengirimkan informasi". Menurut Alter (1992), teknologi informasi mencakup perangkat keras dan perangkat lunak untuk melaksanakan satu atau sejumlah tugas pemrosesan data seperti menangkap, mentransmisikan, menyimpan, mengambil, memanipulasi, atau menampilkan data.

Menurut William dan Sawyer (2003), teknologi informasi adalah teknologi yang menggabungkan komputasi (komputer) dengan jalur komunikasi berkecepatan tinggi yang membawa data, suara, dan vidio.

Secara lebih umum, Lucas (2000), menyatakan teknologi informasi adalah segala bentuk teknologi yang diterapkan untuk memproses dan mengirimkan informasi dalam bentuk elektronis. Mikrokomputer, komputer, mainframe, pembaca barcode, perangkat lunak pemroses transaksi, perangkat lunak lembar kerja (spreadsheet), dan peralatan komunikasi dari jaringan merupakan contoh teknologi informasi.

E. Audit

Menurut Agoes (2012:4) audit adalah suatu pemeriksaan yang dilakukan secara kritis dan sistematis oleh pihak yang independen terhadap laporan keuangan yang telah disusun oleh manajemen, beserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut. Menurut Mulyadi (2014:9) audit adalah suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pernyataan- pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian setara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasil kepada pemakai yang berkepentingan.

Audit menurut Arens dkk. (2015:2) adalah pengumpulan dan evaluasi buku tentang informasi untuk menentukan dan melaporkan derajat kesesuaian antara informasi itu dan kriteria yang telah ditetapkan. Berbagai pengertian dapat dikatakan bahwa audit merupakan suatu proses pemeriksaan yang dilakukan secara sistematik terhadap laporan keuangan, pengawasan intern, dan catatan akuntansi suatu perusahaan. Audit bertujuan untuk mengevaluasi dan memberikan pendapat mengenai kewajaran laporan keuangan berdasarkan bukti-bukti yang diperoleh dan dilakukan oleh seorang yang independen dan kompeten. Menurut Sanyoto (2007) yang dimaksud audit adalah proses pengumpulan dan penilaian bahan bukti tentang informasi untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan dan dilakukan oleh orang yang kompeten dan independen.

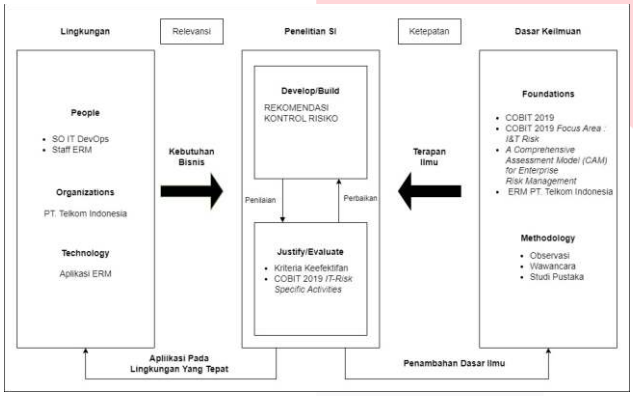
Dari pengertian diatas, dapat disimpulkan bahwa audit adalah proses pengumpulan dan evaluasi bukti dengan tujuan untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria –kriteria yang telah ditetapkan. Tujuan Audit

Adalah mendapatkan informasi faktual dan signifikan berupa data hasil analisa, penilaian, rekomendasi auditor yang dapat digunakan oleh *auditee* atau manajemen untuk berbagai keperluan misalnya untuk dasar pengambilan keputusan, pengendalian manajemen, perbaikan atau perubahan dalam berbagai aspek dalam upaya mengamankan kebijakan dan mencapai tujuan organisasi secara keseluruhan

III. METODOLOGI PENELITIAN

A. Model Konseptual

Konseptual model merupakan sebuah struktur yang digambarkan dalam sebuah diagram, yang merepresentasikan keterkaitan antar konsep sehingga dapat menguasai, menerapkan, mengevaluasi penelitian TI (Hevner, 2004). Penelitian ini menggunakan kerangka kerja tersebut guna membantu memecahkan masalah dengan memperhubungkan teori.



GAMBAR III. 1
Model Konseptual

Model konseptual dapat dijelaskan dengan cara berikut:

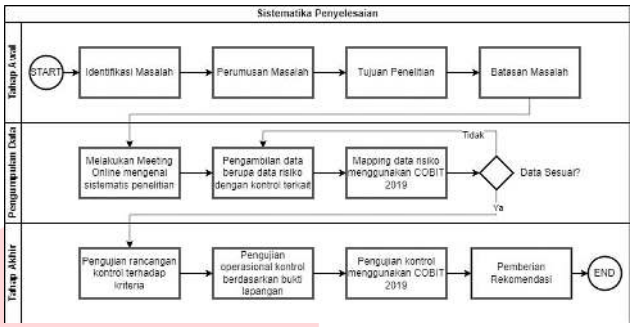
1. People
2. Organisasi
3. Technology
4. Membangun/Mengembangkan
5. Evaluate
6. Dasar
7. Metodologi
8. Data

B. Sistematika Penyelesaian Masalah

Penelitian Audit Teknologi Informasi Pada Unit NITS PT Telkom Indonesia Tbk mendayagunakan COBIT 2019 *I&T Risk* dilakukan di salah satu perusahaan yang bergerak dibidang telekomunikasi dan berada di bawah naungan Badan Usaha Milik Negara (BUMN) Tujuan dari audit ini adalah untuk memastikan bahwa organisasi menjalankan praktik-praktik yang sesuai dengan rekomendasi COBIT guna mencapai tujuan bisnis, mengelola risiko, dan menjaga integritas sistem.

Namun, terkadang ada perbedaan antara praktik yang seharusnya dilakukan berdasarkan COBIT dengan apa yang sebenarnya dilakukan dalam praktik operasional organisasi. Oleh karena itu, audit ini akan melihat sejauh mana perbedaan ini terjadi, apakah ada kesenjangan antara standar COBIT dan implementasi nyata dalam organisasi.

Dengan membandingkan apa yang diharapkan oleh COBIT dengan situasi yang ada di lapangan, organisasi dapat mengidentifikasi area di mana mereka perlu meningkatkan kepatuhan terhadap standar COBIT atau melakukan perbaikan dalam praktik operasional mereka agar lebih sesuai dengan panduan yang diberikan oleh kerangka kerja tersebut.. Adapun alur sistematika penelitian yang dilakukan seperti pada Gambar III.2.



GAMBAR III. 2
Sistematika Penyelesaian Masalah

C. Pengumpulan Data

Penelitian ini menggunakan tipe penelitian deskriptif kualitatif. Metode deskriptif dapat diartikan sebagai prosedur pemecahan masalah yang diselidiki dengan menggambarkan keadaan subjek/objek penelitian (seseorang, lembaga, masyarakat dan lain-lain) pada kondisi saat ini yang didapat dari sumber data dan fakta sebagaimana adanya. Data tersebut berasal dari naskah wawancara, catatan di lapangan, foto, video, dokumen pribadi, dan dokumen resmi lainnya. Metode Pengumpulan Data:

1. Data Primer

a. Wawancara: Pengumpulan data pada penelitian ini dilakukan dengan cara berkomunikasi langsung dengan pihak yang dapat memberikan informasi terhadap permasalahan yang sedang diteliti. Wawancara dilakukan langsung kepada Staff ERM PT Telkom Indonesia

b. Observasi: Pengumpulan data melalui pengamatan dan pencatatan data secara langsung di lapangan terhadap proses yang terjadi.

2. Data Sekunder

a. Studi Pustaka: Metode pengumpulan data dengan mencari data kepustakaan berupa buku, jurnal ilmiah, e-book, dan lain sebagainya yang memiliki kaitannya dengan penelitian ini.

IV. PENGUMPULAN DAN ANALISIS DATA

A. Kriteria Keefektifan Kontrol Risiko

Pada tahap ini, dilakukan penentuan kriteria yang nantinya dijadikan sebagai acuan nilai dari keefektifan kontrol risiko. Penelitian ini mengadopsi model *Evaluating Internal Control Systems: A Comprehensive Assessment Model (CAM) for Enterprise Risk Management* yang dikembangkan oleh Carolyn Dittmeier dan Paolo Casati sebagai kerangka penilaian untuk mengidentifikasi dan mengevaluasi sistem pengendalian internal dalam konteks manajemen risiko

perusahaan. Keefektifan kontrol risiko dapat dilihat dari 6 (enam) poin, yaitu:

1. Apabila kontrol risiko yang dikembangkan telah dirumuskan secara tertulis dan memadai.
2. Apabila kontrol risiko yang dikembangkan telah terbukti berhasil menurunkan level risiko.
3. Apabila kontrol risiko yang dikembangkan telah dilakukan pengawasan bertahap, pengawasan dapat dilakukan harian, mingguan, bulanan, triwulanan, tahunan.
4. Apabila kontrol risiko yang dikembangkan terdapat Segregation of Duties.
5. Apabila kontrol risiko yang dikembangkan telah dinyatakan lulus Independent Test of Control (IToC).
6. Apabila kontrol risiko yang dikembangkan diperbarui secara berkala.

Dari enam poin diatas, jika terdapat poin yang belum terpenuhi, maka harus diberikan rekomendasi pada kontrol risiko terkait.

B. Analisis Data

Tahap ini akan berfokus pada analisis *Risk Register* milik PT Telkom Indonesia, sehingga nantinya dapat menentukan keefektifan dari kontrol risiko terhadap risiko terkait.

1. Daftar Risiko

Berdasarkan diskusi yang sudah dilakukan dengan pihak Enterprise *Risk Management* Telkom dan *Risk Register*, terdapat 10 risiko dengan level *Medium* dan *High* yang sudah dipilih untuk dilakukan audit pada kontrol risikonya.

TABEL IV. 1
Daftar Risiko

Unit	No Risiko	Nama Risiko	Deskripsi Risiko	Level Risiko	*Risk Owner*	*Activity* PIC
Information Technology	O1	*Cyber Attack*	Risiko yang terjadi karena fraud terhadap sistem dan aplikasi perusahaan.	*Medium*	SM SERVICE PLATFORM DEVELOPMENT	SM CAH MANAGEMENT OPERATION CONTROL DE
Information Technology	O2	IT Operational Interruption	Risiko yang terjadi pada *cloud* akibat *lack of computing power*	*High*	SM SERVICE PLATFORM DEVELOPMENT	MGR SDN CLOUD & DATA CENTER DEVELOPMENT
Service Operation	O3	Layanan Internet Degrade	Penurunan kualitas layanan internet, akibat link *congest* (penuh) atau putus	*High*	MGR IP TOOLS OPERATION & PROGRAM PERF	OSM CONNECTIVITY OPERATION
Service Operation	O4	Tingginya *Latency* 4G	Memastikan *latency* 4G optimal sesuai threshold SLA<20 ms	*Medium*	OSM CNOP NETWORK QUALITY	OSM CNOP NETWORK QUALITY
Service Operation	O5	Tingginya *Packet loss* 4G di area JaBo	Memastikan *packet loss* 4G optimal sesuai *threshold* SLA <0,1%	*High*	OSM CNOP NETWORK QUALITY	OSM CNOP NETWORK QUALITY
Service Operation	O6	Gangguan pada mini-OLT yang menyebabkan downtime terhadap layanan pelanggan	Gangguan pada mini-OLT yang menyebabkan downtime terhadap layanan pelanggan yang dapat disebabkan oleh matinya catuan PLN, pihak ke-3, vandalisme dan bencana alam sehingga berdampak kepada tidak tercapainya *availability of service* dari mini-OLT.	*High*	OSM ACCESS NETWORK OPERATION	OSM ACCESS NETWORK OPERATION
Service Operation	O7	Terhentinya operasional infrastruktur dan sistem IT (ME Network Element)	Tidak tersedianya Service Perangkat *Mechanical Electrical* (ME) di *Network* / IT Infrastruktur yang mengakibatkan terganggunya operasional dan layanan Perusahaan	*High*	OSM DC, DEFA OPERATION & TECHNICAL SUPP	OSM DC, DEFA OPERATION & TECHNICAL SUPP
Service Operation	O8	Terhentinya operasional infrastruktur dan sistem IT (Backbone FO system)	Risiko terjadinya gangguan terhadap *Network* (*Backbone*) / IT Infrastruktur yang secara signifikan dapat	*High*	OSM OPERATION ENGINEERING	OSM OPERATION ENGINEERING

			mengganggu operasional dan layanan Perusahaan.			
Service Operation	O9	Terjadi gangguan *massive* di layer agregasi (Metro) dan core setelah implementasi *Future State Architecture* CNOP yang berimpact terhadap *Availability Core* dan Agregat	Risiko pengawalan operasional pasca migrasi Future State Architecture CNOP (L3VPN dan OneIPMPLS), dimana sebelumnya layer core layanan CNOP menjadi SoW Telkomsel, sekarang berpindah menjadi SoW Telkom.	*High*	OSM CNOP SERVICE OPERATION	OSM CNOP SERVICE OPERATION
Service Operation	O10	Risiko terjadinya gangguan massive / critical pada jaringan layanan Telkomsel sehingga target *availability network access* tidak tercapai	Risiko terjadinya gangguan pada infrastruktur yang berimpact pada *service* Telkomsel dan akan mempengaruhi pencapaian *availability site* > 93,6%.	*Medium*	OSM CNOP SERVICE OPERATION	OSM CNOP SERVICE OPERATION

2. Daftar Kontrol

Berdasarkan Risiko yang dipilih diatas, berikut adalah daftar kontrol yang dilakukan oleh PT Telkom dalam melakukan aktivitas mitigasi pada risiko diatas.

TABEL IV. 2
Daftar Kontrol

No Risiko / Unit	Nama Risiko	Kontrol Risiko	Aktivitas
O1 / IT	Cyber Attack	Hardening Cyber Security Telkom Group sehingga tidak terjadi Fraud yang dilakukan oleh privilege user (Zero Fraud)	Monitoring aktivitas *privilege user* menggunakan PAM.
O2 / IT	IT Operational Interruption	Implementasi *Cloud Native Bare-metal environment* di *Data Center* AON dan kemampuan mengelola *multi platform service* (*virtualization, container, physical*) dan *multi cloud service (private-cloud & public-cloud environment)*	Pengawalan Projek Penambahan *resource computing power*
O3 / SO	Layanan Internet Degrade	Mempertahankan *compliance* okupansi link IP *Network* berada di atas target PI NITS sebesar 63%	1. *Reengineering port*, modul, dan node eksisting seoptimal mungkin 2. Rebalancing traffic
		Koordinasi berkala dalam forum PLANO dengan DID untuk mempercepat laju penambahan kapasitas link	1. Forum Plano Rutin dengan DID sebagai upaya percepatan deployment pada link dan node kritis. 2. Skenario *ON DESK* untuk mempersiapkan segala kemungkinan yang dapat terjadi pada *network* IP Telkom, sehingga memudahkan pengambilan langkah pada saat terjadi gangguan berskala nasional. (Dokumen *Always ON*) 3. Menerapkan klasifikasi service ke dalam beberapa tingkatan prioritas (QOS)
O4 / SO	Tingginya *Latency* 4G	Melakukan *weekly* monitoring untuk mengetahui area yang perlu dilakukan *improvement*	1. Menghitung *latency* 4G secara mingguan untuk mengetahui area yang perlu dilakukan *improvement* 2. Melakukan diskusi secara rutin kepada regional untuk pengawalan *latency* area
		Melakukan assess untuk menemukan rootcause dan solusi perbaikan *latency*	Melakukan assessment pada area yang memerlukan perbaikan *latency* untuk menemukan RCA dan solusi yang dapat diakukan
		Meningkatkan koordinasi dengan tim CSO untuk pengawalan infrastruktur jaringan	Melakukan diskusi secara rutin dengan tim CSO terkait mitigasi gangguan jaringan
		Melakukan *monitoring* utilisasi ketika terjadi gangguan	Melakukan *monitoring* utilisasi secara berkala saat terjadi gangguan SKKL yang cukup *massive*
O5 / SO	Tingginya *Packet loss* 4G di area	Melakukan *weekly* monitoring untuk mengetahui area yang perlu dilakukan *improvement*	1. Perhitungan pencapaian *packet loss* setiap minggu 2. Penentuan area prioritas untuk

	JaBo		area yang masih mengalami *packet loss* paling besar
		Melakukan aktivitas perbaikan *packet loss* sesuai dengan RCA yang didapatkan dari hasil assessment	1. Assessment terhadap *site-site* yang mencalami *packet loss* untuk mendapatkan RCA 2. Action perbaikan *packet loss* sesuai RCA yang diperoleh seperti perbaikan suhu, perbaikan redaman, config tcont, dll. 3. Koordinasi dengan bidang terkait (ANO, CSO, DWS, MSO). 4. Monitoring hasil perbaikan untuk evaluasi
		Penambahan teknisi squat romeo dan SoW Quality untuk percepatan penanganan ticket quality	1. Pembuatan amandemen squat romeo untuk perluasan SoW *quality* dan penambahan teknisi 2. Pembuatan ticket quality untuk order perbaikan *packet loss* kepada tim Squat Romeo
O6 / SO	Gangguan pada mini-OLT yang menyebabkan *downtime* terhadap layanan pelanggan	Pembaharuan baterai mini-OLT	1. Penyediaan beberapa genset portable 2. Penggantian baterai mini-zOLT
		Patroli Preventif	1. Pembuatan Notifikasi bot telegram ketika PLN Off dan *Battery* akan habis (untuk OLT Huawei, ZTE dan Fiberhome) 2. Pengusulan probis penanganan vandalism dan bencana alam ke STA NITS 3. Pembuatan bot Alarm di Telegram dengan parameter Door open/Door Alarm dan Battery Bunker door Alarm. 4. Dualhoming feeder untuk miniOLT ke DID 5. Pengawalan jaringan (Patroli)
O7 / SO	Terhentinya operasional infrastruktur dan sistem IT (ME Network Element)	Memastikan sistem redudasi perangakat ME berfungsi normal	1. *Improvement* IT Tools untuk O&M perangkat DEFA 2. Melaksanakan rehearsal test perangkat DEFA secara periodik
		Mengoptimalkan sebaran teknisi pada kontrak Manage Operation perangkat DEFA	Mereview sebaran teknisi agar sesuai dengan kebutuhan O&M di semua lokasi
		Meningkatkan kompetensi teknisi	Program pelatihan, sertifikasi atau pelaksanaan BIT
		Pengawalan serta evaluasi mitra Manage Operation secara periodik	UJi petik performansi mitra
O8 / SO	Terhentinya operasional infrastruktur dan sistem IT (Backbone FO system)	Meningkatkan koordinasi dengan ASKALSI (Asosiasi Kabel Laut Seluruh Indonesia) dan BAKAMLA untuk pengamanan SKKL	1. Beberapa kegiatan melalui ASKALSI terkat dengan kebijakan dengan berbagai pihak 2. Penggunaan aplikasi SCS-AIS untuk monitoring kapalyang mendekati/melintasdi Jalur SKKL
		Meningkatkan koordinasi dan pengawalan pekerjaan pihak ke-3 dibantu dengan system aplikasi monitoring dan meningkatkan Disiplin Operasi dan Kepedulian terhadap Lingkungan Kerja melalui Gerakan #PeduliInfrastruktur	1. Evaluasi MS Squat Bravo 2. Empowering monitoring menggunakan Toos Aplikasi (The Patrol)
		Meningkatkan koordinasi dengan Aparat Penegak Hukum untuk operasi di lokasi rawan criminal dan melakukan program bina lingkungan	1. Melaporkan informasi FO Cut akibat vandalisme/pencurian dari kegiatan Patroli Rutin Squat Bravo ke SAS di Witelnya. 2. Melaksanaan Wasmansus dan koordinasi dengan pihak terkait untuk pengamanan Network 3. Support anggaran ke TREG untuk kegiatan Wasman melalui RRA
		Memastikan system backup ME berfungsi sesuai standar	1. Konsistensi checklist dan preventive maintanance
			2. Pengukuran kapasitas redudansi secara berkala 3. Enhancement early warning system 4. Rehearsal Test untuk memastikan fungsi backup NE berjalan lancar
O9 / SO	Terjadi gangguan massive di layer agregasi (Metro) dan core setelah implementasi Future State Architecture CNOP yang berimpact terhadap Availability Core dan Agregat	Mengupgrade Knowledge EOS TIOC dan Refreshment knowledge to all TREG	1. Sharing Knowledge dan update informasi kepada EOS untuk Service2 yang baru di migrasikan. 2. Sharing knowledge dan diskusi dengan regional (MSO, RNO) 3. Evaluasi sharing knowledge dan operasional implementasi FSA
		Prioritas Pemenuhan Renewal Kontrak MS Setiap Tahunnya	1. Pemenunan renewal kontrak MS PE - Mobile (One IPMPLS) 2. Pemenuhan renewal kontrak MS Metro (termasuk L3VPN)
		Memastikan proses migrasi FSA CNOP berjalan lancar tanpa mengganggu layanan dan live network	1. Read-out dan assessment MOP dalam review meeting persiapan activity migrasi / fulfillment 2. Pengawalan proses migrasi FSA CNOP yang dipimpin oleh Duty Manager (Band II)

O10	Risiko terjadinya gangguan massive / critical pada jaringan layanan Telkomsel sehingga target availability network akses tidak tercapai	Program dual track transport layanan Telkomsel	Pengawalan program SPOF Clearance dan program transport *improvement* berdasarkan incident yang sudah terjadi
		Melakukan patroli jaringan akses	Solusi Penambahan tim teknisi patroli akses serta pemberlakuan KPI based on Performance Teknisi

3. Pemetaan Risiko pada COBIT 2019 *Governance and Management Objectives*

Pada tahap ini, dilakukan pemetaan tiap risiko terhadap GMO COBIT 2019 yang berkaitan.

TABEL IV. 3
Pemetaan Risiko pada COBIT 2019 *Governance and Management Objectives*

No Risiko	Nama Risiko	Deskripsi Risiko	Skenario Risiko	Objektif Terkait	Prioritas Objektif
O1	Cyber Attack	Risiko yang terjadi karena fraud terhadap sistem dan aplikasi perusahaan.	User Access Rights Management	• APO01 • APO07 • APO12 • APO13 • APO14 • BAI06 • BAI07 • BAI09 • BAI10 • DSS01 • DSS04 • DSS05 • DSS06	DSS05
				• MEA02 • MEA04	
O2	IT Operational Interruption	Risiko yang terjadi pada cloud akibat lack of computing power	IT Hardware	• APO10 • DSS01 • DSS04	DSS04
O3	Layanan Internet Degrade	Penurunan kualitas layanan internet, akibat link congest (penuh) atau putus	IT Hardware	• APO10 • DSS01 • DSS04	DSS01
O4	Tingginya *Latency* 4G	Memastikan *latency* 4G optimal sesuai threshold SLA<20 ms	IT Operation	• BAI06 • BAI08 • DSS01 • DSS02 • DSS03 • DSS04 • DSS05 • DSS06 • MEA02	DSS02
O5	Tingginya *Packet loss* 4G di area JaBo	Memastikan *packet loss* 4G optimal sesuai threshold SLA <0,1%	IT Operation	• BAI06 • BAI08 • DSS01 • DSS02 • DSS03	DSS02
				• DSS04 • DSS05 • DSS06 • MEA02	
O6	Gangguan pada mini-OLT yang menyebabkan downtime terhadap layanan pelanggan	Gangguan pada mini-OLT yang menyebabkan downtime terhadap layanan pelanggan yang dapat disebabkan oleh matinya catuan PLN, pihak ke-3, vandalisme dan bencana alam sehingga berdampak kepada tidak tercapainya availability of Service dari mini-OLT.	Internal and external security threats	• APO01 • APO12 • APO13 • BAI03 • BAI06 • BAI10 • DSS02 • DSS04 • DSS05 • MEA01 • MEA02 • MEA03 • MEA04	DSS04
O7	Terhentinya operasional infrastruktur dan sistem IT (ME Network Element)	Tidak tersedianya Service Perangkat Mechanical Electrical (ME) di Network / IT Infrastruktur yang mengakibatkan terganggunya operasional dan layanan Perusahaan	IT Expertise, Skills And Behavior	• EDM04 • APO07	EDM04
O8	Terhentinya operasional infrastruktur dan sistem IT (Backbone FO system)	Risiko terjadinya gangguan terhadap Network (Backbone) / IT Infrastruktur yang secara signifikan dapat mengganggu operasional dan layanan Perusahaan.	Internal And External Security Threats	• APO12 • APO13 • BAI03 • BAI06 • BAI10 • DSS02 • DSS04 • DSS05 • MEA01 • MEA02 • MEA03 • MEA04	
O9	Terjadi gangguan massive di layer agregasi (Metro) dan core setelah implementasi Future State Architecture CNOP yang berimpact terhadap Availability Core dan Agregat	Risiko pengawalan operasional pasca migrasi Future State Architecture CNOP (L3VPN dan OnelPMPLS), dimana sebelumnya layer core layanan CNOP menjadi SoW Telkomsel, sekarang berpindah menjadi SoW Telkom.	IT Expertise, Skills And Behavior	• EDM04 • APO07	APO07
O10	Risiko terjadinya gangguan massive / critical pada jaringan layanan Telkomsel sehingga target availability network akses tidak tercapai	Risiko terjadinya gangguan pada infrastruktur yang berimpact pada service Telkomsel dan akan mempengaruhi pencapaian availability site > 93,6%.	Internal And External Security Threats	• APO01 • APO12 • APO13 • BAI03	MEA04
				• BAI06 • BAI10 • DSS02 • DSS04 • DSS05 • MEA01 • MEA02 • MEA03 • MEA04	

V. PENGUJIAN DAN REKOMENDASI

A. Pengujian Kontrol Risiko

Setelah melakukan analisis pada risiko beserta kontrolnya, maka selanjutnya akan dilakukan tahap pengujian kontrol risiko. Dilakukan pengujian keefektifan kontrol risiko terhadap data risiko yang terkait. Tahap ini dilakukan dari dua sisi, yaitu:

1. Rancangan: Pengujian dari sisi rancangan dilakukan dengan menganalisis seberapa tepatnya desain dari kontrol terhadap risiko terkait.
2. Operasional: Pengujian dari sisi operasional dilakukan dengan menganalisis bagaimana kondisi lapangan dari pelaksanaan rancangan kontrol risiko.
3. Pengujian Kontrol Risiko pada Operasional menggunakan COBIT 2019

Setelah melakukan penilaian kontrol untuk setiap risiko yang terkait dengan objektif yang sudah dimapping, berikut hasil penilaian untuk masing - masing aktivitas dapat ditemukan pada sub-bab berikut.

a. Risiko O1 (Objektif DSS05)

TABEL V. 1
Risiko O1 (Objektif DSS05.04)

DSS05.04 Mengelola identitas pengguna dan akses logis.		
Memastikan bahwa semua pengguna memiliki hak akses informasi sesuai dengan persyaratan bisnis. Berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis.		
Description	Answer	Evidence
Memelihara hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan. Menyesuaikan manajemen identitas dan hak akses dengan peran dan tanggung jawab yang telah ditentukan, berdasarkan prinsip hak terendah, kebutuhan harus ada, dan kebutuhan untuk mengetahui.	Yes	Terdapat pembagian role dan hak akses pada aplikasi ERM milik PT Telkom
Mengelola semua perubahan hak akses (pembuatan, modifikasi, dan penghapusan) tepat waktu berdasarkan hanya pada transaksi yang telah disetujui dan didokumentasikan, yang diotorisasi oleh individu manajemen yang ditunjuk.	Yes	Pengimplementasian Priviledge Access Management menurut Laporan Triwulan IV
Memisahkan, mengurangi jumlahnya menjadi sekecil mungkin yang diperlukan, dan mengelola akun pengguna dengan hak istimewa secara aktif. Pastikan pemantauan pada semua aktivitas yang terjadi pada akun-akun tersebut.	Yes	Pengimplementasian Priviledge Access Management menurut Laporan Triwulan IV
Mengidentifikasi secara unik semua kegiatan pemrosesan informasi berdasarkan peran fungsional. Berkoordinasi dengan unit bisnis untuk memastikan bahwa semua peran didefinisikan secara konsisten, termasuk peran yang didefinisikan oleh bisnis itu sendiri dalam aplikasi proses bisnis.	Yes	Pengimplementasian Priviledge Access Management menurut Laporan Triwulan IV
Mengotentikasi semua akses ke aset informasi berdasarkan peran individu atau aturan bisnis. Berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan dalam	Yes	Terdapat pembagian role dan hak akses pada aplikasi ERM milik PT Telkom
proses bisnis untuk memastikan bahwa kontrol otentikasi telah dikelola dengan benar.		
Memastikan bahwa semua pengguna (internal, eksternal, dan sementara) dan aktivitas mereka pada sistem TI (aplikasi bisnis, infrastruktur TI, operasi sistem, pengembangan, dan pemeliharaan) dapat diidentifikasi secara unik.	Yes	Pengimplementasian Priviledge Access Management menurut Laporan Triwulan IV
Memelihara jejak audit dari akses ke informasi berdasarkan sensitivitasnya dan persyaratan regulasi.	No	Tidak terdapat bukti jejak pengaksesan informasi
Melakukan tinjauan manajemen secara berkala terhadap semua akun dan hak-hak terkait.	Yes	Dilakukan monitor pada aktivitas user menurut Laporan Triwulan IV

b. Risiko O2 (Objektif DSS04)

TABEL V. 2
Risiko O2 (Objektif DSS04.03)

DSS04.03 Mengembangkan dan melaksanakan respons kelangsungan bisnis.			
Mengembangkan rencana kelangsungan bisnis (BCP) dan rencana pemulihan bencana (DRP) berdasarkan strategi yang telah ditentukan. Mendokumentasikan semua prosedur yang diperlukan agar perusahaan dapat melanjutkan aktivitas kritis dalam kejadian insiden.			
Activities	Description	Answer	Evidence
1	Memberikan semua pihak terkait sesi pelatihan berkala tentang prosedur BCP dan DRP serta peran dan tanggung jawab mereka dalam menghadapi kejadian atau bencana.	No	Belum ada pelatihan mengenai peran dan tanggung jawab ketika ada insiden
2	Memverifikasi dan meningkatkan pelatihan sesuai dengan hasil dari uji coba kontinjensi.	No	Belum ada pelatihan berdasarkan hasil *contingency tests*
3	Menentukan apakah telah dilakukan penilaian risiko yang mengidentifikasi paparan bisnis dan operasional.	Yes	Sudah ada identifikasi risiko terhadap bisnis dan operasional pada Laporan Triwulan
4	Memastikan bahwa langkah-langkah penilaian kerusakan dengan titik keputusan dan ambang batas yang formal telah ditetapkan untuk mengaktifkan rencana tersebut.	Yes	Sudah terdapat pada Laporan Triwulan

c. Risiko O4 (Objektif DSS02)

TABEL V. 3
Risiko O4 (Objektif DSS02.01)

DSS02.01 Menentukan skema klasifikasi untuk insiden dan permintaan layanan.			
Menentukan skema dan model klasifikasi untuk insiden dan permintaan layanan.			
Activities	Description	Answer	Evidence
1	Menentukan skema dan prioritas klasifikasi untuk insiden dan permintaan layanan, serta kriteria untuk pendaftaran masalah. Gunakan informasi ini untuk memastikan pendekatan yang konsisten dalam menangani dan memberitahukan pengguna tentang masalah serta melakukan analisis tren.	Yes	Sudah terdapat dalam SOP penginputan risiko pada ERM
2	Definisikan model insiden untuk kesalahan yang diketahui guna memungkinkan pemecahan masalah yang efisien dan efektif.	Yes	Sudah terdapat keterangan model insiden pada Laporan Triwulan
3	Definisikan model permintaan layanan berdasarkan jenis permintaan layanan untuk memungkinkan bantuan mandiri dan pelayanan yang efisien untuk permintaan standar.	No	Belum ada definisi mengenai service request models
4	Definisikan aturan dan prosedur eskalasi insiden, terutama untuk insiden besar dan insiden keamanan.	No	Belum ada aturan dan prosedur mengenai eskalasi saat adanya insiden besar
5	Definisikan sumber pengetahuan tentang insiden dan permintaan, dan jelaskan bagaimana cara menggunakannya	Yes	Sudah terdapat definisi mengenai sumber masalah pada Lesson Learned Laporan Triwulin

TABEL V. 4
Risiko O4 (Objektif DSS02.02)

DSS02.02 mencatat, mengklasifikasikan, dan memberikan prioritas pada permintaan dan insiden.			
Mengidentifikasi, mencatat, dan mengklasifikasikan permintaan layanan dan insiden serta menetapkan prioritas berdasarkan kritikalitas bisnis dan kesepakatan layanan.			
Activities	Description	Answer	Evidence
1	Catat semua permintaan layanan dan insiden, mencatat semua informasi yang relevan, sehingga dapat ditangani dengan efektif dan catatan historis lengkap dapat dipertahankan.	Yes	Sudah ada catatan mengenai service request dan incident dalam Laporan Triwulan
2	Untuk memungkinkan analisis tren, klasifikasikan permintaan layanan dan insiden dengan mengidentifikasi jenis dan kategori.	Yes	Sudah ada identifikasi insiden pada Laporan Triwulan
3	Memprioritaskan permintaan layanan dan insiden berdasarkan definisi SLA (Service Level Agreement) mengenai dampak bisnis dan urgensi.	No	Belum ada bukti pemrioritasan service request dan insiden berdasarkan SLA

d. Risiko O5 (Objektif DSS02)

TABEL V. 5
Risiko O5 (Objektif DSS02.01)

DSS02.01 Mendefinisikan skema klasifikasi untuk insiden dan permintaan layanan.			
Mendefinisikan skema dan model klasifikasi untuk insiden dan permintaan layanan.			
Activities	Description	Answer	Evidence
1	Menentukan skema dan prioritas klasifikasi untuk insiden dan permintaan layanan, serta kriteria untuk pendaftaran masalah. Gunakan informasi ini untuk memastikan pendekatan yang konsisten dalam menangani dan memberitahukan pengguna tentang masalah serta melakukan analisis tren.	Yes	Sudah terdapat dalam SOP penginputan risiko pada ERM
2	Definisikan model insiden untuk kesalahan yang diketahui guna memungkinkan pemecahan masalah yang efisien dan efektif.	Yes	Sudah ada insiden yang berkaitan dengan kesalahan yang sudah diketahui sebelumnya menurut root cause Laporan Triwulan
3	Definisikan model permintaan layanan berdasarkan jenis permintaan layanan untuk memungkinkan bantuan mandiri dan pelayanan yang efisien untuk permintaan standar.	No	Belum ada definisi mengenai service request models
4	Definisikan aturan dan prosedur eskalasi insiden, terutama untuk insiden besar dan insiden keamanan.	No	Belum ada aturan dan prosedur mengenai eskalasi saat adanya insiden besar
5	Definisikan sumber pengetahuan tentang insiden dan permintaan, dan jelaskan bagaimana cara menggunakannya	Yes	Sudah terdapat definisi mengenai sumber masalah pada Lesson Learned Laporan Triwulin

TABEL V. 6
Risiko O5 (Objektif DSS02.02)

DSS02.02 Rekam, klasifikasikan dan prioritaskan permintaan dan insiden.			
Mengidentifikasi, mencatat, dan mengklasifikasikan permintaan dan insiden layanan, serta menetapkan prioritas sesuai dengan kekritisan bisnis dan perjanjian layanan.			
Activities	Description	Answer	Evidence
1	Catat semua permintaan layanan dan insiden, mencatat semua informasi yang relevan, sehingga dapat ditangani dengan efektif dan catatan historis lengkap dapat dipertahankan.	Yes	Sudah ada catatan mengenai service request dan incident dalam Laporan Triwulan
2	Untuk memungkinkan analisis tren, klasifikasikan permintaan layanan dan insiden dengan mengidentifikasi jenis dan kategori.	No	Belum ada identifikasi tipe dan kategori insiden
3	Memprioritaskan permintaan layanan dan insiden berdasarkan definisi SLA (Service Level Agreement) mengenai dampak bisnis dan urgensi.	No	Belum ada bukti pemrioritasan service request dan insiden berdasarkan SLA

TABEL V. 7
Risiko O5 (Objektif DSS02.07)

DSS02.07 Melacak status dan menghasilkan laporan.			
Secara rutin melacak, menganalisis, dan melaporkan insiden serta pemenuhan permintaan. Memeriksa tren untuk memberikan informasi bagi perbaikan berkelanjutan.			
Activities	Description	Answer	Evidence
1	Memantau dan melacak eskalasi dan resolusi insiden serta prosedur penanganan permintaan untuk mencapai kemajuan menuju penyelesaian atau penyelesaian penuh.	Yes	Sudah dilakukan pemantauan eskalasi insiden pada Laporan Triwulan
2	Identifikasi pemangku kepentingan informasi dan kebutuhan mereka akan data atau laporan. Tentukan frekuensi pelaporan dan media yang digunakan.	Yes	Sudah ada permintaan *support* kepada *stakeholders* terkait pada Laporan Triwulan
3	Menghasilkan dan mendistribusikan laporan tepat waktu atau menyediakan akses terkontrol ke data secara online.	Yes	Sudah ada dalam bentuk Laporan Triwulan pada ERM
4	Menganalisis insiden dan permintaan layanan berdasarkan kategori dan jenisnya. Menentukan tren dan mengidentifikasi pola dari isu-isu yang sering muncul, pelanggaran SLA (Service Level Agreement), atau ketidakefisienan.	No	Belum ada analisis dan penetapan Trend
5	Menggunakan informasi tersebut sebagai masukan (input) untuk perencanaan perbaikan berkelanjutan.	Yes	Informasi yang didapat tiap triwulan terus dijadikan sebagai improvement, dilihat dari laporan triwulan yang merujuk ke laporan sebelumnya

e. Risiko O6 (Objektif DSS04)

TABEL V. 8
Risiko O6 (Objektif DSS04.03)

DSS04.03 Mengembangkan dan melaksanakan respons kelangsungan bisnis.			
Mengembangkan rencana kelangsungan bisnis (BCP) dan rencana pemulihan bencana (DRP) berdasarkan strategi yang telah ditentukan. Mendokumentasikan semua prosedur yang diperlukan agar perusahaan dapat melanjutkan aktivitas kritis dalam kejadian insiden.			
Activities	Description	Answer	Evidence
1	Memberikan semua pihak terkait sesi pelatihan berkala tentang prosedur BCP dan DRP serta peran dan tanggung jawab mereka dalam menghadapi kejadian atau bencana.	Yes	Sudah dilakukan Workshop Integrated Management System (IMS) pada laporan triwulan
2	Memverifikasi dan meningkatkan pelatihan sesuai dengan hasil dari uji coba kontinjensi.	No	Belum ada pelatihan berdasarkan hasil *contingency tests*
3	Menentukan apakah telah dilakukan penilaian risiko yang mengidentifikasi paparan bisnis dan operasional.	Yes	Sudah ada identifikasi risiko terhadap bisnis dan operasional pada Laporan Triwulan
4	Memastikan bahwa langkah-langkah penilaian kerusakan dengan titik keputusan dan ambang batas yang formal telah ditetapkan untuk mengaktifkan rencana tersebut.	Yes	Sudah ada penilaian kerugian serta ambang batas pada laporan triwulan

f. Risiko O9 (Objektif APO07)

TABEL V. 9
Risiko O9 (Objektif APO07.02)

APO07.02 Identifikasi personel TI utama.			
Identifikasi personel TI utama. Gunakan pengambilan pengetahuan (dokumentasi), berbagi pengetahuan, perencanaan suksesi, dan cadangan staf untuk meminimalkan ketergantungan pada satu individu yang melakukan fungsi pekerjaan penting.			
Activities	**Description**	**Answer**	**Evidence**
1	Identifikasi dan latih sumber daya cadangan untuk personel kunci.	Yes	dilakukan *upgrade Knowledge* EOS TIOC dan *Refreshment knowledge to all* TREG
2	Membangun mekanisme transfer pengetahuan yang solid	Yes	dilakukan *upgrade Knowledge* EOS TIOC dan *Refreshment knowledge to all* TREG
3	Mengembangkan dan memelihara rencana suksesi untuk personil risiko utama	No	Tidak ditemukan succession plan untuk Key Risk Personnel

TABEL V. 10
Risiko O9 (Objektif APO07.03)

APO07.03 Menjaga keterampilan dan kompetensi personil.			
Mendefinisikan dan mengelola keterampilan dan kompetensi yang dibutuhkan personil. Secara teratur memverifikasi bahwa personil memiliki kompetensi untuk memenuhi peran mereka berdasarkan pendidikan, pelatihan dan / atau pengalaman mereka. Verifikasi bahwa kompetensi ini dipertahankan, menggunakan program kualifikasi dan sertifikasi yang sesuai. Memberikan karyawan pembelajaran dan kesempatan berkelanjutan untuk mempertahankan pengetahuan, keterampilan, dan kompetensi mereka pada tingkat yang diperlukan untuk mencapai tujuan perusahaan.			
Activities	Description	Answer	Evidence
1	Memberikan pelatihan dan program pengembangan profesional tentang manajemen risiko	Yes	dilakukan *upgrade Knowledge* EOS TIOC dan *Refreshment knowledge to all* TREG
2	Gunakan sertifikasi untuk memastikan keahlian profesional manajemen risiko yang berkualitas	No	Tidak ada bukti dilakukan sertifikasi untuk memastikan kualitas risk management personnel
3	Menetapkan program pendidikan, pelatihan, dan kesadaran di seluruh perusahaan yang tepat untuk risiko.	Yes	dilakukan *upgrade Knowledge* EOS TIOC dan *Refreshment knowledge to all* TREG

B. Rekomendasi

Setelah dilakukan pengujian terhadap kontrol risiko, tahap selanjutnya adalah memberikan rekomendasi terhadap tiap kontrol risiko yang perlu diberikan rekomendasi terhadap kontrol risikonya dari tiap pengujian.

1. Rekomendasi COBIT 2019

Pada bagian Rekomendasi, Penelitian ini ingin mengusulkan beberapa langkah tindakan yang dapat diambil untuk mengatasi permasalahan yang telah diidentifikasi sebelumnya.

TABEL V. 11
Rekomendasi COBIT 2019

No	Objektif	Aktivitas	Rekomendasi
O1	DSS05	DSS05.04 Mengelola identitas pengguna dan akses logis.	Perancangan sistem *tracking* penggunaan informasi berdasarkan sensitivitas dan persyaratan regulasi
O2	DSS04	*DSS04.03 Mengembangkan dan melaksanakan respons kelangsungan bisnis.*	Pengadaan pelatihan mengenai peran dan tanggung jawab
			Pengadaan pelatihan lanjutan dari hasil uji kontingensi mengenai menghadapi situasi darurat atau bencana.
O4	DSS02 Managed Service Requests and Incidents	*DSS02.01 Menentukan skema klasifikasi untuk insiden dan permintaan layanan.*	Pendefinisian *Service Request Models* yang akan digunakan untuk peningkatan efisiensi pelayanan *Service Request*
			Pendefinisian aturan dan prosedur dalam menanggulangi eskalasi pada insiden
		DSS02.02 mencatat, mengklasifikasikan, dan memberikan prioritas pada permintaan dan insiden.	Pembuatan prosedur pemrioritasan *Service Request* berdasarkan dampak terhadap bisnis dan urgensinya
O5	DSS02 Managed Service Requests and Incidents	*DSS02.01 Mendefinisikan skema klasifikasi untuk insiden dan permintaan layanan.*	Pendefinisian *Service Request Models* yang akan digunakan untuk peningkatan efisiensi pelayanan *Service Request*
			Pendefinisian aturan dan prosedur dalam menanggulangi eskalasi pada insiden
		DSS02.02 Rekam, klasifikasikan dan prioritaskan permintaan dan insiden.	Pembuatan pengklasifikasian insiden berdasarkan jenis dan kategori untuk digunakan dalam pembuatan tren
			Pembuatan prosedur pemrioritasan *Service Request* berdasarkan dampak terhadap bisnis dan urgensinya
		DSS02.07 Melacak status dan menghasilkan laporan.	Melakukan analisis dan penetapan tren berdasarkan pola dari isu-isu yang sering muncul.
O6	DSS04	*DSS04.03 Mengembangkan dan melaksanakan respons kelangsungan bisnis.*	Pengadaan pelatihan lanjutan dari hasil uji kontingensi mengenai menghadapi situasi darurat atau bencana.
O9	APO07	APO07.02 Identifikasi personel TI utama.	Pengembangan *succession plan* yang diperuntukkan kepada *Key Risk Personnel*
		APO07.03 Menjaga keterampilan dan kompetensi personil.	Pengadaan sertifikasi demi memastikan kualitas staff manajemen risiko

VI. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian audit kontrol risiko pada unit NITS divisi information technology dan service operation PT Telkom Indonesia Tbk menggunakan framework COBIT 2019 dapat diambil beberapa kesimpulan sebagai berikut:

1. Hasil dari pengujian rancangan kontrol risiko memberikan hasil bahwa kontrol milik risiko O4, O5, O6, O7, O8, O9, dan O10 belum terbukti dapat mengurangi level dari risiko dan belum adanya bukti *Segregation of Duties* sehingga penelitian ini memberikan beberapa rekomendasi terkait kriteria keefektifan rancangan kontrol risiko.
2. Hasil dari analisis data menyatakan bahwa seluruh rancangan dari kontrol risiko sudah dirumuskan secara tertulis dan memadai, kontrol risiko juga sudah dilakukan pengawasan dalam janga waktu per Triwulan atau 3 bulanan, dan sudah diperbarui secara berkala dengan meninjau dari keberhasilan kontrol risiko dalam mengurangi level dari risiko
3. Hasil dari pengujian operasional kontrol risiko menyatakan seluruh aktivitas kontrol risiko sebagai Efektif, dengan alasan bahwa seluruh aktivitas kontrol risiko sudah memiliki bukti aktual dari pelaksanaan aktivitas pengontrolan risiko kepada risiko terkait.
4. Hasil dari pengujian operasional kontrol risiko menggunakan COBIT 2019 menyatakan bahwa terdapat beberapa kesenjangan pada risiko O1 dengan objektif DSS05 Managed Security Services, risiko O2 dengan objektif DSS04 Managed Continuity, risiko O4 dengan objektif DSS02 Managed Service Requests and Incidents, risiko O5 dengan objetif DSS02 Managed Service Requests and Incidents, risiko O6 dengan objektif DSS04 Managed Continuity, dan risiko O9 dengan objektif APO07 Managed Human Resources.

B. Saran

Berdasarkan hasil penelitian audit kontrol risiko pada unit NITS divisi information technology dan service operation PT Telkom Indonesia Tbk menggunakan framework COBIT 2019 menghasilkan saran sebagai berikut:

1. Saran untuk perusahaan, sebaiknya PT Telkom Indonesia dapat mempertimbangkan hasil rekomendasi berdasarkan rancangan, dan COBIT 2019 untuk pengontrolan risiko dengan tujuan membantu meningkatkan efektivitas pengontrolan risiko
2. Saran untuk penelitian selanjutnya, penelitian ini diharapkan dapat menjadi referensi untuk penilaian keefektifan dari kontrol risiko dari sisi rancangan, operasional, serta COBIT 2019

REFERENSI

Sukrisno Agoes. (1996). Auditing (pemeriksaan akuntan) oleh Kantor Akuntan Publik / Sukrisno Agoes. Jakarta: Lembaga Penerbit Fakultas Ekonomi Universitas Indonesia,

MULYADI. (2002). Auditing / Mulyadi. Jakarta: Salemba Empat,

Arens, Alvin A.; Loebbecke, James K., 1936-; Hutauruk, Gunawan. (1990). Auditing: suatu pendekatan terpadu / Alvin A. Arens, James K. Loebbecke; alih bahasa, Gunawan Hutauruk. Jakarta: Erlangga,

Harahap, V., & Novita, N. (2022). Control Self Assessment (CSA) In Improving Company Performance. Jurnal Akuntansi, Keuangan, Dan Manajemen, 3(3), 207–223. https://doi.org/10.35912/jakman.v3i3.731

ISACA. (2018). Governance and Management Objectives. In COBIT® 2019 Framework. https://www.isaca.org/resources/cobit

ISACA. (2018). Introduction and methodology. In Developing Reading and Writing in Second-Language Learners: Lessons from the Report of the National Literacy Panel on Language-Minority Children and Youth: Second Edition. https://doi.org/10.4324/9780203937600

COSO. (2013). Internal Control - Integrated Framework: Guidance on Monitoring Internal Control Systems. Committee of Sponsoring Organizations of the Treadway Commission.

Dittmeier, C., & Casati, P. (2014). Evaluating Internal Control Systems, A Comprehensive Assessment Model (CAM) for Enterprise Risk Management Carolyn Dittmeier, CIA, CRMA Paolo Casati, CIA, CRMA. www.theiia.org/research

ISACA. (2021). COBIT Focus Area: Information & Technology Risk. www.isaca.org

Arthur, J. Keown dkk. (2000). Dasar-Dasar Manajemen Keuangan.Jakarta: Salembe Empat.

Lucas, G.F. (2000). Information Technology for Management. McGraw-Hill

Alter, S. (1992). Information Systems: A Management Perspective. The Benjamin, CummingsPublishing Company, Inc.

William, B.K., Sawyer, S.C. (2003). Using Information Technology, A Practical Introduction to Computers & Communications. McGraw-Hill.

Gondodiyoto, Sanyoto. (2007) “Audit Sistem Informasi Lanjutan “. Mitra Wacana Media, Jakarta.

Gondodiyoto, Sanyoto. (2007) “Audit Sistem Informasi + Pendekatan COBIT”. Mitra Wacana Media, Jakarta.

Fadhilah, R., Santosa, I., Abdurrahman, L., Informasi, P. S., Industri, F. R., Telkom, U., Informasi, P. S., Industri, F. R., Telkom, U., Informasi, P. S., Industri, F. R., & Telkom, U. (2021). Rencana Audit Teknologi Informasi Menggunakan Cobit 2019 Information Technology Audit Plan Using

Cobit 2019 At Telkom. 4(3), 157–163. https://doi.org/10.33387/jiko

Khairuna, D., Wibowo, S., & Gamayanto, I. (2020). Evaluasi Pengelolaan Risiko Teknologi Informasi Menggunakan Framework COBIT 5 Berdasarkan Domain APO12 (Manage Risk) Pada Kantor Pusat BPR Agung Sejahtera. JOINS (Journal of Information System), 5(1), 18–26. https://doi.org/10.33633/joins.v5i1.3088

Firdaus, N. Z., & Suprapto. (2018). Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus: PT. Petrokimia Gresik). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 2(1), 1–10. http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/702

ISACA. (2012). Risk IT Framework. Information Systems Audit and Control Association.

ISO. (2018). ISO 31000:2018 Risk management - Guidelines. International Organization for Standardization.

Kusuma, R. P. (2020). Audit Teknologi Informasi Menggunakan Framework Cobit 5 Pada Domain Dss (Deliver, Service, and Support) (Studi Kasus: Konsultan Manajemen Pusat). Jurnal Digit, 9(1), 97. https://doi.org/10.51920/jd.v9i1.137

Iqbal Agselmora, D., Prasetyo Utomo, A., Stikubank Semarang, U., & Tri Lomba Juang Mugassari, J. (2022). Audit Teknologi Informasi Menggunakan COBIT 5 Domain DSS Pada Universitas Stikubank Semarang. Jurnal Teknik Informatika Dan Sistem Informasi, 9(4). https://doi.org/10.35957/jatisi.v9i4.2612

Ningtyas, K. T., Gumilang, S. F. S., & Hanafi, R. (2023). Perancangan Arsitektur Sistem Pemerintahan Berbasis Elektronik Pada Urusan Sosial Di Pemerintah Provinsi Jawa Barat Berbasis Konsep Enterprise Architecture Menggunakan Kerangka Kerja Togaf Adm. JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika), 8(2), 355–369. https://doi.org/10.29100/jipi.v8i2.3454

Sugiyono. (2015). Metode Penelitian Pendidikan: Pendekatan Kuantitatif, Kualitatif, Dan R&D.

Satori, D. (2013). Metode penelitian kualitatif / Djam'an Satori, Aan Komariah. Bandung: Alfabeta.

Cade, E. (2002). Managing Banking Risk. Cornwall, England. TJ International Ltd.

McNamee, D., Selim, G. M. (1998). Risk management: Changing the Internal Auditor's Paradigm. Institute of Internal Auditors Research Found.

Rejda, G. (2021). Principles of Risk Management and Insurance. In Pearson Education (Vol. 53, Issue 9).

Joint Standards Australia/ Standards New Zealand Committee OB/7. (1933). AS/NZS 4360:1999 Risk Management. In Standards Association of Australia (Vol. 4, Issue 7). Standards Association of Australia, PO Box 1055, Strathfield NSW 2135. https://doi.org/10.1080/00050326.1933.10436323

Suseno, P. (2014). Konsep Dasar Manajemen Risiko. Modul, 1–50.\

Tampubolon, C. J., Abdurrahman, L., & Mulyana, R. (2023). Control Self-Assessment (CSA) Pada Unit Riset dan Layanan TI Direktorat Pusat Teknologi Informasi Universitas Telkom. E-Proceeding of Engineering, 10(2), 1483–1488.