Analisis Proses Manajemen Risiko Ti Menggunakan Kerangka Kerja *Cobit Focus Area Information And Technology Risk* Di Yayasan Pendidikan Telkom

1st Syahren Adil Hakim
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
syahrenadilhakim@student.telkomuniversity.ac.id

2nd Falahah
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
falahah@telkomuniversity.ac.id

3rd Ari Fajar Santoso
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
arifajar@telkomuniversity.ac.id

***Abstrak*— Yayasan Pendidikan Telkom adalah sebuah yayasan dengan mengusung konsep One Pipe Education System (OPES) dan tersebar diseluruh wilayah indonesia, hal ini terselenggara atas bergabungnya dua yayasan dibidang pendidikan yang diprakarsai oleh PT Telkom yaitu Yayasan Sandhykara Telkom dan Yayasan Pendidikan Telkom pada tahun 2015. Sudah banyak perusahaan yang menggunakan teknologi informasi tersebut untuk mengoptimalkan pencapaian tujuan perusahaan. Salah satu aspek yang mempengaruhinya adalah penggunaan teknologi informasi untuk mempertimbangkan aspek risiko yang mungkin menghambat pencapaian sebuah tujuan atau terdapat ancaman terhadap keberlangsungan perusahaan itu sendiri. Untuk melihat sejauh mana pencapaian divisi TI Yayasan Pendidikan Telkom terhadap penanganan risiko atau manajemen risiko, dibutuhkan penilaian ulang atau evaluasi untuk melakukan penilaian ulang tersebut yang diantaranya adalah dengan cara menghitung assesment setiap aktivitas per-domain yang akan menghasilkan Capability Level dari proses manajemen risiko Yayasan Pendidikan Telkom, kemudian akan dilakukan pemberian rekomendasi yang nantinya akan digunakan untuk mencapai Capability Level yang sudah ditargetkan. Hasil assesment yang telah dilakukan dengan COBIT Focus Area Information & Technology Risk menunjukan penilaian Capability Level dari Yayasan Pendidikan Telkom dalam melakukan penanganan risiko pada domain DSS01 menunjukan level 2 dan 3. Analisis hasil assesment yang dilakukan beradasarkan setiap aktivitas perdomain menghasilkan total 41 rekomendasi**

***Kata kunci*— Manejemen Risiko, COBIT Focus Area Information and Technology Risk, 7 COBIT Implementaion Road Map, Capability Risk Assesment.**

I. PENDAHULUAN

Customer Semakin berkembangnya Teknologi Informasi pada zaman ini sangat penting perannya dalam berbagai aspek kehidupan. Sudah banyak perusahaan yang menggunakan teknologi informasi tersebut untuk mengoptimalkan pencapaian tujuan perusahaan. Salah satu aspek yang mempengaruhinya adalah penggunaan teknologi informasi untuk mempertimbangkan aspek risiko yang mungkin menghambat pencapaian sebuah tujuan atau terdapat ancaman terhadap keberlangsungan perusahaan itu sendiri.

Inovasi digital telah mengubah berbagai aspek kehidupan masyarakat dalam berbagai sektor. Kemajuan Teknologi Informasi (TI) yang telah mengubah cara proses kerja menjadi lebih cepat serta efisien. Menurut (Hilda, E) prioritas dari perusahaan industri yang perlu dipertimbangkan adalah memperkuat aspek manajemen risiko sistem informasi dan infrastruktur teknologi yang dapat mengelola manajemen risiko yang kuat untuk mengurangi hal-hal tidak diinginkan yang menganggu bisnis sebuah perusahaan. Manajemen risiko menjadi sebuah aspek kritis dalam dunia bisnis dan organisasi modern. Perubahan lingkungan eksternal yang cepat dan kompleks, seperti fluktuasi pasar keuangan, perubahan regulasi, dan dinamika global, menunjukkan perlunya pendekatan yang terstruktur dan efektif dalam mengelola risiko. Salah satu disiplin ilmu yang merangkum pengelolaan risiko ini adalah analisis manajemen risiko.

Untuk melihat sejauh mana pencapaian divisi TI Yayasan Pendidikan Telkom terhadap penanganan risiko atau manajemen risiko, dibutuhkan penilaian ulang atau evaluasi untuk melakukan penilaian ulang tersebut yang diantaranya adalah risk capability assesment, gap analysis dan priorities improvement. Dari hasil tahapan tersebut akan menghasilkan sebuah rekomendasi manajemen risiko yang sekiranya dapat dijadikan acuan atau masukan terkait implementasi oleh Yayasan Pendidikan Telkom. Penelitian ini akan membahas analisis manajemen risiko khususnya pengelolaan risiko TI pada menggunakan kerangka kerja *COBIT Focus Area Information and Technology Risk* yang sebelumnya data Risk Registernya diperoleh dari pemetaan dengan COBIT 2019

II. KAJIAN TEORI

A. *COBIT Focus Area Information and Technology Risk*

COBIT 2019 *Focus Area Information and Technology Risk* adalah salah satu area fokus kerja dari COBIT 2019 yang membahasa tentang pengelolaan risiko TI. Area ini dirancang untuk membantu organisasi dalam melakukan identifikasi, menilai, mengurangi, dan memantau risiko TI yang dapat mempengaruhi pencapaian dari tujuan bisnis dan operasional (ISACA, 2021). Perbedaan COBIT 2019 biasa dengan COBIT *Focus Area Information and Technology Risk* ialah COBIT 2019 *Focus Area Information and Technology Risk* lebih mengarah kedalam pengelolaan risiko TI secara efektif dan juga lebih mendetail terkait pengintergrasian pengelolaan risiko TI dengan tata kelola dan manajemen TI secara keseluruhan, penerapan pendekatan berbasis risiko, dan pemantauan kinerja kontrol dan kebijakan (ISACA, 2021).

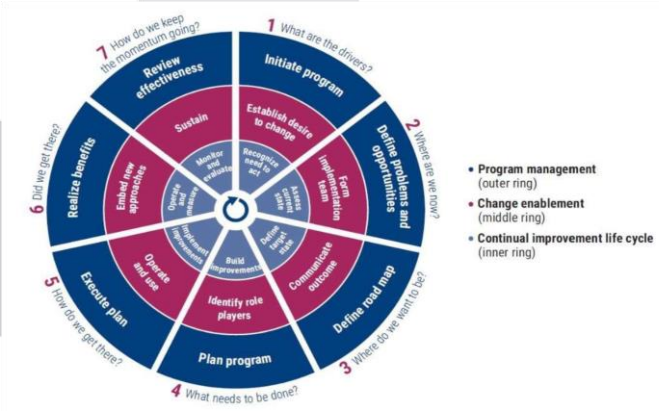
B. Metode Manajemen Risiko

Pada kajian pustaka ini akan menjelaskan terkait metode - metode apa saja yang biasanya digunakan dalam Manajemen Risiko TI.

1. Identifikasi Risiko (*Risk Identification*) : Langkah pertama yang perlu diketahui sebelum melakukan analisis manajemen risiko adalah melakukan observasi risiko yang kemungkinana akan terjadi. Ada beberapa cara yang dapat dilakukan saat identifikasi risiko yaitu salah satunya melakukan brainstroming yang lebih terstruktur untuk melihat suatu masalah. Kemudian akan dituangkan kedalam dokumen atau laporan risiko risiko yang telah diidentifikasi sebelumnya yang nanti akan dianalisa.
2. Analisa Risiko (*Risk Analyze*) : Ketika risiko telah diidentifikasi selanjutnya adalah menentukan seberapa besar kemungkinan setiap risiko yang akan terjadi dengan cara melakukan analisis risiko kualitatif dan kuantitatif. Ada beberapa tingkatan terkait risiko risiko yang telah dilakukan analisis, seperti rendah, sedang dan tingginya risiko tersebut. Adapun juga beberapa kriteria dampak dari risiko tersebut yang nanti akan dilakukan penanganan dari analisis risiko tersebut.
3. Prioritas Risiko (*Risk prioritaze*) : Setelah melakukan analisis risiko, hal yang perlu dilakukan adalah melakukan evaluasi terhadap risiko tersebut untuk mengetahui apa yang harus dilakukan ketika risiko tersebut terjadi dan bagaimana cara mengatasinya. Ada beberapa risiko yang berdampak sedikit atau tidak sama sekali sehingga masih bisa diterima. Namun, ada pula risiko yang membutuhkan penanganan segera agar tidak menganggu jalannya operasional dari suatu organisasi atau perusahaan.
4. Merespond Risiko (*Risk Response*) : Ketika sudah melakukan prioritas risiko, selanjutnya mengetahui apakah risiko ini bersifat positif ataupun negatif untuk kemajuan organisasi atau perusahaan. Yang harus dilakukan adalah menentukan respon dari risiko untuk membuat perencanaan mitigasi, menerima, menghindari, atau mengirimkan dari risiko yang terjadi. Bagaimanapun cara merespond risiko tiap perusahaan atau organisasi berbeda beda sesuai dengan visi dan misi perusahaan.
5. Memantau Risiko (*Risk Monitoring*) : Setelah melakukan respon, risiko harus tetap di pantau dengan cara komunikasi dan transaparasi. Sehingga orang dalam organisasi ataupun perusahaan mengetahui hal yang sedang terjadi dan membantu dalam mengelolanya. Memantau risiko juga berguna dalam membantu menilai risiko risiko yang telah direspond sebelumnya untuk melihat perkembangan dari risiko tersebut.

C. *COBIT 2019 Implementation Guide*

COBIT 2019 Implementation Guide adalah referensi yang berguna untuk memberikan panduan bagaimana cara menyediakan pendekatan praktik implementasi Enterprise Goverment Information Technology (EGIT). Kerangka kerja, praktik yang baik, dan standar yang bermanfaat jika diadopsi dan di adaptasi secara efektif. Ada beberapa tantangan yang harus diatasi dalam agar EGIT sukses. Manajer tinggi perusahaan perlu menerima lebih banyak akuntabilitas untuk bidang TI, memberikan prinsip panduan dan kerangka kerja, dan menanamkan pola pikir dan budaya yang selaras dengan visi misi perusahaan untuk memberikan nilai baik dari bidang TI tersebut. Dalam melakukan implementasi COBIT 2019 ada beberapa penekanan yang berguna yaitu pada sudut pandang seluruh perusahaan tentang tata kelola TI. COBIT 2019 ini merupakan tata kelola dan manajemen TI yang perlu diimplementasikan sebagai bagian intergral dari perusaahan tersebut.



GAMBAR 1 7
Phase COBIT Implementation Road Map

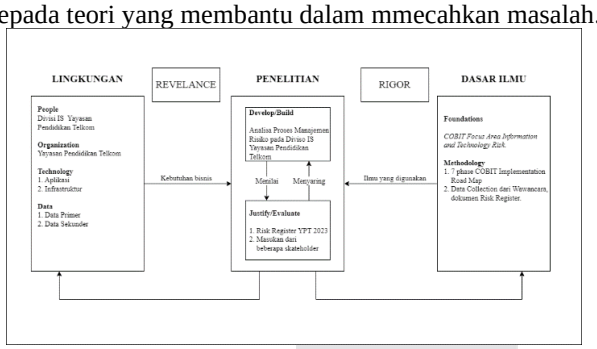
1. What are the driver : Menentukan apa pemicu yang akan dilakukan implementasi pada *COBIT Focus Area Information and Technology Risk*
2. Where are we now : Menentukan kondisi saat ini yang sesuai dengan perusahaan agar bisa melihat batasan kemampuan perusahaan.
3. Where do we want to be : Menentukan target yang sudah ditentukan sebeleumnya sebagai target atau menentukan target baru sebagai acuan kedepannya.

4. What needs to be done : Menentukan apa yang harus diselesaikan terlebih dahulu atau di penuhi agar bisa mencapai target yang sudah ditentukan.
5. How do we get there : Menentukan cara atau metode yang dilakukan agar implementasi COBIT 2019 dapat dilakukan.
6. Did we get there : Memastikan apakah dari implementasi yang sudah dilakukan sudah sesuai atau belum.
7. How do we keep momentum going : Memastikan bahwa impelementasi yang sudah dilakukan dapat dijalankan secara berkelanjutan.

III. METODE PENELITIAN

A. Model Konseptual

(Henver, 2004) menjelaskan bahwa model koseptual adalah model yang mendeskripsikan kedalam bentuk diagram yang menggambarkan hubungan antara konsep yang dimana hubungan tersebut merupakan faktor utama yang mempengaruhi sebuah kondisi penyampaiannya. Koseptual model ini sangat membantu dalam memetakan masalah - masalah relevan dan menghubungkannya kepada teori yang membantu dalam mmecahkan masalah.



GAMBAR 2
Model Konseptual

Model Konseptual penelitian ini diilustrasikan seperti gambar 2, pada penelitian ini akan memfokus pada bagian people, organisasi, dan develop/build. Model konseptual yang dipakai dalam penelitian ini menjadi tiga bagian yaitu lingkungan, penelitian, dan dasar ilmu.

B. Metode Pengumpulan Data

Dalam melakukan analisis manajemen risiko TI berdasarkan *COBIT Focus Area Information and Technology Risk*, dibutuhkan beberapa data yang akan diolah dan nantinya akan dilakukan pencocokan terkait kinerja dan penanganan dari risiko yang ada. Jenis data yang akan digunaka nsendiri dibagi menjadi dua yaitu data primer dan data skunder.

TABLE 1
Metode Pengumpulan Data

Jenis Data	Sumber Data
Data Primer	Laporan Daftar Risiko Yayasan Pendidikan Telkom
	Standar Operasional Yayasan Pendidikan Telkom
Data Sekunder	Profil Yayasan Pendidikan Telkom
	Visi dan Misi Yayasan Pendidan Telkom
	Struktur Organisasi Yayasan Pendidikan Telkom

IV. PENGUMPULAN DATA

A. Phase 1 : Whare are the driver

IT Pain Point adalah poin - poin masalah yang muncul pada proses bisnis khususnya dibidang IT di Yayasan Pendidikan Telkom.

TABLE 2
IT Pain Point

Objective	IT Pain Point
Empowering Layanan TS : Modul Pembayaran PPDB	Ketidakjelasan kebutuhan fungsional maupun nonfungsional aplikasi
	Perubahan kebutuhan aplikasi dari pengguna di luar dari yang disepakati di awal
	Waktu pengembangan mundur dari jadwal yang ditargetkan
Empowering Layanan TC : Mengawal Migrasi Data dan Operasional Igracias TUNC untuk ITTJ	Data tidak termigrasi dengan baik
Empowering Layanan BPK : Dashboard Finance AP	Ketidakjelasan kebutuhan fungsional maupun non fungsional aplikasi
	Perubahan Kebutuhan aplikasi dari pengguna di luar dari yang disepakati di awal
	Waktu pengembangan mundur dari jadwal yang ditargetkan
	Tidak menggunakan teknologi yang sama dalam pengembangan sistem
Empowering Layanan BPK : Pembuatan ISAK 35	Proses integrasi yang gagal

B. Phase 2 : Where are we now

Pada fase dua ini akan melakukan penilaian Capability Risk Management Assesment yang pada IT Pain Point menggunakan kerangka kerja COBIT Focus Area Information and Technology Risk terkait domain DSS (Deliver, Service and Support) untuk melihat sejauh mana tingkatan Capability Level divisi IS Yayasan Pendidikan Telkom.

TABLE 3
Hasil Capability Risk Management Assesment Component : Process

Domain	Hasil Assesment Capability Level
DSS01 Managed Operations	2
DSS04 Managed Continuity	2
DSS06 Managed Business Process Controls	2

TABLE 4
Hasil Capability Risk Management Assesment Component : Organizational Structure

Jabatan	Deskripsi Jabatan
Audit department	bertanggung jawab untuk menyediakan laporan audit internal mengenai risiko yang terkait dengan keberlangsungan perusahaan.

Compliance department	memberikan wawasan terkait risiko risiko perusahaan dan peraturan, tindakan, serta kebijakan dan standar pengelolaan risiko.
I&T risk officers/ managers	Sekelompok jabatan yang mengelola serta bertanggung jawab untuk mengidentifikasi, menilai dan melaporkan risiko yang ada.

TABLE 5
Hasil Capability Risk Management Assesment Component : Information Flow and Items

Management Practice	Dokumen
DSS01.02 Manage outsourced I&T services.	Vendor risk management plan
DSS01.03 Monitor I&T infrastructure.	Risk management monitoring process and procedure (Documment Input)
DSS01.04 Manage the environment.	
DSS01.05 Manage facilities.	
DSS04.02 Maintain business resilience	Risk management plan (Documment Input)
DSS04.04 Exercise, test and review the (BCP) and (DRP).	Newly identified risk in BCP/DRP (Doccument Output)
DSS04.08 Conduct post-resumption review.	Risk management plan (Documment Input)
DSS06.04 Manage errors and exceptions.	Record of risk associated with approved changes
DSS06.06 Secure information assets.	Risk identified from new threats or events

TABLE 6
Hasil Capability Risk Managent Assesment Component : Principles, Policies, and Procedure

Kebijakan
Core IT risk policy
Compliance policy
Ethics policy
Quality management policy
Change management policy
Data privacy policy

TABLE 7
Hasil Capability Risk Management Assesment Component : Services, Infrastructure, and Application

Aplikasi yang ada	Deskripsi
Tools for risk communication/reporting	Alat yang bertujuan untuk mengomunikasikan terkait identifikasi pengelolaan risiko.

TABLE 8
Hasil Capability Risk Management Assesment Component : People, Skills and Competencies

Jabatan yang ada	Deskripsi
Analisis Risiko	Bertujuan untuk analisis ,penilaian, pemantauan risiko.

V. HASIL DAN PEMBAHASAN

A. Phase 3 : Where do we want to be

Setelah melakukan penilaian terhadap sejauh mana kemampuan divisi IT dalam mengelola manajemen risiko yang ada dengan *COBIT Focus Area Information and Technology Risk*. Pada fase 3 ini akan menjelaskan terkait target yang akan dicapai dari divisi TI untuk penilaian DSS01, DSS04 dan DSS06 manajemen risiko, menjelaskan celah antara penilaian domain tersebut dan memberikan perbaikan yang bsia dilakukan untuk menutupi celah tersebut.

TABLE 9
Target Improvement

Management Practice	Target
DSS01 Managed Operations	3
DSS04 Managed Continuity	3
DSS06 Managed Business Process Controls	3

B. Analisis GAP

Analisis GAP adalah proses di COBIT 2019 yang berguna untuk mengetahui kesenjangan antara pencapaian divisi IS saat ini dengan proses target domain yang ditentukan. Tujuan dari analisis gap adalah mencari celah dalam pencapaian divisi IS sehingga bisa menemukan kesenjangan antara pencapaian divisi IS dengan DSS01, DSS04 dan DSS06 di *COBIT Focus Area Information and Technology Risk*. Kesenjangan ini akan digunakan untuk proses selanjutnya dalam menentukan bagian proses mana yang belum terpenuhi sesuai target, menentukan kesenjangan kenapa belum terpenuhi dan menentukan rekomendasi apa yang digunakan untuk menutupi kesenjangan tersebut.

TABLE 10
Analisis GAP

Management Practice	Exsisting	Target
DSS01 Managed Operations	2	3
DSS04 Managed Continuity	2	3
DSS06 Managed Business Process Controls	2	3

C. Target Improvement

Setelah menemukan celah atau GAP antara pencapaian proses divisi IS terkait *domain* DSS01, DSS04, dan DSS06 maka sudah bisa ditentukan bagian mana yang bisa dilakukan perbaikan terkait *domain* tersebut, *potential improvement* adalah proses yang ada di COBIT 2019 untuk menemukan kesenjangan yang dapat dilakukan perbaikan agar pencapaian divisi IS dalam *domain* tersebut dapat sesuai dengan target.

TABLE 11
Target Improvement Component : Process

Management Practice	Rekomendasi
DSS01.02 *Managed outsourced IT services (Capability Level 3)*	Perlu adanya pihak ketiga seperti audit departement atau helpdesk untuk melakukan evaluasi dan penanganan pengendalian risiko
DSS01.03 *Monitor IT Infrastructure (Capability Level 3)*	Membuat pendekatan lebih awal terkait indentifikasi risiko dan melakukan tindakan yang cepat sesuai dengan keputusan atasan.

DSS04.01 *Define the business continuity policy, objectives and scope. (Capability Level 2)*	• Melakukan identifikasi proses bisnis internal dan outsource Membuat dokumentasi terhadap kontrol kebijakan minimum yang disepakati
DSS04.02 *Maintain business resilience. (Capability Level 2)*	• Menentukan siapa yang bertanggung jawab terkait pemeliharan dalam ketahan bisnis Membuat laporan DRP sesuai dengan risiko yang terjadi
DSS04.03 *Develop and implement a business continuity response (Capability Level 2)*	Membuat sesi pelatihan kepada anggota staff yang terlibat terkait BCP dan DRP yang terjadi
DSS04.04 *Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP) (Capability Level 2)*	Membuat laporan dokumentasi terhadap hasil tes terkait BCP dan DRP.
DSS04.06 *Conduct continuity plan training (Capability Level 2)*	Membuat latihan dan tes cara menangani RDP.
DSS06.02 *Control the processing of information. (Capability Level 2)*	Membuat issue log terkait transaksi dan verifikasi individu yang memiliki kewenangan.

TABLE 12
Target Improvement Component : Organization Structures

Rekomendasi Jabatan	Deskripsi Jabatan
Enterprise risk management (ERM) committee	Kelompok eksekutif perusahaan yang bertanggung jawab atas kolaborasi dan konsensus tingkat perusahaan yang diperlukan untuk mendukung aktivitas dan keputusan ERM. Dewan risiko TI dapat dibentuk untuk mempertimbangkan risiko TI secara lebih rinci dan memberikan nasihat kepada komite ERM.

TABLE 13
Target Improvement Component : Information Flow and Items

Management Practice	Dokumen Rekomendasi
DSS04.05 Review, maintain and improve the continuity plans	*Newly identified risk in BCP/DRP*
DSS06.02 Control the processing of information	*Risk data quality management policy*
DSS06.05 Ensure traceability and accountability for information events	*System generated audit log*

TABLE 14
Target Improvement Component : Principles, Policies, and Procedure

Rekomendasi Kebijakan
Information security policy
Crisis management policy
Third-party IT service delivery management polic
Fraud risk policy
Change management policy

TABLE 15
Target Improvement Component : Services, Infrastructure and Application

Rekomendasi Aplikasi	Deskripsi Aplikasi
Governance, risk and compliance (GRC) tools .	GRC Tools adalah aplikasi yang berguna untuk menampilkan dashboard potensial atau kartu skor yang ditentukan oleh perusaahan untuk mengumpulkan, menganalisis, mengelola, dan melaporkan risiko yang terjadi. Salah satu tujuan aplikasi ini juga berguna untuk mengomunikasikan risiko dalam urutan prioritas sehingga informasi inti dapat diambil langkah tepat.
Knowledge repositories	Knowledge repositories adalah aplikasi yang berguna untuk mengelola informasi yang digunakan untuk memfasilitasi analisis manajemen risiko dan proses keseluruhannya.

TABLE 16
Target Improvement Component : People, Skills and Competencies

Rekomendasi Jabatan	Deskripsi Jabatan
Kepala Jabatan Risiko	Kepala Jabatan Risiko bertanggung jawab untuk memperjuangkan insiatif untuk memitigasi risiko bisnis yang dapat merugikan profitabilitas dan produktivitas perusahaan. Peran tersebut juga mengawasi program manajemen risiko perusahaan dan menerapkan kebijakan dan prosedur untuk meminimalkan atau mengelola risiko operasional.
Manajer Risiko	Manajer Risiko bertanggung jawab atas keberhasilan penerapan, strategi, dan kerangka risiko. Manajer risiko juga terlibat dengan pemangku kepentingan untuk memastikan proses manajemen risiko dipahami, diberi sumber daya dan diterapkan untuk mendukung tujuan bisnis. Kemudian hasil risiko dilaporkan kepada Kepala Jabatan Risiko dan akan dimasukan kedalam profil risiko.

D. Phase 4 : How do we get there

Fase empat ini akan menentukan perancangaan proses implementasi dari rekomendasi yang sudah ada, namun pada penelitian ini hanya membahas sampai pada titik perencangan untuk implementasi dan akan dijabarkan dengan metode roadmap.

E. Rollout Solution

Roll Out Solution adalah fase untuk menentukan roadmap yang sebelumnya direkomendasikan dan sudah bisa disosialisasikan dan digunakan oleh Yayasan Pendidikan Telkom. Roadmap ini diharapkan bisa menjadi panduan bagi

perusahaan terkait jadwal prioritas rekomendasi yang sudah dibuat

TABLE 17
Roadmap Rollout Solution

No	Aktivitas	Kategori	Tahun	Quarter
1.	Memastikan pihak ketiga (jika ada) untuk melakukan pemeliharaan, menjaga, dan mengevaluasi secara berkala tingkat risiko IT perusahaan. *(DSS01.02 Managed outsourced IT services)*	Process, Policy, Procedure	2024	Q3
2.	Mengecek ancaman IT yang dirasa berdampak signifikan. (*DSS01.03 Monitor IT Infrastructure*)	Process	2024	Q3
3.	Membuat SOP pertahanan pada managemen fasilitas perusahaan. (*DSS01.05 Managed facillities)*	Procedure	2024	Q3
4.	Mementingkan proses bisnis internal untuk aktivitas layanan operasional perusahaan. *(DSS04.01 Define the business continuity policy, objectives and scope)*	Process	2024	Q3
5.	Membuat syarat minumum untuk mempertahankan proses bisnis ketika terjadinya risiko. *(DSS04.01 Define the business continuity policy, objectives and scope)*	Process, Procedure	2024	Q3
6.	Menentukan siapa yang bertanggung jawab untuk memelihara dan meninjau proses mitigasi risiko. *(DSS04.02 Maintain business resilience)*	Process, Procedure	2024	Q3
7.	Membuat prosedur peruhahan BCP dan DRP untuk meminimalisir kerugian. *(DSS04.02 Maintain business resilience)*	Process, Procedure	2024	Q4
8.	Membuat pelatihan reguler kepada pihak yang menangani BCP dan DRP. *(DSS04.03 Develop and implement a business continuity response, DSS04.06 Conduct continuity plan training)*	Process, Procedure, Recruitment	2025	Q1
9.	Memvertifikasi tingkat pelatihan sesuai dengan hasil tes yang telah dilakukan. *(DSS04.03 Develop and implement a business continuity response)*	Process, Recruitment	2025	Q2
10.	Membuat laporan hasil tes ketika melakukan pelatihan BCP dan DRP. *(DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP))*	Process, Procedure, Recruitment	2025	Q2
11.	Memastikan pelatihan BCP dan DRP sampai pada proses akhir. *(DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP))*	Process, Policy, Procedure, Recruitment	2025	Q2
12.	Membuat rencana tindakan yang akan diambil pada periode tertentu pada saat proses pemulihan dari risiko yang terjadi. *(DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP))*	Process, Procedure	2024	Q3
13.	Mempertimbangkan apakah proses bisnis perlu direvisi jika terdampak pada risiko. *(DSS04.05 Review, maintain and improve the continuity plans)*	Process	2024	Q3
14.	Memastikan bahwa sistem, aplikasi, data dan dokumentasi sudah dilakukan backup. *(DSS04.07 Manage backup arrangements)*	Process, Procedure	2024	Q3
15.	Meninjau dan mendokumentasikan pemeliharaan risiko sesuai dengan prosedur BCP dan DRP. *(DSS04.08 Conduct post-resumption review)*	Process, Procedure	2024	Q3
16.	Melakukan identifikasi dan dokumentasikan pada saat pengandalian risiko proses bisnis utama. *(DSS06.01 Align control activities embedded in business processes with enterprise objectives)*	Procecss, Procedure	2024	Q3
17.	Membuat kontrol system otomatis pada proses bisnis yang terkena dampak	Process, Application	2025	Q3

	risiko. *(DSS06.01 Align control activities embedded in business processes with enterprise objectives)*			
18.	Memantau terus aktivitas pengendalian risiko. *(DSS06.01 Align control activities embedded in business processes with enterprise objectives)*	Process, Procedure	2024	Q4
19.	Merubah atau meningkatkan desain pengendalian risiko pada proses bisnis jika diperlukan. *(DSS06.02 Control the processing of information)*	Process	2025	Q3
20.	Membuat kebijakan vertifikasi yang berguna untuk transaksi. *(DSS06.02 Control the processing of information)*	Policy	2025	Q1
21.	Menentukan siapa yang bergantung jawab terkait persetujuan transaksi. *(DSS06.02 Control the processing of information)*	Process	2025	Q1
22.	Memvertifikasi bahwa transaksi akurat, lengkap dan valid. *(DSS06.02 Control the processing of information)*	Process, Procedure	2025	Q2
23.	Melakukan backup data secara berulang terkait transaksi asli. *(DSS06.02 Control the processing of information)*	Process, Procedure	2025	Q2
24.	Memastikan bahwa prosedur sesuai dalam melakukan identifikasi dalam menyelesaikan risiko dalam proses bisnis otomatis. *(DSS06.04 Manage errors and exceptions)*	Process, Procedure	2025	Q3
25.	Bekerja sama dengan divisi bisnis untuk identifikasi proses bisnis tertentu dalam memantau proses bisnis otomatis. *(DSS06.05 Ensure traceability and accountability for information events)*	Process, Procedure	2025	Q3
26.	Memastikan bahwa dokumentasi dan pemetaan proses bisnis manual sudah sesuai untuk proses bisnis otoamtis. *(DSS06.05 Ensure traceability and accountability for information events)*	Process	2025	Q3
27.	Membentuk divisi Enterprise Risk Management Committe yang berguna untuk bergantung jawab dalam penangana risiko TI secara lebih rinci	Organize	2024	Q3
28.	Membuat dokumen risiko yang telah diidentifikasi oleh BCP dan DRP.	Process, Procedure, Document	2024	Q4
29.	Membuat dokumen log audit yang sudah terintergrasi oleh sistem.	Process, Document	2025	Q4
30.	Memiliki kebijakan dokumentasi terkait pengelolaan risiko berbasis kualitas data.	Policy	2024	Q4
	Membuat kebijakan pedoman untuk melindungi informasi perusahaan, sistem dan infrastruktur terkait persyaratan bisnis.	Policy, Procedure, People	2024	Q1
32.	Membuat kebijakan terkait manajemen jaringan dan keamanan data untuk keperluan operasional.	Policy	2025	Q2
33.	Membuat kebijakan terkait layanan pihak ketiga yang digunakan.	Policy	2025	Q2
34.	Membuat pedoman untuk perlindungan merek, reputasi dan aset perusaahan.	Policy	2024	Q1
35.	Membuat pedoman kebijakan terkait perubahan pada bagian IT perusahaan.	Policy, Procedure	2025	Q1
36.	Membuat GRC (Governance, risk and compliance) tools yang berguna untuk menampilkan dashboard potensial atau kartu skor yang ditentukan oleh perusaha untuk mengumpulkan, menganalisis, mengelola dan melaporkan risiko yang terjadi.	Procecss, Application	2025	Q4
37.	Membuat Knowledge repositories yang berguna untuk mengelola berbagai informasi yang bertujuan untuk memfasilitasi manajemen risiko dan seluruh prosesnya.	Feature	2025	Q4
38.	Melakukan recruitment Kepala Jabatan Risiko yang	Recruitment	2026	Q1

	bertangung jawab untuk memitigasi risiko bisnis agar tidak merugikan profitabilitas dan produktifitas perusahaan.			
39.	Melakukan requirment Manajer Risiko yang bertanggung jawab atas penerapan dan strategi dalam mengelola kerangka risiko.	Recruitment	2026	Q1

VI. KESIMPULAN

Berdasarkan hasil dari penelitian yang sudah dilakukan mengenai Analisis Proses Manajemen Risiko TI Menggunakan Kerangka Kerja COBIT *Focus Area Information and Technology Risk* di Yayasan Pendidikan Telkom diperoleh kesimpulan berikut :

1. Beberapa risiko terjadi dan sudah disimpulkan kedalam Risk Register dari Yayasan Pendidikan Telkom pada tahun 2023, beberapanya diambil dan dimasukan kedalam IT Pain Point untuk dilakukan assesment dan diberikan rekomendasi, berikut resiko eksisting yang relavan dengan penelitian ini:

i) Metode yang digunakan dengan lembaga-lembaga di bawah naungan YPT tidak selaras (*Bussines Impact Analysist*)

ii) Data tidak termigrasi dengan baik (*Empowering* Layanan TC: Mengawal Migrasi Data dan Operasional Igracias TUNC untuk ITTJ)

iii) Integrasi dengan sistem eksisting (*Empowering Layanan* BPK: Pembuatan ISAK 35)

iv) Teknologi yang dipilih kurang tepat (Kajian BCP dan DRP)

v) Peserta yang ikut tidak tepat sasaran (*Information Security Awareness & Training*)

2. Hasil assesment yang telah dilakukan dengan COBIT Focus Area Information & Technology Risk menunjukan penilaian capability level dari Yayasan Pendidikan Telkom dalam melakukan penanganan risiko pada domain DSS01 menunjukan level 2 yaitu bernilai 33% (*Partially*), DSS04 menunjukan capability level 2 yaitu bernilai 46%, (*Partially*) DSS06 menunjukan capability level 2 yang bernilai 70% (*Large*)
3. Analisis hasil assesment yang dilakukan beradasarkan setiap aktivitas perdomain menggunakan COBIT *Focus Area Information and Technology Risk* menghasilkan 41 rekomendasi yang perlu ditingkatkan untuk mencapai Capability Level 3 yang telah di kelompokan menjadi 3, yaitu aspek *process*, *people*, dan *technology*. Ada 31 rekomendasi pada aspek *process*, 5 rekomendasi aspek *people*, dan 5 rekomendasi aspek *technology*.

REFERENSI :

Al-Hakim, N. (2020). *Analisis dan Perancangan Proses Manajemen Risiko TI Menggunakan Kerangka Kerja COBIT 2019 di PT INTI (Persero)*.

Amelia, N. (2020). *Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 dan ISO 31000:2018 pada PT. SOLUSI INTEGRASI TEKNOLOGI.*

De Haes, S. &. (2004). *IT Governance and Its Mechanicsm.* www.isaca.org.

Henver, A. R. (2004). *DESIGN SCIENCE IN INFORMATION SYSTEM RESEARCH.* MIS: Quarterly.

Hilda, E. (n.d.). *Global Risk Management Survey.* Deloitte: 10th edition.

Husein, G. M. (2015). Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika(Jatel). In *Jurnal Teknik Informatika dan Sistem Informasi* (pp. 75-87).

ISACA. (2018). *COBIT 2019 Framework Governance and Management Objectives.*

ISACA. (2019). *COBIT 2019 Implementation Guide - Implementing and Optimizing an Information and Technology Governance Solution.* ISACA.

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

Kozina, M. (2021). *IT Risk Management in the enterprise using COBIT 5*.

Mutiah, N. (2019). Penilitian Tata Kelola Teknologi Informasi Universitas Tanjungpura Menggunakan COBIT 5 Domain Align, Plan, and Organise (APO).

Paterson, R. (2004). Crafting Information Technology Governance. In R. Paterson. EDPACS.

Pratama, I. P. (2020). Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018.

Suhendi. (2020). Risk Assesment, Risk Management, and Cominication at Drug Industries PT. Kimia Farma (Persero) Tbk. Plant Bandung.

Surendro, K. (2009). *Pengembangan Rencana Induk Sistem.* Bandung: Penerbit Informatika.

Tampang, B. L. (2012). Peran Teknologi Informasi Dalam Pengembangan Vokasi Pendidikan Tinggi. 419.

Telkom, Y. P. (2021). *Yayasan Pendidikan Telkom About Us.* Bandung: ypt.co.id.

Thenu, P. P. (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 (Studi Kasus : PT Global Infotech).

Wardiana, W. (2002). *Perkembangan Teknologi Informasi di Indonesia.*

Yahyah, Z. F. (2023). Mendayagunakan COBIT 2019 IT Risk Management Focus Area Dalam Pengelolaan Risiko Transformasi Digital REINSURCO.