Audit Keamanan Sistem Informasi Euclid Menggunakan *Framework* Cobit 5 pada PT. XYZ

Nur Arifin[1], Eki Saputra[2], Tengku Khairil Ahsyar[3], Fitriani Muttakin[4]
[1,2,3,4] Fakultas Sains dan Teknologi, Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia
Email: 1175014838@students.uin-suska.ac.id[1], eki.saputra@uin-suska.ac.id[2], tengkukhairil@uin-suska.ac.id[3], fitrianimuttakin@uin-suska.ac.id[4]

Abstract – PT. XYZ is a private company engaged in the planting and processing of oil palm fruit. Currently PT. XYZ has implemented a technology called the EuClid system which functions to assist the data collection process and reports for each staff. However, in its implementation, there are still several problems, such as missing submission reports, providers who often experience network interruptions, and data hacking or leaks that have occurred. For this reason, it is necessary to carry out a security audit of EuClids information system at PT. XYZ in order to measure, guarantee, and find the root of the problem also makes recommendations on the information system used. This study uses the COBIT 5 Framework with the DSS05 (Manage Security Service) domain to measure the EuClid Information System Capability Level. The results of achieving the value of each level in the DSS05 domain process are level 1 (performed process) of 62.5%, level 2 (Manage Process) of 65.36%, level 3 (Established Process) of 63.02%, level 4 (Predictable Process) is 62.6%, and level 5 (Optimizing Process) is 59.63%. Achievement at each level is in the range of 50% - 85%, so that the ranking in the ISO/IEC 15501-2-2003 standard is Largely Achieved. Of the average achievements, no one has crossed the gap value of 85.01%. This means that the existing information security service process has not been fully reached at level 1, so that the target level is currently still at level 1.

Keywords: *audit; capability level; COBIT 5; DSS05; information system*

Intisari – PT. XYZ ialah perusahaan swasta bergerak di bidang penanaman juga pengolahan buah kelapa sawit. Saat ini PT. XYZ telah menerapkan teknologi bernama sistem EuClid yang berfungsi untuk membantu proses pendataan dan laporan bagi setiap staff. Dalam penerapannya, masih terdapat permasalahan, yaitu adanya laporan pengajuan yang hilang, provider yang sering mengalami gangguan jaringan, dan pernah mengalami peretasan atau kebocoran data. Untuk itu diperlukan melakukan audit keamanan sistem informasi Euclid di PT. XYZ untuk mengukur, menjamin, dan menemukan akar permasalahan juga membuat rekomendasi kepada sistem informasi yang dipakai. Penelitian ini menggunakan *Framework* COBIT 5 dengan *domain* DSS05 (*Manage Security Service*) untuk mengukur tingkat *Capability Level* Sistem Informasi EuClid. Hasil pencapaian nilai dari setiap level pada proses domain DSS05 yaitu level 1 (*performed process*) sebesar 62,5%, level 2 (*Manage Process*) adalah 65,36%, level 3 (*Established Process*) sebesar 63,02%, level 4 (*Predictable Process*) adalah 62,6%, dan level 5 (*Optimizing Process*) adalah 59,63%. Pencapaian pada setiap level berada pada rentang 50% - 85%, sehingga peringkat dalam standar ISO/IEC 15501-2-2003 berada pada *Largely Achieved* (Sebagian besar terpenuhi). Dari rata-rata pencapaian tersebut tidak ada yang melewati batas dari nilai gap sebesar 85,01%. Hal ini menunjukkan proses layanan keamanan informasi yang ada belum sepenuhnya tercapai pada level 1, sehingga target levelnya saat ini masih pada level 1.

Kata Kunci: audit, capability level, COBIT 5, DSS05, sistem informasi

I. PENDAHULUAN

Semakin hari semakin tinggi ketergantungan manusia terhadap Sistem Informasi. Saat ini informasi merupakan kebutuhan dasar manusia, dimulai dari yang sederhana sampai dengan yang sifatnya rumit [1]. Untuk menggapai tujuan bisnis, perusahaan perlu menerapkan Tata Kelola TI yang baik juga benar. Perusahaan haruslah menjaga keamanan sistem informasi yang dimilikinya [2]. Keamanan Sistem Informasi ialah masalah utama baik buat perusahaan, organisasi, juga pemerintah. Permasalahan tersebut bisa terjadi karena belum adanya audit keamanan sistem informasi terhadap tingkat kematangan suatu sistem, kurangnya pendokumentasian laporan, dan belum adanya pedoman SOP terkait kebijakan keamanan Sistem Informasi. Maka dari itu, diperlukan audit keamanan sistem informasi agar mengetahui tingkat kematangan sistem informasi dalam menjamin berjalannya proses bisnis dan memberi peningkatan keamanan sistem informasi yang sudah ada [3].

PT. XYZ ialah perusahaan swasta bergerak di bidang penanaman juga pengolahan buah kelapa sawit yang telah memiliki gudang persediaan pupuknya sendiri. Dalam menjalankan proses bisnisnya, PT. XYZ memiliki layanan teknologi informasi yang digunakan oleh karyawan yang bernama EuClid. Sistem Informasi EuClid merupakan aplikasi yang dikembangkan oleh perusahaan WIDYATECH *Company*. Pada sistem informasi EuClid terdapat beberapa fitur atau modul yang disediakan, diantaranya HRIS (*Human Resource Information System*) untuk pengelolaan informasi sumber daya manusia perusahaan, administrasi kepegawaian, pengembangan personalia, akuntansi keuangan, sistem akuntasi, sistem keuangan, sistem logistik, manajemen bahan, pengadaan dan penjualan.

PT. XYZ menggunakan Sistem informasi EuClid dalam hal administrasi hingga *payslip*. Sistem informasi ini berfungsi sebagai pendataan, laporan bagi setiap staff atau karyawan baik di kantor pusat maupun cabang. Sistem ini dipilih dikarenakan PT. XYZ memiliki beberapa kantor perwakilan dibeberapa daerah, dan kantor unit diperkebunan, sehingga dibutuhkannya sistem informasi yang efesien, *up to date*, dan terintegrasi, agar *stake holder* sampai *staff* yang berjumlah hampir 150 orang dapat diwadahi dengan satu sistem informasi. Berdasarkan hasil wawancara, terdapat beberapa permasalahan dalam penerapan sistem EuClid tersebut, diantaranya beberapa laporan pengajuan yang hilang pada system sementara pengajuan tersebut belum disetujui ataupun dilihat oleh pimpinan, hal ini menjadi masalah karena laporan pengajuan ada yang bersifat penting. Permasalahan selanjutnya yaitu jaringan, sulitnya mengakses sistem informasi ketika server mengalami gangguan, ataupun ketika provider mengalami gangguan, akibatnya menghambat proses administrasi dan pelaporan. Sistem informasi yang digunakan juga pernah mengalami peretasan dan kebocoran data. Permasalahan tersebut dapat menghambat kinerja staff yang melakukan input data, staff yang melalukan laporan pengajuan dan staff keuangan yang akan melakukan remunisasi, dan keamanan dari data yang ada pada perusahaan. Untuk itu penting melakukan audit sistem informasi Euclid di PT. XYZ guna mengukur, menjamin, menemukan akar permasalahan juga membuat rekomendasi kepada sistem informasi yang dipakai di pelayanan proses bisnis perusahaan.

COBIT ialah rangkaian dari dokumentasi *best practice,* jika didalam manajemen IT memiliki tujuan yakni memberi bantuan terhadap pengguna, auditor serta manjemen dalam menjembatani kesenjangan diatara masalah dengan IT, persyaratan manajemen dan resiko bisnis. Standar komprehensif yang memberi bantuan untuk perusahaan dalam meraih tujuannya serta menciptakan nilai dengan menggunakan pengelolaan dan manajememen teknologi informasi yang efektif ialah COBIT 5. Penelitian ini menggunakan *Framework* COBIT 5 sebab COBIT 5 menggabungkan pemikiran terbaru di teknik tata kelola perusahaan juga manajemen, menyediakan model, alat analisis, praktik, serta prinsip yang dapat diterima secara global untuk memberi bentuan supaya nikai system informasi dan tingkat kepercayaan meningkat [4].

Penelitian tata kelola TI menggunakan COBIT 5 pernah dilaksanakan oleh [5] yang membahas mengenai implementasi kerangka kerja COBIT 5 yang menyarankan beberapa langkah yang dapat dilakukan guna membuat kinerja meningkat dan mengajukan saran untuk membuat pengelolaan rencana kedepannya. Akan tetapi penelitian ini terbatas, hanya mencakup domain EDM4 dari area tata kelola (Governance).

Selanjutnya penelitian yang dilakukan oleh [6] mengenai penggunaan framework COBIT 5 untuk menilai, mengukur, dan mengendalikan kinerja Sistem Informasi Akademik (SIA) dengan menggunakan domain Plan and Organise (PO). Berdasarkan penelitian tersebut dinyatakan bahwa "tingkat kematangan (maturity level) yang ada pada setiap proses TI yang terdapat dalam domain Plan and Organise (PO) rata-rata pada level 2,446 dan masih berada pada level 2 (repeatable but intuitive)".

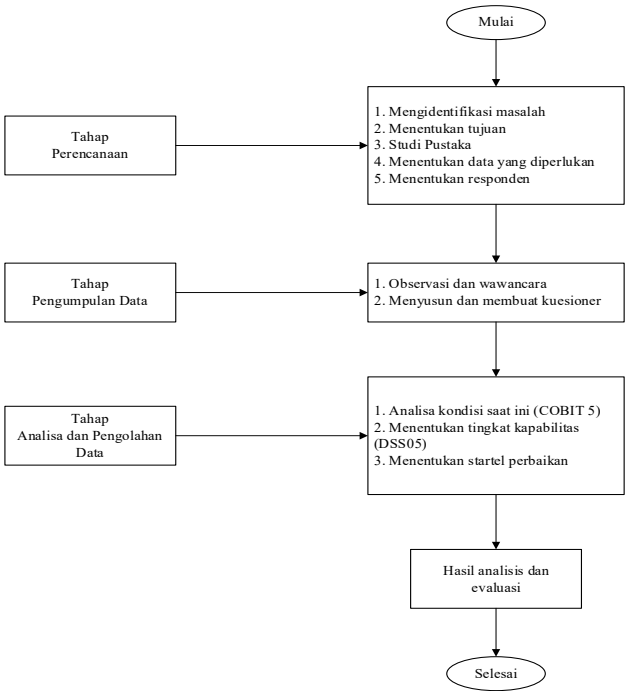
Penelitian lain dilakukan oleh [7] mengenai audit kemanan tata kelola teknologi informasi menggunakan framework COBIT 5 pada Universitas X. Penelitian ini memakai domain DSS03 dan MEA01 yang menghasilkan domain DSS03 dengan rata-rata berada pada 2.6 (Manage process) dan Domain MEA01 rata-rata berada pada 2.8 (Manage process). Selanjutnya penelitian yang dilakukan oleh [8] menggunakan framework COBIT 5 pada Disduk Capil Kota Tangerang dengan domain EDM (Evaluate, Direct, and Monitor). Penelitian ini menyatakan bahwa "pengoptimalan Tata Kelola TI yang berjalan (EDM01) saat ini berada pada level 3 (manage process) dengan status Largely Achieved sebesar 65%, proses pengoptimalan pelayanan manajerial EDM02 berada pada level 4 (Predictable Process) dengan status pencapaian largely achieved sebesar 65%, Proses pengelolaan resiko (EDM03) saat ini berada di level 3 (established process) dengan status pencapaian largely achieved sebesar 65 %. Proses optimalisasi sumber daya (EDM04) saat ini berada pada level 3 (established process) dengan pencapaian partially achieved sebesar 45 %. Untuk Proses optimalisasi kinerja (EDM05) saat ini berada pada level 5 (optimizing process) dengan status pencapaian fully achieved sebesar 100%".

Perbedaan penelitian yang sudah disebutkan di atas di penelitian dilakukan penulis terdapat pada *domain* yang digunakan. Berdasarkan dari beberapa permasalahan pada studi kasus, penulis berkeinginan melakukan penelitian dengan domain DSS05. DSS05 merupakan salah satu proses dalam DSS (*Deliver*, *Service*, *Support*). Pemilihan domain DSS05 dikarenakan berdasar kondisi pada PT. XYZ yang memiliki sistem informasi EUCLID, teknologi informasi tersebut sudah dibuat rencana (*plan*), sudah dibangun (*build*), juga saat ini tengah berjalan (*run*) melihat *workflow* juga *business process*. Penelitian ini diharapkan dapat memberikan usulan memakai *Framework* COBIT 5 sebagai rekomendasi untuk perbaikan sistem informasi kedepannya dengan domain DSS05 untuk mencapai IT-goals pada perusahaan.

II. SIGNIFIKANSI STUDI

A. Tahapan Penelitian

Penelitian ini terdiri atas 3 tahap, mulai dari tahap perencanaan, pengumpulan data, serta analisadan pengolahan data.



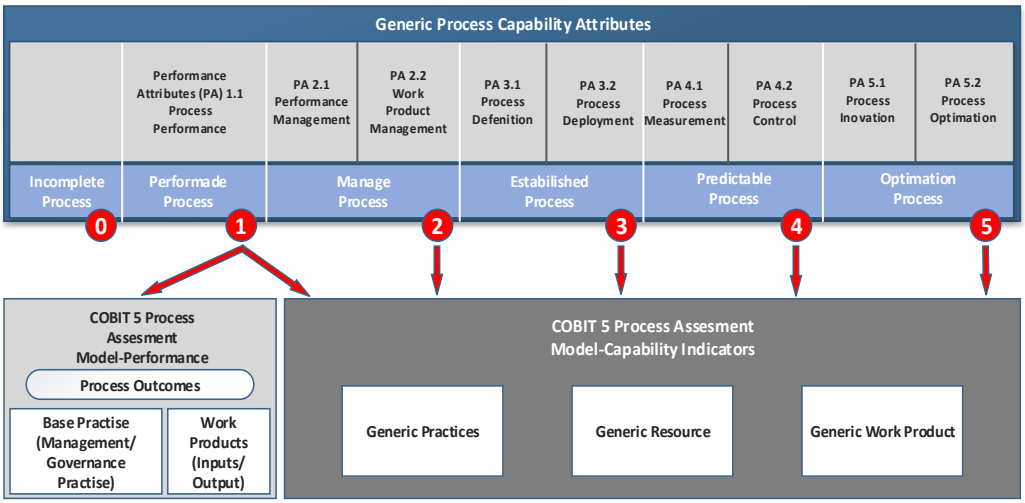
Gambar 1. Metodologi Penelitian

1. Tahap Perencanaan

Tahapan ini terdiri dari identifikasi masalah, menentukan tujuan, studi pustaka, menentukan data yang diperlukan, dan menentukan responden. Identifikasi masalah bertujuan untuk mengetahui permasalahan-permasalahan yang pernah terjadi dalam Sistem Informasi EUCLID. Tujuan dari penelitian ini adalah untuk mengetahui tingkat kapabilitas dan keamanan sistem informasi pada sistem euclid. Untuk menghasilkan rekomendasi kedepannya sebagai perbaikan sistem informasi dengan domain DSS05 untuk mencapai IT-goals pada perusahaan. Studi pustaka dilakukan untuk mengetahui teori mengenai tata kelola IT, COBIT 5 sebagai Framework dalam pengelolaan IT, DSS05 (*Manage Service Security*), RACI *Chart* dan juga *Process Assesment Model* (PAM). Selanjutnya menentukan data yang diperlukan untuk meneliti keamanan sistem, dan terakhir yaitu menentukan responden. Dalam penelitian ini, peneliti menggunakan RACI Chart untuk mengetahui individu/kelompok yang memiliki peran pada COBIT 5.

2. Tahap Pengumpulan Data

Tahap ini terdiri dari observasi dan wawancara. Observasi dilakukan di PT. XYZ yang bertujuan untuk mengumpulkan informasi yang dibutuhkan dan mengidentifikasi masalah yang ada. Wawancara dilakukan pada staff perusahaan PT. XYZ bertujuan untuk mengetahui masalah pada keamanan sistem informasi yang terdapat pada perusahaan ini. Langkah selanjutnya yaitu menyusun dan membagikan kuesioner. Kuisioner merupakan angket yang berisi beberapa pertanyaan tertulis yang disebar kepada responden yang dibuat berdasarkan *Framework* COBIT 5 proses domain DSS05 (*Manage Security Service*). Penelitian ini menggunakan kuisioner *Capability Level*. Pembuatan Kuesioner *Capability Level* Kuesioner ini nantinya akan dibuat berdasarkan*Key Management Practice* yang ada didalam *Framework* COBIT 5 proses domain DSS05 (*Manage Security Service*). Kapabilitas proses dinyatakan dalam atribut proses yang dikelompokkan ke dalam tingkat kapabilitas, seperti yang ditunjukkan pada Gambar 2 [9].



Gambar 2. *Capability Levels and Process Atribute*

Kapabilitas memiliki 6 tingkatan yang bisa diraih proses, mencakup "proses yang tidak lengkap" apabila pelaksanannya tidak memenuhi sasaran proses yang diinginkan:

a. Incomplete Process (Level 0)
   Di tingkat level 0, proses tidak dilaksanakan ataupun mengalami kegagalan dalam meraih tujuan dari proses. Pada tahap ini, bukti perolehan tujuan proses secara sistematis hanya sedikit bahkan atau tidak ada.
b. Performed Process (Level 1)
   Di tingkat ini pengimplementasian proses meraih tujuan dari proses.
c. Managed Process (Level 2)
   Di tingkat level 2, penjelasan proses yang sudah diuraikan sebelumnya, saat ini dilakukan pengelolaan (disesu aikan, dipantau, dan direncanakan) dan produk kerja ditetapkan, dipelihara, dan di kendalikan dengan benar.
d. Established Process (Level 3)
   Di tingkat ini, proses telah dikelola yang sudah dibeli penjelasan sebelumnya, saat ini diimplementasikan menggunakan proses pendefinisikan yang dapat meraih hasil dari proses tersebut.
e. Predictable Process (Level 4)
   Ditingkat ini, proses yang sudah diberi penjelasan sebelumnya, saat ini berjalan dengan batas yang ditetapkan guna mendapatkan keluaran proses.
f. Optimazing Process (Level 5)
   Ditingkat level 5, proses yang mampu di ramal yang sudah diberi penjelasan sebelumnya senantiasa dilakukan peningkatan supata mampu mencapai tujuan bisnis sekarang ini dan yang relevan proyeksinya. Masing-masing tingkatan kemampunya bisa diraih apabila tingkatan setelah level ini tercapai sepenuhnya.

3. Tahap Analisis dan Pengolahan Data

Di fase ini, ditentukan tingkatan Kapabilitas yang memberi gambaran seberapa jauh pengukuran mengenai audit keamanan informasi pada Sistem EuClid di PT, XYZ, apa sudah sesuai standar proses tata kelola IT yang baik dilihat dari domein DSS *Framework* COBIT 5 yakni pada proses domain DSS05 (*Manage Security Service*). DSS singkatan dari *Deliver*, *Service*, and *Suppor.* Saat menentukan tingkatan kapabilitas tersebut, nilai yang dihasilkan berasal dari hasil perolehan di setiap atribut, apakah telah dicapai sepenuhnya menggunakan tanda huruf F ataupun kebanyakan telah dicapai menggunakan tanda huruf L. Simbol F menyatakan *Fully Achived,* melainkan simbol L menyatakan *Large achieved*. Persyarakan supaya dapat lanjut ke proses setelahnya yakni apabila atribut tersebut telah meraih peringkat F

(*Fully Achived*) pada proses sebelumnya. Sesudah kuesioner disebar, langkah setelahnya yakni mengolah data dan mendapatkan hasil kapabilitas yang mencakup rekapabilitas jawaban dari setiap responden.

Maing masing atribut diberi penilaian berupa peringkat dengan memakai skala peringkat standar ISO / IEC 15501-2-2003 yang diperjelas didalam Tabel I memperlihatkan peringkat sebagai persentase [9].

TABEL I
ISO / IEC 15501-2-2003. SKALA PERINGKAT.

Abbreviation	***%Achieved***	***Description***
N	0% to 15% *achievement*	*Not Achieved*
P	>15% to 50% *achievement*	*Partially achieved*
L	>50% to 85% *achievement*	*Large achieved*
F	>85% to 100% *achievement*	*Fully achieved*

Peringkat tersebut meliputi:

a. *Not Archivied* (N)
   Pada skala peringkat ini ada sedikit atau tidak ada bukti pencapaian atribut yang didefinisikan dalam proses yang dinilai. Dengan rentang nilai antara 0% sampai 15% *achievement*.
b. *Partially Archived (P).*
   Pada skala peringkat ini ada beberapa bukti pendekatan, dan beberapa pencapaian, atribut yang ditentukan dalam proses yang dinilai. Beberapa aspek pencapaian atribut mungkin tidak dapat diprediksi. Dengan rentang nilai antara 15% sampai 50% *achievement*.
c. *Largery Archived (L)*
   Pada peringkat ini sebagian besar telah dicapai. Ada bukti pendekatan sistematis, dan pencapaian signifikan, atribut yang ditentukan dalam proses yang dinilai. Beberapa kelemahan terkait dengan atribut ini mungkin ada dalam proses yang dinilai. Dengan rentang nilai antara 50% sampai 85% *achievement*.
d. *Full Archived (F)*
   Pada peringkat ini sepenuhnya telah tercapai. Ada bukti pendekatan yang lengkap dan sistematis, dan pencapaian penuh dari, atribut yang ditentukan dalam proses yang dinilai. Tidak ada kelemahan signifikan terkait dengan atribut ini ada dalam proses yang dinilai. Ada kebutuhan untuk memastikan tingkat interpretasi yang konsisten ketika memutuskan peringkat mana yang akan ditetapkan. Dengan rentang nilai pencapaian diantara 85% hingga 100%.

III. HASIL DAN PEMBAHASAN

A. Analisis Sistem Informasi Euclid

EuClid *Application Framework* adalah sebuah perangkat lunak pengembangan sistem untuk solusi bisnis perusahaan agar lebih inovatif dan efisien yang membantu untuk proses pengajuan dan approval proposal pendanaan di PT. XYZ, administrasi hingga *payslip*. Selain itu Euclid berfungsi sebagai pendataan, laporan bagi setiap *staff* /karyawan baik di kantor pusat maupun dicabang. Adapun user yang terlibat pada system informasi *Euclid* ini adalah direktur, *grand manager, assistant manager, staff* dan admin.

Dalam implementasinya, EuClid sebagai sistem informasi yang digunakan oleh perusahaan sudah berjalan cukup lama, Dari hasil wawancara didapatkan beberapa kendala yang dihadapi dalam penggunaannya, diantaranya beberapa laporan pengajuan yang hilang pada system

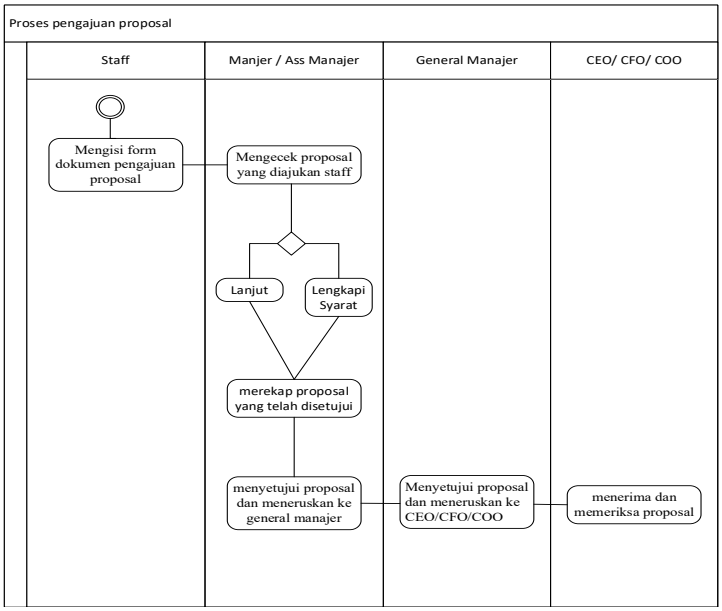
sementara pengajuan tersebut belum disetujui ataupun dilihat oleh pimpinan, hal ini menjadi masalah karena laporan pengajuan ada yang bersifat penting, pernahnya mengalami peretasan dan kebocoran data dan permasalahan selanjutnya yaitu jaringan, sulitnya mengakses sistem informasi ketika *server* mengalami gangguan, ataupun ketika *provider* mengalami gangguan, akibatnya menghambat proses administrasi dan pelaporan. Ini tentu beresiko kepada keamanan di sistem informasi itu, hingga dikaitkan dengan hal ini, penulis menghubungkannya dengan proses DSS05 *(Manage Security Service).*

Berikut ini merupakan analisa system yang sedang berjalan pada EuClid di PT. XYZ yang terdiri dari:

a. Proses pengajuan proposal

Proses pengajuan proposal dilakukan oleh staff di PT. XYZ. Didalam proses ini ada 4 bagian user yang terlibat yaitu staff, manager/asisten manajer, general manajer, CEO /CFO/COO degan keterangan sebagai berikut:

1. Staff masuk ke system
2. Staff mengisi form dokumen pengajuan proposal
3. Manajer/assisten manajer mengecek proposal yang diajukan staff
4. Manajer/assisten manajer merekap proposal
5. Manajer/assisten manajer menyetujui proposal dan meneruskan ke general manajer
6. General manager menyetujui proposal dan meneruskan ke CEO/CFO/COO
7. CEO/CFO/COO menerima dan memeriksa proposal.



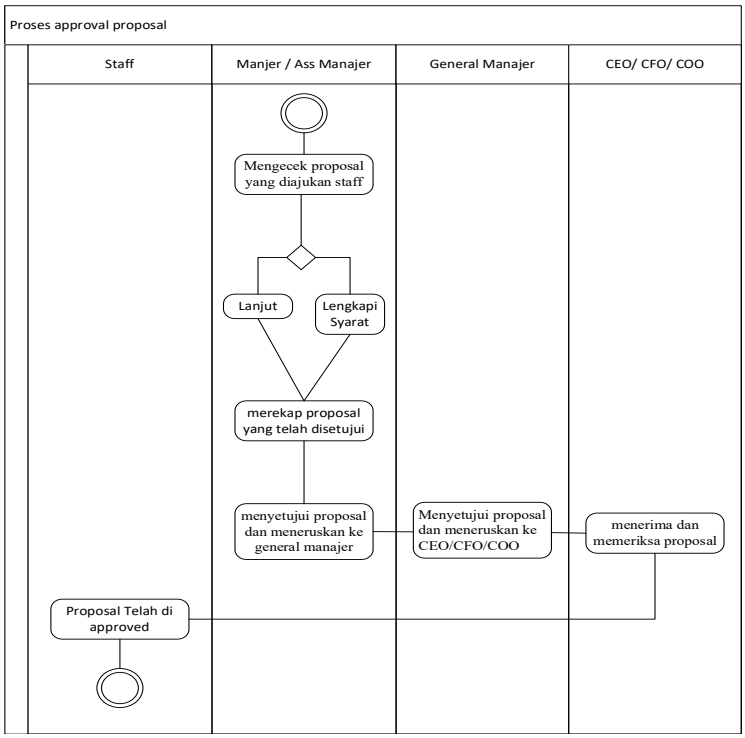
Gambar 3 Proses Pengajuan Proposal

b. Proses Approval

Proses approval proposal dilakukan oleh CEO/CFO/COO di PT. XYZ. Didalam proses ini ada 4 bagian user yang terlibat yaitu staff, manager/asisten manajer, general manajer, CEO /CFO/COO degan keterangan sebagai berikut:

1. Manajer/assiten manajer menerima proposal yang diajukan oleh staff
2. Manajer/assiten manajer memeriksa proposal
3. Manajer/assiten manajer menyetujui proposal
4. Manajer/assiten manajer merekap proposal yang disetujui dan meneruskan ke general manajer
5. General manajer menyetujui proposal dan meneruskan ke CEO/CFO/COO
6. CEO/CFO/COO memeriksa proposal

7. CEO/CFO/COO menyetujui proposal
8. Staff menerima feedback bahwa proposal telah di approved



Gambar 4. Proses Approve Proposal

B. Mengindentifikasi Masalah

Identifikasi masalah adalah tahap awal yang dilakukan dalam proses analisis. Hal yang dilakukan pada tahap ini meliputi menganalisa data dengan mendefenisikan masalah yang terjadi pada studi kasus. Proses ini didapat dari hasil wawancara dengan *staff* IT PT. XYZ adapun permasalahan yang ditemukan terdiri dari:

a. Adanya laporan pengajuan yang hilang pada system sementara pengajuan tersebut belum disetujui ataupun dilihat oleh pimpinan.
b. Pernahnya mengalami peretasan dan kebocoran data
c. Sulitnya mengakses sistem informasi ketika *server* mengalami gangguan, ataupun ketika *provider* mengalami gangguan.

C. Analisis RACI Chart

RACI Chart digunakan untuk menentukan responden pada penelitian ini. RACI Chart yaitu matriks yang memberi penggambaran peran beberapa pihak guna menyelesaikan tugas kerja di proyek juga proses bisnis yang ada. Berikut ini merupakan Tabel II daftar responden DSS05:

TABEL II
DAFTAR RESPONDEN DSS05

Management Practice (COBIT 5)	Jabatan (Pelaksana)	Studi Kasus	Jumlah
Chief Risk Officer	CEO/CFO/COO	PT. XYZ	**1**
Chief Risk Officer	General manajer	PT. XYZ	**1**
Chief Risk Officer	Manajer / Asisten manajer	PT. XYZ	**1**
Head IT Operation	Staff	PT. XYZ	**1**
Jumlah			**4**

Berikut merupakan strukur RACI Chart yang ada pada PT. XYZ:

TABEL III
STRUKTUR RACI

Activity	CEO/CFO/COO	*General manajer*	*Manager/ Asisstant Manager*	Staff
DSS05.01 Protect againts malware	C	C	C	R
DSS05.02 Manage network and connectivity security	C	C	C	R
DSS05.03 Manage endpoint security	C	C	C	R
DSS05.04 Manage user identify and logical access	C	C	C	R
DSS05.05 Manage physical access to IT assets	C	C	C	R
DSS05.06 Manage sensitive document and output device	C	C	C	R
DSS05.07 Monitor the infrastructure	C	C	C	R

Bentuk pernyataan RACI chart yaitu "pernyataan panduan yang meliputi *Responsible* (Tanggung Jawab) yang menjelaskan siapa mendapatkan tugas yang harus dilakukan, *Accountable* (Akuntabel) menjelaskan siapa bertanggung jawab atas keberhasilan tugas, *Consulted* (Konsultasi) menjelaskan siapa memberi masukan, *Informed* (Informasi) menjelaskan siapa menerima informasi ketika keputusan dibuat ataupun diselesai".

D. Penggunaan COBIT 5.0 Process Assesment Model

Process Assesment Model (PAM) ialah standar pengukuran untuk mengukur tingkat kematangan dalam IT Enterprise bersumber dari ISO/IEC 15504. Dalam PA, suatu pencapaian yang penting bagi organisasi sudah termasuk dalam level kapabilitas 1. Pada level 1 ini telah menunjukkan tujuan dari proses yang telah tercapai. Sedangkan pada maturity level, proses dapat menggapai level 1 ataupun level 2 tanpa harus memperoleh pencapaian kriteria yang penuh. Ini berarti bahwasanya pengukuran yang dilakukan memakai PAM dapat memberi penilaian lebih rendah jika dibandingkan dengan maturity level.

E. Hasil Kuesioner

Berikut ringkasan hasil pencapaian level beserta rincian spesifik perihal penilaian proses dan penilaian atribut, dapat dilihat pada Tabel IV.

TABEL IV
RINGKASAN HASIL PENCAPAIAN KUESIONER

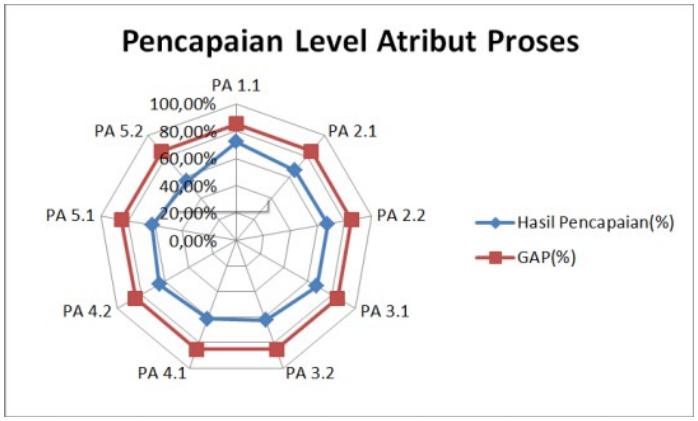
Level	**1**	**2**		**3**		**4**		**5**	
Process Atribute	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Percentage	62.5	63.54	67.18	62.5	63.54	61.45	63.75	60.93	58.33
Rating by Criteria	L	L	L	L	L	L	L	L	L
Capability Level	62.5%	65.36%		63.02%		62.45%		59.63%	

Berdasarkan tabel diatas, maka didapatkan hasil tingkat kapabilitas pengelolaan layanan keamanan informasi hasilnya ada di level 1 (*Performed Process*) di status *Large Achieved* yakni 62,5% dimana proses layanan keamanan informasi belum sepenuhnya dikelola dengan baik juga belum adanya kebijakan tertulis mengenai prosedur pengaplikasian proses layanan keamanan sehingga rencana belum jelas dan belum bisa direalisasikan dari pihakperusahaan.

Implementasi proses layanan keamanan informasi pada sistem informasi Euclid pihak perusahaan telah menyadari pentingnya perlindungan terhadap *malware* dimana setiap perangkat yang digunakan untuk menjalankan sistem Euclid harus windows asli, pemasangan anti virus serta menggunakan *Virtual Privat Number* (VPN) untuk pencegahan pengaksesan dari luar oleh orang yang tak bertanggung jawab. Pegawai juga sangat memperhatikan keamanan terhadap perangkat yang mereka pakai dengan cara selalu menyertakan password pada perangkat yang akan digunakan mengakses sistem Euclid, yang terdiri dari password saat menghidupkan perangkat pc maupun laptop, kemudian password saat hendak masuk menggunakan jaringan VPN, dan terakhir memakai password pada saat hendak login kedalam aplikasi. Dokumen penting yang digunakan disimpan dalam lemari terkunci untuk menjamin keamanan dokumen tersebut, dan permasalahan yang ada mengenai sistem Euclid dapat langsung disampaikan kebagian pusat agar dapat segera ditangani.

F. Pencapaian Level pada Proses DSS05

Berikut ini nilai hasil pencapaian proses DSS05 *(Manage Security Service)* yang bisa dilihat di Gambar dibawah ini:



Gambar 5. Diagram Radar Pencapaian Level pada DSS05

Berdasarkan grafik level domain DSS05 diatas, diketahui bahwasanya rata-rata pencapaian pada level 1 adalah 62,5%, level 2 adalah 65,36%, level 3 adalah 63,02%, level 4 adalah 62,6%, dan level 5 adalah 59,63% yang mana keseluruhannya berada pada status *largery achieved.* Dan dari rata-rata pencapaian tersebut tidak ada yang melewati batas dari nilai gap sebesar 85,01%. Hal ini menunjukkan bahwa sebagian besar atribut sudah tercapai ditunjukkan dengan adanya proses layanan keamanan informasi walaupun masih terdapat beberapa kriteria yang masih belum terpenuhi.

G. Analisis Kesenjangan (GAP Analysis)

Dari hasil pencapaian tingkat kapabilitas proses layanan keamanan informasi yang berkaitan dengan sistem informasi Euclid pada PT. XYZ saat ini sebesar 62,5% di status *Largely Achieved.* Ini bahwasanya proses layanan keamanan informasi yang ada belum sepenuhnya tercapai pada level 1, sehingga target levelnya saat ini masih pada level 1. Berikut ini merupakan Tabel GAP *Analysis*.

TABEL V
ANALISIS KESENJANGAN PROSES ATRIBUT

Process Atributte	***Percentase as is***	***Percentase to be***	***GAP***	**Pembahasan**
Level 1 PA 1.1 *Process Performance*	62,5%	85,01%	22,51%	Kesenjangan pada level ini cukup besar. Hal ini dikare nakan proses keamanan indormasi hanya diawasi jika terdapat gangguan ataupun masalah pada sistem informasi Euclid.
Level 2 PA 2.1 *Performance Management*	63,54%	85,01%	21,47%	Kesenjangan pada level ini cukup besar, hal ini dikarenakan layanan keamanan informasi belum diidentifikasi dengan jelas, komunikasi mengenai proses layanan keamanan hanya dilakukan ketika terjadi masalah.
PA 2.2 Work *Product Managemen*	67,18%	85,01%	17,83%	Kesenjangan pada level ini cukup besar, hal ini dikarenakan belum adanya kriteria kualitas terhadap layanan keamanan informasi.
Level 3 PA 3.1 *Process Defenition*	62,5%	85,01%	22,51%	Kesenjangan pada level ini cukup besar, hal ini dikarenakan belum adanya prosedur tertulis yang diterapkan untuk menjalankan proses layanan keamanan informasi.
PA 3.2 *Process Deployment*	63,54%	85,01%	21,47%	Kesenjangan pada level ini cukup besar, hal ini dikarenakan belum adanya standar tertulis yang ditetapkan untuk menjalankan proses layanan keamanan informasi.
Level 4 PA 4.1 *Process Measurement*	61,45%	85,01%	23,56%	Kesenjangan pada level ini cukup besar, hal ini dikarenakan belum adanya penetapan pengukuran performa dan pendefenisian mengenai proses keamanan layanan informasi.
PA 4.2 *Process Control*	63,75%	85,01%	21,26%	Kesenjangan pada level ini cukup besar, hal ini dikarenakan belum terdapat detail teknik analisa dan kontrol untuk mengukur efektivitas, belum adanya penetapan parameter dan standar untuk mengontrol performa kegiatan proses layanan keamanan informasi yang dilakukan.
Level 5 PA 5.1 *Process Inovation*	60,93%	85,01%	24,08%	Kesenjangan pada level ini cukup besar, hal ini dikarenakan rencana peningkatan proses layanan keamanan informasi dibuat oleh bagian pusat bersama dengan pemangku kepentingan lainnya, sehingga belum diketahui apa saja yang akan dilakukan.
PA 5.2 *Process Optimation*	58,33%	85,01%	26,68%	Kesenjangan pada level ini sangat besar, hal ini dikarenakan belum terdapat penilaian khusus terhadap proses layananan keamanan informasi.

H. Strategi Perbaikan

Dalam strategi perbaikan yang akan dilakukan dengan cara mengaudit dan mengontrol kembali dalam setiap proses atribut yang telah dicapai pada level 1 dengan berpedoman indikator proses atribut. Berikut ini pemaparan strategi perbaikan pada tiap proses atribut:

a. Level 1 PA 1.1 *Process Performance*
   1) Melaksanakan pelatihan supaya bisa membuat tingkat kedadaran meningkat terhadap perlindungan pada malware sangatlah penting dengan mengembangkan kebijakan keamanan guna memberi perlingdungan PC ataupun laptop setiap karyawan di PT X dari ancaman *malware* seperti virus, worm, trojan dan sebagainya. Tidak membuka website sembarangan, tidak mendownload dari website yang tidak terpercaya, dan menggunakan email sembarangan, rutin membersihkan temporary internet files, cookie, dsb. Selalu melakukan pembaharuan terhadap aplikasi yang digunakan (update plugin, update web browser, update antivirus dsb), tidak memberikan password kepada orang lain dan melakukan penggantian password secara berkala.
   2) Membuat kebijakan mengenai pengamanan perangkat seperti laptop, printer, PC dengan membuat prosedur pengelolaan pengamanan perangkat TI untuk penggunaan tugas kerja pribadi seperti misalnya pegawai tidak diperbolehkan membawa makanan/minuman disekitar PC. Kemudian dengan untuk tetap mangamankan PC pegawai dengan mengunci otomatis atau mati otomatis saat tidak digunakan lebih dari 10 menit serta menambahkan alat penutup pada perangkat TI seperti PC, laptop dan printer.
   3) Melaksanakan komunikasi dengan semua pemangku kepentingan mengenai proses penyediaan keamanan informasi.

b. Level 2 PA 2.1 *Performance Management*
   1) Pengamatan pada proses pelayanan keamanan infomasi tidak hanya dilaksanakan saat terjadinya gengguan ataupun permasalahan saja,, tetapi juga termasuk dengan bagaimana cara melakukan pencegahan agar tidak terjadi permasalahan yang dapat mengganggu keberjalanannya pelayanan keamanan informasi.
   2) Mendefenisiskan dengan sejelas jelasnya kepada pihak yang berhubungan pada proses pelayanan keamanan informasi, melakukan identifikasi peran dan tanggung jawab untuk tiap pihak yang terlibat, serta merencanakan dan memantau proses layanan keamanan informasi.

c. Level 2 PA 2.2 *Work Product Management*
   1) Menentukan standar guna menilai proses pelayanan keamanan informasi yang dilakukan. Misalnya seperti kriteria kualitas untuk frekuensi terjadinya permasalahan atau ancaman TI.
   2) Menetapkan waktu utnuk penilaian hasil kerja proses layanan keamanan informasi untuk dapat mengetahui perkembangan proses layanan keamanan informasi.
   3) Melaksanakan aksi guna menganalisis hasil pproses pelayanan keamanan informasi, melaksanakan rembukan bersama pihak yang berhubungan, hal ini dilakukan supaya dapat melihat pengambaran sekarang ini tentang proses pelayanan keamanan informasi.

IV. KESIMPULAN

Audit keamanan Sistem Informasi EuClid pada PT. XYZ dilakukan memakai *framework* COBIT 5 dengan domain DSS05 (*Manage Security Service*). Audit keamanan sistem informasi ini dilakukan dengan menyebarkan kuesioner kepada 4 responden yang pilih berdasarkan RACI *Chart*. Hasil pencapaian nilai dari setiap level pada proses domain DSS05 yaitu level 1 (*performed process*) sebesar 62,5%, level 2 (*Manage Process*) adalah 65,36%,

level 3 (*Established Process*) sebesar 63,02%, level 4 (*Predictable Process*) adalah 62,6%, dan level 5 (*Optimizing Process*) adalah 59,63%. Pencapaian pada setiap level berada pada rentang 50% - 85%, sehingga peringkat dalam standar ISO/IEC 15501-2-2003 berada di *Largely Achieved* (Sebagian besar terpenuhi). Dari rata-rata pencapaian tersebut tidak ada yang melewati batas dari nilai gap sebesar 85,01%. Hal ini menunjukkan bahwa sebagian besar atribut sudah tercapai ditunjukkan dengan adanya proses layanan keamanan informasi walaupun masih terdapat beberapa kriteria yang masih belum terpenuhi. Strategi yang dapat dilakukan oleh PT. XYZ untuk mencapai kapabilitas di level 1 antara lain (1) PA 1.1 *Process Performance* dengan memberikan pelatihan untuk membuat orang lebih sadar bagaimana melindungi diri dari malware, membuat kebijakan tentang bagaimana perangkat IT harus dilindungi, berkomunikasi dengan semua pihak yang terkait tentang proses pelayanan keamanan informasi, juga mencari tahu banyak hal tentang tanggung jawab serta peran keamanan informasi proses layanan. 2) PA 2.1 Manajemen Kinerja dengan mendefinisikan dengan jelas pihak terlibat di proses layanan keamanan informasi dan melakukan pemantauan proses secara berkala. 3) PA 2.2 Manajemen Produk Kerja dengan menetapkan kriteria untuk mengevaluasi hasil kerja proses layanan keamanan informasi dan melakukan analisis guna menentukan deskripsi proses saat ini.

REFERENSI

[1] A. Gunawan and J. F. Andry, "Audit Aplikasi Zahir di PT Radisa Mahardi Rekatama Menggunakan Framework COBIT 5," vol. 2, no. 2502, 2017.

[2] D. Ciptaningrum, E. Nugroho, and D. Adhipta, "COBIT 5 Sebagai Metode Alternatif Bagi Audit Keamanan Sistem Informasi (Sebuah Usulan Untuk Diterapkan di Pemerintah Kota Yogyakarta)," *Semin. Nas. Teknol. Inf. dan Multimed.*, no. 2302–3805, pp. 6–8, 2015.

[3] R. P. Kusuma, "AUDIT TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 PADA DOMAIN DSS (DELIVER, SERVICE, AND SUPPORT) (STUDI KASUS: KONSULTAN MANAJEMEN PUSAT)," vol. 9, no. 1, pp. 97–109, 2019.

[4] H. M. Kurnia, R. N. Shofa, and R. Rianto, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Berdasarkan Domain APO12," *J. SITECH Sist. Inf. dan Teknol.*, vol. 1, no. 2, pp. 99–106, 2019, doi: 10.24176/sitech.v1i2.2723.

[5] R. W. Witjaksono, "Audit Sistem Informasi Akademik Universitas Telkom menggunakan Framework COBIT 5 Domain DSS untuk Optimasi Proses Service Delivery Telkom University Academic Information System Audit using COBIT 5 Framework Domain DSS for Optimization Service Delivery Pro," vol. 6, 2019.

[6] P. A. Pratama, G. R. Dantes, and G. Indrawan, "AUDIT SISTEM INFORMASI UNIVERSITAS PENDIDIKAN GANESHA DENGAN FRAMEWORK COBIT 5," vol. 9, no. 2, 2020.

[7] M. Muthmainnah, S. Safwandi, M. Jannah, and V. Ilhadi, "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Proses Dss03 Dan Mea01 Di Universitas X," *Sisfo J. Ilm. Sist. Inf.*, vol. 5, no. 1, pp. 1–12, 2021, doi: 10.29103/sisfo.v5i1.4848.

[8] M. A. Wicaksono, Y. Rahardja, and H. P. Chernovita, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Domain Edm," *JSiI (Jurnal Sist. Informasi)*, vol. 7, no. 1, p. 25, 2020, doi: 10.30656/jsii.v7i1.2017.

[9] ISACA, *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT- Executive Summary*. 2016.

[10] Pertama, P. P. G. P., & Ardiyasa, I. W. Audit Keamanan Sistem Informasi Perpustakaan

STMIK STIKOM Bali Menggunakan Kerangka Kerja COBIT. *Jurnal Sistem Dan Informatika (JSI)*, *13*(2), 77–86. 2019

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih banyak kepada Tim *Jurnal Informatika Polbeng* yang telah meluangkan waktunya untuk membuat template ini. Dengan adanya template ini, penulis dimudahkan dalam membuat dan menyusun penelitian hingga menjadi sebuah jurnal yang siap untuk dipublikasikan