Volume 9 Nomor 1, 2023, 34-41
ISSN: 2460-1799 P-ISSN: 1432-602743

Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019

Asro Nasiri[1*]

[1] Ilmu Komputer, Informatika, Universitas Amikom, Yogyakarta, Indonesia
Email: [1]asro@amikom.ac.id*
[1] *Jurusan Informatika Ilmu Komputer AMIKOM*
Jl. Pajajaran, Condong Catur, Yogyakarta, Indonesia
[1]asro@amikom.ac.id

Abstrak

Ketergantungan organisasi terhadap dukungan teknologi informasi semakin besar. Proses bisnis saat ini hampir tidak ada yang tidak menggunakan teknologi informasi untuk meningkatkan daya saing. Penggunaan teknologi informasi harus disertasi dengan peningkatan keamanan informasinya. Gangguan terhadap keamanan informasi di organisasi akan menghambat pencapaian tujuan dan strategi organisasi. Informasi saat ini merupakan aset yang sangat penting bagi universitas XYZ, karena itu evaluasi terhadap seberapa baik pengendalian dan kegiatan dalam melindungi aset informasi perlu dilakukan di universitas XYZ. Evaluasi dilakukan menggunakan kerangka kerja COBIT 2019 pada domain APO12, APO13 dan DSS05 untuk mengidentifikasi berapa tingkat kapabilitas universitas XYZ dalam mengelola keamanan informasi. Hasil evaluasi menunjukkan pengelolaan keamanan informasi di Universitas XYZ masih di tingkat kepabilitas 2 untuk domain APO12, APO13 dan DSS05. Telah dihasilkan 17 rekomendasi perbaikan peningkatan implementasi keamanan informasi.
Kata kunci : Keamanan informasi, COBIT 2019, evaluasi, tingkat kapabilitas, APO12, APO13, DSS05

Abstract

Organizational dependence on information technology support is getting bigger. Very few business processes today use information technology to increase competitiveness. An increase in information security must accompany the use of information technology. Disruption of information security in the organization will hinder organizational goals and strategies. Information is currently a vital asset for the XYZ university; therefore, an evaluation of how well the controls and activities are in protecting information assets needs to manage at the XYZ university. The assessment uses the COBIT 2019 framework in the APO12, APO13, and DSS05 domains to identify XYZ university's capability in managing information security. The evaluation results show that information security management at XYZ University is still at capability level 2 for the APO12, APO13, and DSS05 domains. There are 19 recommendations for improving the implementation of information security.

Key Words: Information security, COBIT 2019, evaluation, capability level, APO12, APO13, DSS05.

I. PENDAHULUAN

Peran teknologi informasi dalam mendukung proses bisnis organisasi saat ini cukup tinggi. Penggunaan teknologi informasi harus juga disertasi dengan pengendalian terhadap faktor resikonya yaitu resiko kehilangan atau penyalahgunaan data karena aset informasi saat ini menarik bagi penyerang baik karena motif ekonomi atau motif lainnya [1] Informasi merupakan aset berharga bagi organisasi sehingga keamanan informasi menjadi penting untuk dikendalikan sesuai standar. Keamanan informasi mempertimbangkan keamanan sistem komputer untuk melindunginya dari pengungkapan, modifikasi subyektif, akses tidak sah, pelecehan, atau perusakan yang bertujuan untuk memastikan integritas, kerahasiaan, dan ketersediaan informasi [2] Keamanan informasi adalah bagian penting dari operasi organisasi mana pun, karena membantu melindungi aset teknologi dan informasi yang digunakan oleh organisasi. Keamanan data yang lemah dapat menyebabkan informasi penting hilang atau dicuri, menciptakan pengalaman buruk bagi pelanggan dan merusak reputasi organisasi. Keamanan informasi juga membantu mengurangi risiko insiden keamanan dan kehilangan data, memastikan kelangsungan bisnis dan melindungi klien organisasi.

Keamanan informasi mencakup perlindungan informasi terhadap berbagai ancaman yang bertujuan untuk meminimalkan risiko aktivitas bisnis, memaksimalkan pengembalian investasi, memanfaatkan peluang bisnis, dan memastikan kelangsungan bisnis. Pertimbangan keamanan informasi menargetkan integritas, kerahasiaan, dan ketersediaan sumber daya informasi. Manajemen keamanan sistem informasi bertujuan untuk meminimalkan risiko yang dihadapi sistem informasi dalam operasinya. Ini melibatkan beberapa kegiatan, seperti perencanaan, perancangan, implementasi, pemantauan, peninjauan, dan peningkatan [3]

Volume 9 Nomor 1, 2023, 34-41
ISSN: 2460-1799 P-ISSN: 1432-602743

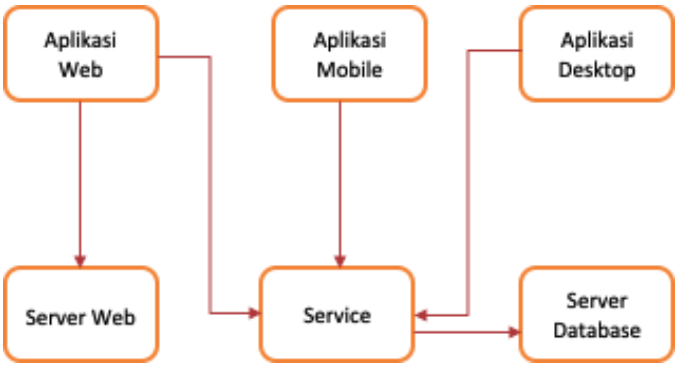
Universitas XYZ merupakan perguruan tinggi yang berdiri sejak tahun 1998. Perguruan tinggi tersebut mengelola 15 ribu mahasiswa dan 500 dosen dan karyawan. Lembaga XYZ merupakan perguruan tinggi dengan 16 program studi yang sudah mengimplementasikan teknologi informasi dari proses penerimaan mahasiswa, perkuliahan dan kelulusan. Implementasi tersebut sudah dilakukan sejak tahun 2003. Sistem informasi akademik merupakan sistem informasi utama yang telah dikembangkan mencakup layanan dari penerimaan mahasiswa baru sampai ke proses kelulusan. Pada gambar 1 dibawah ini dijelaskan komponen sistem akademik yang mendukung alur proses bisnis utama pada universitas XYZ.

Gambar 1 Komponen Sistem Akademik

Komponen tersebut adalah sistem penerimaan mahasiswa baru yang terdiri dari modul pendaftaran, modul ujian seleksi dan modul heregistrasi (pembayaran). Kemudian ada sistem informasi KRS yang terdiri dari modul alokasi dosen dan mata kuliah dan penjadwalan. Daftar sistem informasi dan modulnya dijelaskan pada table 1. Ada 3 tipe aplikasi untuk mengakses sistem informasi akademik yaitu aplikasi berbasis web, desktop dan aplikasi mobile android. Pada gambar 2 dijelaskan arsitektur informasi dari sistem informasi akademik [4] .

Tabel 1 Daftar Sistem Informasi [5]

No	Komponen Sistem Informasi	Modul
1	PMB	Pendaftaran, ujian seleksi, heregistrasi
2	KRS	alokasi dosen dan mata kuliah, alokasi penjadwalan
3	Perkuliahan	Penjadwalan, presensi, e-learning
4	Ujian	Penjadwalan, alokasi pengawas, upload soal dan koreksi
5	Kelulusan	Proses Tugas Akhir, yudisium dan wisuda



Gambar 2 Arsitektur Informasi Sistem Akademik

Ketergantungan universitas XYZ terhadap dukungan IT sudah sangat tinggi karena hampir semua proses bisnis menggunakan TI sebagai pendukung utama, sehingga evaluasi terhadap seberapa baik pengendalian di aspek keamanan informasi sangat urgen untuk menghindari gangguan terhadap kegiatan bisnisnya. Usaha serangan terhadap infrastruktur maupun layanan aplikasi sudah sering terjadi baik dari kalangan internal yaitu dari mahasiswa atau dari sumber eksternal.

Evaluasi terhadap tingkat kepabilitas organisasi dalam pengendalian keamanan informasi dapat mengacu ke beberapa kerangka kerja seperti misalnya ISO 27001, ITIL, atau COBIT [6]. Pada penelitian ini kerangka kerja yang digunakan adalah COBIT 2019 yang merupakan versi terbaru dari COBIT. COBIT 20019 terdiri dari 40 kegiatan yang memberikan acuan praktek baik dalam mengelola TI baik dari sisi perencanaan, operasional maupun pengawasan kinerjanya [7]. 40 kegiatan dari COBIT 2019 yang terkait dengan aspek keamanan hanya ada 3 domain yaitu domain APO12 (*managed risk*), APO13 (*managed security*) dan DSS05 (*managed security services*).

Beberapa penelitian sebelumnya yang telah dilakukan untuk evaluasi keamanan informasi menggunakan COBIT diantaranya yang dilakukan oleh Lilis [8] yang menggunakan COBIT 5 untuk mengevaluasi sebuah perusahaan yang menghasilkan skor tingkat kapabilitas, analisis gap dan juga rekomendasi peningkatan pengendalian keamanan. Penelitian lain ada yang menggunakan COBIT 2019 tetapi untuk mendesain keamanan informasi di POLRI yang menghasilkan cetak biru implementasi keamanan informasi [9], bukan untuk melakukan evaluasi pengendalian keamanan. Penelitian berikut ini juga menggunakan COBIT 2019 untuk mendesain tata kelola keamanan *e-governance* [10]

Penelitian lain menggunakan COBIT 5 untuk menyusun model pengendalian keamanan untuk transaksi keuangan berbasis web [11]. Terdapat juga peneliti yang melakukan evaluasi terhadap keamanan informasi sebuah organisasi tetapi masih menggunakan kerangka kerja COBIT versi 4.1 [12]. Penelitian lain mengkombinasikan COBIT 2019 dan ITIL 4 untuk mengevaluasi tata kelola (*govern)* dan manajemen sebuah orgniasasi dengan terlebih dahulu

Volume 9 Nomor 1, 2023, 34-41
ISSN: 2460-1799 P-ISSN: 1432-602743

memetakan proses teknologi informasi yang ada baik di COBIT 2019 dan ITIL 4. Proses pemetaan tersebut menghasilkan 9 domain pada COBIT 2019. Pada penelitian tersebut domain yang terkait dengan evaluasi aspek keamanan hanya pada domain DSS05 saja. [13] Diah Sulistyowati melakukan perbandingan antara beberapa kerangka kerja seperti NIST CSF, COBIT 2019, ISO/IEC 27002 dan PCI DSS untuk menyusun metodologi pengukuran tingkat kematangan pengendalian keamanan [14]

Pada penelitian ini penulis mencoba melakukan evaluasi khusus yang terkait dengan keamanan informasi yaitu pada domain APO12, APO13 dan DSS05 menggunakan kerangka kerja COBIT 2019 dengan pengukurannya menggunakan CMMI (*capability maturity model integration)*

II. METODOLOGI PENELITIAN

2.1 Alur Penelitian

Penelitian ini bersifat kualitatif yaitu penelitian yang menggunakan data yang diperoleh dari teknik pengumpulan data berupa wawancara, kuisioner, dan observasi [15]. Penelitian ini bertujuan melakukan pengukuran tingkat kapabilitas kegiatan dan pengendalian keamanan informasi berdasarkan kerangka COBIT 2019 pada proses APO12, APO13, dan DSS05 dan menghasilkan angka tingkat kapabilitasnya dan rekomendasi perbaikan untuk meningkatkan ke tingkat yang lebih tinggi.

Tata kelola teknologi informasi memerlukan kerangka kerja sebagai pedoman dalam teknologi informasi pengelolaan. Salah satu frameworknya adalah COBIT. COBIT membantu perusahaan dalam mengelola informasi dan teknologi perusahaan. Perusahaan informasi dan teknologi mengacu pada semua teknologi dan pemrosesan informasi yang diterapkan oleh perusahaan, tidak hanya oleh departemen teknologi dan informasi. ISACA merilis versi terbaru COBIT yaitu COBIT 2019. COBIT 2019 dinilai lebih fleksibel dan terbuka untuk berbagai referensi dan memudahkan pengguna untuk memperluas fokus bidang teknologi informasi pengelolaan. COBIT 2019 adalah penyempurnaan dari kerangka kerja sebelumnya dan mengakui bahwa hal itu dapat terjadi diterapkan di berbagai bidang organisasi. Di COBIT 2019, ada sebuah konsep baru bernama design faktor. COBIT 2019 terdiri dari 40 proses atau kegiatan seperti pada gambar 3.

Tujuan tata kelola dan manajemen dalam COBIT dikelompokkan menjadi lima domain. Domain memiliki nama dengan kata kerja yang mengungkapkan tujuan utama dan bidang kegiatan tujuan yang terkandung di dalamnya:

• Tujuan tata kelola dikelompokkan dalam domain Evaluate, Direct and Monitor (EDM). Dalam domain ini, badan pengelola mengevaluasi opsi strategis, mengarahkan manajemen senior pada opsi strategis yang dipilih, dan memantau pencapaian strategi.

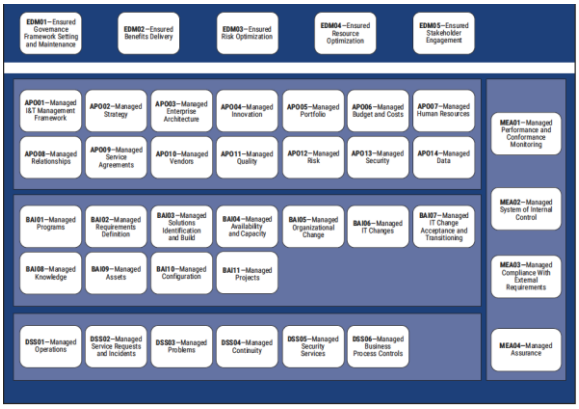
• Tujuan manajemen dikelompokkan dalam empat domain.

• Align, Plan and Organize (APO) membahas keseluruhan organisasi, strategi, dan aktivitas pendukung untuk TI.

• Build, Acquire and Implement (BAI) memperlakukan definisi, akuisisi dan implementasi solusi TI dan integrasinya dalam proses bisnis.

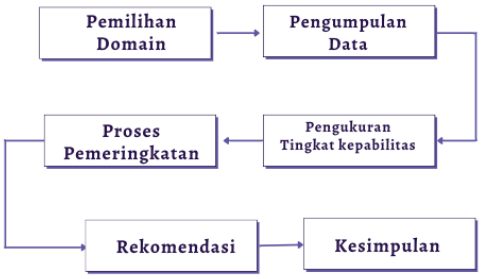
• Deliver, Service and Support (DSS) menangani operasional dan dukungan layanan TI, termasuk keamanan.

• Monitor, Evaluate and Assess (MEA) menangani pemantauan kinerja dan kesesuaian TI dengan target kinerja internal, tujuan pengendalian internal, dan persyaratan eksternal.



Gambar 3 Domain tata kelola COBIT 2019

Proses evaluasi dilakukan dengan menggunakan metologi evaluasi yang terdapat di *COBIT 2019 Introduction and Methodology* [16] seperti tergambar pada gambar 4



Gambar 4. Alur penelitian

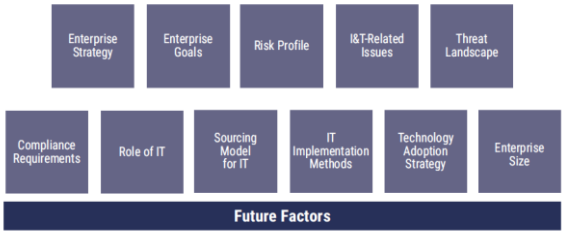
Hasil penelitian hendaknya dituliskan secara jelas dan padat. Diskusi hendaknya menguraikan arti pentingnya hasil penelitian, bukan mengulanginya. Hindari penggunaan sitasi dan diskusi yang berlebihan tentang literatur yang telah dipublikasikan.

2.1.1 Pemilihan domain:

Proses pemilihan COBIT 2019 menggunakan perangkat faktor desain (*design factor)* yang merupakan

Volume 9 Nomor 1, 2023, 34-41
ISSN: 2460-1799 P-ISSN: 1432-602743

perangkat yang baru disediakan untuk pengukuran menggunakan COBIT 2019 [17]. Pada COBIT versi sebelumnya pemilihan dilakukan dengan menggunakan metode pemetaan antara tujuan bisnis dan tujuan teknologi informasi [18]. Faktor desain adalah faktor yang dapat mempengaruhi desain sistem tata kelola perusahaan dan memposisikannya untuk sukses dalam penggunaan TI. Pada COBIT 2019, faktor inilah yang akan mempengaruhi pemilihan domain dalam rangka evaluasi seperti terlihat pada gambar 5



Gambar 5 Faktor Desain

2.1.2 Pengumpulan data:

Kuesioner dan wawancara dilakukan untuk pengumpulan data dan dalam menentukan responden menggunakan metode RACI Chart. RACI Chart adalah metode menggunakan tabel RACI pada COBIT 2019 [7]. Proses pemilihan responden dengan memilih peran (role) pada table RACI dengan tingkat tanggung jawab Responsible dan Accountable yang memiliki arti bahwa peran (role) tersebut lebih mengerti dan lebih menguasai praktek TI yang akan diteliti, sehingga data yang diolah akan lebih valid. Sama halnya seperti pada proses sebelumnya, data dari responden dengan tingkat tanggung jawab Accountable hanya akan dipakai jika tidak ada data dari responden dengan tingkat tanggung jawab Responsible yang dapat diolah atau dengan kata lain hanya bersifat opsional [19]. Berdasarkan metode ini responden yang diwawancari adalah para personil terkait seperti yang tercantum di tabel 2.

2.1.3 Menentukan tingkat kapabilitas (capability level):

Pada tahapan ini ditentukan tingkat kapabilitas yang sesuai untuk setiap kegiatan tata kelola teknologi infomasi perguruan tinggi XYZ. Pemeringkatan tingkat kapabilitas menggunakan model Capability and Maturity Model Integration (CMMI). Tingkat kemampuan ditandai dengan Level 0, Level 1, Level 2, Level 3, Level 4, dan Level 5. Penjelasan dari masing-masing karakteristik tersebut adalah sebagai berikut:

1. Level 0 - Proses ini tidak memiliki kemampuan dasar dan mencerminkan pendekatan yang tidak lengkap untuk menangani tujuan tata kelola dan manajemen atau tidak memenuhi maksud dari praktik proses apa pun.
2. Level 1 - Proses ini kurang lebih mencapai tujuannya melalui penerapan serangkaian aktivitas yang tidak lengkap yang dapat dikategorikan sebagai awal atau intuitif dan kurang terorganisir.
3. Level 2 - Proses ini mencapai tujuannya dengan mengimplementasikan serangkaian aktivitas dasar, namun lengkap, yang dapat dikategorikan telah dilakukan.
4. Level 3 - Proses pencapaian tujuannya dengan cara yang jauh lebih terorganisir dengan menggunakan aset organisasi. Proses biasanya didefinisikan dengan baik.
5. Level 4 - Proses pencapaian tujuannya didefinisikan dengan baik, dan kinerjanya diukur secara kuantitatif.
6. Level 5 - Proses pencapaian tujuannya, didefinisikan dengan baik, kinerjanya diukur untuk meningkatkan kinerja, dan dilakukan perbaikan terus-menerus

2.1.4 Proses pemeringkatan:

Proses ini untuk menilai seberapa besar pencapaian setiap tingkat kapabilitas di setiap domain dengan menggunakan kriteria NPFL yaitu Note, Partially, Fully, dan Largerly. Informasi prosentase masing-masing kriteria penilaian adalah sebagai berikut:

1. Fully (F) - Tingkat kapabilitas dicapai lebih dari 85 persen
2. Largerly (L) - Tingkat kapabilitas dicapai lebih dari sama dengan 50 persen dan kurang dari sama dengan 85 persen
3. Partially (P) - Tingkat kapabilitas dicapai lebih dari sama dengan 15 persen dan kurang dari sama dengan 50 persen
4. Note (N) - Tingkat kapabilitas kurang dari 15 persen dapat dicapai

Kriteria yang paling tinggi dari tingkat kapabilitas adalah di posisi Fully dimana hampir semua persyaratan sudah dipenuihi, sehingga apabila universitas XYZ sudah mencapai level tersebut maka dianggap sudah mengelola keamanan informasi dengan sangat baik dan bisa menjadi contoh praktek baik bagi perguruan tinggi lain

2.1.5 Rekomendasi:

Rekomendasi yang diberikan oleh COBIT 2019 mengikuti kegiatan yang ada pada level kapabilitas yang belum dicapai saat ini dan perlu diperbaiki sehingga dapat meningkat ke level kapabilitas berikutnya. Rekomendasi ini juga bermanfaat untuk pengembangan tata kelola teknologi informasi lebih lanjut karena Universitas XYZ dapat mengetahui apa saja kekurangan dari sistem tata kelola teknologi informasi saat ini. [20]

III. HASIL DAN PEMBAHASAN

3.1 Pemilihan Domain

Pemilihan proses dengan menggunakan perangkat faktor desain menghasilkan 3 domain dengan skor tertinggi yaitu domain terkait keamanan dan resiko informasi antara lain APO12, APO13 dan DSS05.

3.2 Pemilihan responden

Pemetaan RACI COBIT 2019 terhadap struktur organisasi Universtas XYZ yang terkait dengan tugas dan wewenang

Volume 9 Nomor 1, 2023, 34-41
ISSN: 2460-1799 P-ISSN: 1432-602743

keamanan informasi menghasilkan 4 responden untuk proses wawancara dan pengisian kuisioner. Kuisioner menggunakan pernyataan persyaratan yang terdapat di buku COBIT 2019 *Design and Objective* [1]

3.3 Perhitungan tingkat kapabilitas

3.3.1 Proses APO12:

APO12. Secara kontinu mengidentifikasi, menilai, dan mengurangi risiko terkait TI dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan *(Continually identify, assess and reduce TI-related risk within tolerance levels set by enterprise executive management).*

Evaluasi kegiatan ini berdasarkan data yang diambil dari hasil kuisioner dan wawancara yaitu terkait implementasi penanganan resiko pada saat ini. Data kuisioner ditujukan pada pelaksanaan proses APO12, yang dimulai pada *capability level* 2 terlebih dahulu. Dari hasil kuisioner diperoleh data dari 6 kegiatan yang dipersyaratkan oleh COBIT 2019, hanya ada 1 kegiatan yang sudah diimplementasikan dengan baik yaitu pada kegiatan no 4.
Sehingga level kapabilitasnya:

$$Proficient\_level = \frac{Number\_activities\ have\ been\ done}{number\_of\_acivities}\ x100\%$$

$$Proficient\_level = \frac{1}{6}\ x\ 100\% = 17\%$$

TABEL 2

HASIL RACI CHART

No	RACI Chart COBIT 2019	Struktur Orgnasisasi Universitas XYZ
1	Chief Executive Officer adalah orang yang berkedudukan tinggi yang bertanggung jawab atas seluruh manajemen organisasi	Direktur Teknologi Informasi
2	Business Process Owner adalah orang yang bertanggung jawab atas perfomansi proses bisnis	Direktur Akademik dan Kepala prodi
3	Service Manager adalah structural yang bertanggung jawab atas pelayanan untuk mendukung kebutuhan bisnis	Manajer layanan Sistem Akademik
4	Information Security Manager adalah struktural yang bertanggung jawab atas keamanan cyber.	Manajer Infrastruktur

Karena pada proses APO12 yang berada di capability level 2, hanya mendapatkan nilai 17% yang berarti ada di level *partially*, maka proses pengukuran *capability level* di level 3 tidak bisa dilakukan. Perlu dilakukan perbaikan di level 2 sebelum dapat diukur di level diatasnya.

Gambaran umum kondisi di Universitas XYZ terkait pengendalian resiko adalah belum ada upaya untuk mengidentifikasi resiko TI apa saja yang mungkin terjadi di lingkungan perguruan tinggi baik dari resiko yang disebabkan oleh manusia, lingkungan atau kejadian alam. Direktorat TI belum memnpuyai risk register untuk dianalisa dan ditentukan pilihan mitigasinya. Catatan insiden juga belum ada, tetapi sedang mengembangkan aplikasi ticketing untuk menangani dan mencatat semua permintaan penanganan insiden dari pengguna.

Persyaratan APO12 di level 2 yang terpenuhi hanya di no 4 yaitu telah tersedianya kesepakatan di tingkat Universitas layanan IT dan insfrastruktur mana yang diprioritaskan dan sudah diidentifikasi faktor faktor yang kritis yang perlu dijaga supaya layanan tetap kontinu dalam kondisi apapun

Rekomendasi untuk perbaikan di proses ini supaya bisa mencapai *fully* di tingkat 2 adalah:

1. Direktorat TI hendaknya menetapkan metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko TI.
2. Hendaknya ada catatan data terkait risiko TI yang relevan dan signifikan di lingkungan operasi internal dan eksternal universitas.

TABEL 3
HASIL KUISIONER APO12

	CAPABILITY LEVEL 2	Y/T
1	Tetapkan dan terus dijalankan metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko TI	T
2	Rekam data terkait risiko TI yang relevan dan signifikan di lingkungan operasi internal dan eksternal universitas.	T
3	Menginventarisasi proses bisnis dan mencatat ketergantungannya pada proses manajemen layanan TI dan sumber daya infrastruktur TI. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan outsourcing.	T
4	Menentukan dan menyepakati layanan TI dan sumber daya infrastruktur TI mana yang penting untuk mempertahankan pengoperasian proses bisnis. Menganalisis dependensi dan mengidentifikasi link yang lemah.	Y
5	Identifkasi skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.	T
6	Menjaga pencatatan aktivitas pengendalian yang ada untuk memitigasi risiko dan yang memungkinkan pengambilan risiko sejalan dengan resiko yang bisa diterima dan ditoleransi risiko. Mengklasifikasikan aktivitas kontrol dan memetakannya ke skenario risiko TI tertentu dan penyatuan skenario risiko TI.	T

3. Menginventarisasi proses bisnis apa saja yang mempunyai ketergantungan pada proses manajemen layanan TI dan sumber daya infrastruktur TI. Identifikasi tingkat ketergantungan tersebut dalam beberapa kategori. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual kritis, vendor, pemasok.

Berdasarkan wawancara, pada saat ini proses penerimaan mahasiswa baru merupakan proses bisnis yang mempunyai tingkat ketergantungan paling tinggi dan menjadi prioritas utama.

Volume 9 Nomor 1, 2023, 34-41
ISSN: 2460-1799 P-ISSN: 1432-602743

4. Membuat identifikasi resiko dengan kategorisasi, bisnis proses yang terkait dan area fungsionalnya
5. Mempertahankan inventarisasi aktivitas pengendalian yang ada untuk memitigasi risiko dan yang memungkinkan pengambilan risiko sesuai dengan selera dan toleransi risiko. Mengklasifikasikan aktivitas kontrol dan memetakannya ke skenario risiko TI tertentu dan agregasi skenario risiko TI.

3.3.2 Proses APO13:

APO13. Mendefinisikan dan memantau sebuah sistem manajemen keamanan informasi (SMKI) (*Define, operate and monitor an information security management system*).
Kegiatan yang harus dilaksanakan pada domain ini adalah pendefinisian, pengoperasian dan pemantauan sebuah sistem manajemen keamanan informasi (SMKI).

Evaluasi kegiatan ini berdasarkan data yang diambil dari hasil kuisioner terhadap pimpinan dan personil di bagian TI yaitu terkait implementasi SMKI pada saat ini. Data kuisioner ditujukan pada pelaksanaan proses APO13, yang dimulai pada *capability level* 2 terlebih dahulu. Dari hasil kuisioner diperoleh data dari 7 kegiatan yang dipersyaratkan oleh COBIT 2019, hanya ada 2 kegiatan yang sudah diimplementasikan dengan baik yaitu pada kegiatan no 4 dan no 7.
Sehingga level kapabilitasnya:

$$Proficient\_level = \frac{Number\_activities\ have\ been\ done}{number\_of\_acivities}\ x100\%$$

$$Proficient\_level = \frac{2}{7}\ x\ 100\% = 28\%$$

TABEL 4.

HASIL KUISIONER APO13

	CAPABILITY LEVEL 2	**Y/T**
1	Tentukan ruang lingkup dan batasan sistem manajemen keamanan informasi (ISMS) dalam kaitannya dengan karakteristik perusahaan, organisasi, lokasi, aset, dan teknologinya. Sertakan detail, dan justifikasi untuk, setiap pengecualian dari cakupan	T
2	Tetapkan ISMS sesuai dengan kebijakan perusahaan dan konteks di mana perusahaan beroperasi	T
3	Selaraskan ISMS dengan pendekatan perusahaan secara keseluruhan untuk pengelolaan keamanan.	T
4	Dapatkan otorisasi manajemen untuk menerapkan dan mengoperasikan atau mengubah SMKI.	Y
5	Dapatkan otorisasi manajemen untuk menerapkan dan mengoperasikan atau mengubah SMKI.	T
6	Menetapkan dan mengomunikasikan peran dan tanggung jawab manajemen keamanan informasi	T
7	Komunikasikan pendekatan ISMS.	Y

Karena pada proses APO13 yang berada di capability level 2, hanya mendapatkan nilai 28% yang berarti ada di level *partially*, maka proses pengukuran *capability level* di level 3 tidak bisa dilakukan. Perlu dilakukan perbaikan di level 2 sebelum dapat diukur di level diatasnya.

Rekomendasi untuk perbaikan di proses ini supaya bisa mencapai *capability level 3* adalah:

1. Tentukan ruang lingkup dan batasan sistem manajemen keamanan informasi (ISMS) dalam kaitannya dengan karakteristik organisasi yaitu sebagai universitas yang menyelenggarakan kegiaatan akademik, lokasinya, aset yang dianggap penting, dan teknologi yang digunakan saat ini. Sertakan juga detail, dan justifikasinya kalau ada, pengecualian dari cakupan.
2. Tetapkan ISMS sesuai dengan kebijakan universitas terkait keamanan informasi dalam dunia pendidikan
3. Selaraskan ISMS dengan pendekatan universitas secara keseluruhan dalam pengelolaan keamanan
4. Mempersiapkan dan memelihara pernyataan implementasi yang menjelaskan ruang lingkup SMKI
5. Menetapkan dan mengomunikasikan peran dan tanggung jawab manajemen keamanan informasi

3.3.3 Proses DSS05:

DSS05 Melindungi informasi perusahaan untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. Tetapkan dan pertahankan peran keamanan informasi dan hak akses. Lakukan pemantauan keamanan.

Evaluasi kegiatan ini berdasarkan data yang diambil dari hasil kuisioner terhadap pimpinan dan personil di bagian TI yaitu terkait implementasi SMKI pada saat ini.

Hasil kuisioner pada proses ini diperoleh data dari 26 kegiatan yang berada di *capability level 2*, ada 18 kegiatan yang sudah diimplementasikan dan masih ada 8 kegiatan yang belum dilakukan, sehingga *capability level* pada saat ini ada di tingkat:

$$Proficient\_level = \frac{18}{26}\ x\ 100\% = 69\%$$

Proses DSS05 dari perhitungan diatas saat ini sebesar 69% yang berarti masih berada di level *largerly* (sebagian besar terpenuhi). Karena angka yang tercapai belum memenuhi kriteria Fully maka pengukuran pada *capability level* 3 tidak bisa dilakukan sebelum ada perbaikan di level 2

Rekomendasi yang kami usulkan untuk peningkatan perbaikan pengelolaan layanan keamanan informasi supaya naik ke level 3 adalah sebagai berikut:
Semua perangkat keras bekas yang masuk kategori *endpoint device* seperti server, komputer, laptop, harus dibuang dengan aman karena ada potensi data data penting yang tersimpan di perangkat tersebut bisa dipulihkan lagi oleh pihak yang tidak berhak

Volume 9 Nomor 1, 2023, 34-41
ISSN: 2460-1799 P-ISSN: 1432-602743

1. Catat dan monitor semua tamu, termasuk vendor, kontraktor yang masuk ke area aset IT seperti server, ruang kerja dan ruang *network*
2. Semua tamu yang masuk ke area IT harus didampingi
3. Semua personil IT harus menunjukkan ID card yang sah setiap saat
4. Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan, dan pembuangan dokumen sensitif dan perangkat output(printer, hardisk eksternal) ke dalam, di dalam, dan di luar perusahaan.
5. Gunakan secara kontinu tool untuk deteksi kerentanan (*vulnerability)* untuk mengidentifikasi kerentanan keamanan informasi
6. Tetapkan dan sosialisasikan potensi risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.
7. Pastikan tiket insiden terkait keamanan dibuat tepat waktu saat pemantauan identifikasi potensi insiden. Contohnya ketika melihat ada potensi koneksi dari server ke database sering tidak stabil maka segera mengeluarkan tiket

TABEL 5
HASIL KUISIONER DSS05

	CAPABILITY LEVEL 2	**Y/T**
1	Instal dan aktifkan alat perlindungan perangkat lunak berbahaya di semua fasilitas pemrosesan, dengan file definisi perangkat lunak berbahaya yang diperbarui sesuai kebutuhan (secara otomatis atau semi otomatis)	Y
2	Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (spyware, email phishing).	Y
3	Izinkan hanya perangkat resmi yang memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasikan perangkat ini untuk memaksa entri kata sandi	Y
4	Terapkan mekanisme penyaringan jaringan, seperti firewall dan perangkat lunak pendeteksi intrusi. Terapkan kebijakan yang sesuai untuk mengontrol lalu lintas masuk dan keluar.	Y
5	Terapkan protokol keamanan yang disetujui untuk konektivitas jaringan.	Y
6	Konfigurasi peralatan jaringan dengan cara aman	T
7	Konfigurasi sistem operasi dengan cara yang aman	Y
8	Terapkan mekanisme penguncian perangkat.	Y
9	Kelola akses dan kontrol jarak jauh (mis., perangkat seluler, teleworking).	Y
10	Kelola konfigurasi jaringan dengan cara yang aman.	Y
11	Terapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.	Y
12	Melindungi integritas sistem.	Y
13	Berikan perlindungan fisik perangkat titik akhir.	Y
14	Buang perangkat endpoint dengan aman.	T
15	Kelola akses berbahaya melalui email dan browser web. Misalnya, blokir situs web tertentu dan nonaktifkan tautan klik-tayang untuk ponsel cerdas	Y
16	Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan. Menyelaraskan pengelolaan identitas dan hak akses ke peran dan tanggung jawab yang ditentukan, berdasarkan prinsip-prinsip yang paling tidak diistimewakan, perlu dimiliki dan perlu diketahui	Y
17	Catat dan pantau semua titik masuk ke situs TI. Daftarkan semua pengunjung, termasuk kontraktor dan vendor, ke situs	T
18	Pastikan semua personel menampilkan identifikasi yang disetujui dengan benar setiap saat	T
19	Mengharuskan pengunjung untuk diantar setiap saat saat berada di tempat.	T
20	Tetapkan prosedur untuk mengatur penerimaan, penggunaan, penghapusan, dan pembuangan dokumen sensitif dan perangkat keluaran ke dalam, di dalam, dan di luar perusahaan.	Y
21	Pastikan kontrol kriptografi tersedia untuk melindungi informasi sensitif yang disimpan secara elektronik.	T
22	Terus gunakan portofolio teknologi, layanan, dan aset yang didukung (mis., pemindai kerentanan, fuzzers dan sniffer, penganalisa protokol) untuk mengidentifikasi kerentanan keamanan informasi	Y
23	Tetapkan dan komunikasikan skenario risiko, sehingga dapat dengan mudah dikenali, dan kemungkinan serta dampaknya dipahami.	T
24	Tinjau log peristiwa secara teratur untuk potensi insiden.	Y
25	Pastikan tiket insiden terkait keamanan dibuat tepat waktu saat pemantauan mengidentifikasi potensi insiden.	T

IV. KESIMPULAN

Berdasarkan evaluasi pelaksanaan pengendalian keamanan informasi di Universitas XYZ untuk persyaratan domain APO12 yaitu mengelola resiko diperoleh hasil 20% pada evaluasi tingkat kapabilitasnya tingkat 2. Perolehan angka 20% ini menunjukkan implementasi pengendalian resiko masih dilaksanakan sebagian saja (partly).

Sedangkan pada domain APO13 yaitu pengendalian keamanan informasi diperoleh hasil sebesar 28% pada evaluasi tingkat kapabilitasnya di tingkat 2 yang artinya pelaksanaan SMKI masih jauh dari persyaratan yang distandarkan oleh COBIT 2019 karena secara pelaksanaan masih sebagian kecil (partly). Universitas XYZ harus mendefinisikan SMKI yang standar, dijaga dan dimonitor pelaksanaannya. Selain itu juga harus ada bagian yang khusus menangani kegiatan pengendalian keamanan informasi. Pelaksanaan keamanan informasi untuk domain DSS05 yaitu layanan keamanan informasi hasil perhitungan tercapai sebesar 69% pada tingkat kapabilitas 2 dan pelaksanaannya sudah sebagian besar (largely) persyaratan telah dilakukan. Pada ketiga domain tersebut, pencapaian tingkat kapabilitas masih di tingkat 2 atau tingkat yang paling rendah dan tingkat kematangannya juga masih di posisi partly dan largely belum ada yang masuk ke kategori fully. Perlu kerja keras untuk

dapat memenuhi posisi fully pada semua persyaratan COBIT 2019 di tingkat kapabilitas 2.

Ada 19 rekomendasi perbaikan praktis yang perlu segera dilakukan untuk melengkapi persyaratan di tingkat 2 supaya bisa naik ke tingkat 3

UCAPAN TERIMA KASIH

Terima kasih kepada Universitas XYZ, khususnya kepada karyawan di Direkorat TIK Universitas XYZ yang telah memberikan dukungan bagi kami untuk melakukan penelitian ini, dan terima kasih kepada Direktorat Akademik yang telah bersedia meluangkan waktu untuk membantu penelitian ini, dan terima kasih untuk semua tim yang telah bekerja keras untuk mengidentifikasi masalah di Direktorat TIK.

REFERENSI

[1] J. v. N. Rayne Reid, "From Information Security to Cyber Security Cultures Organizations to Societies," in *ISSA*, Johannesburg, South Africa , 2014.

[2] &. W. G. Wang, "Measuring information security and cybersecurity on private cloud computing," *Journal of Theoretical and Applied Information Technology*, vol. 1, no. 96, pp. 156-168, 2019.

[3] BSI, nformation Security Management – Part 2: Specification for Information SecurityManagement System, London: British Standards Institute, 2002.

[4] T. D. IT, Buku manual penggunaan Sistem Akademik, Yogyakarta, 2017.

[5] D. T. Informasi, Panduan Layanan Teknologi Informasi, Yogyakarta, 2016.

[6] N. R. I. S. &. I. Rochmania, "Tren Penggunaan Framework COBIT, ITIL, dan ISO 27001 pada Rentang Tahun 2014- 2018 di Indonesia," *EDUMATIC Jurnal Pendidikan Informatika*, vol. 4, no. 2, pp. 10-19, 2020.

[7] ISACA, COBIT 2019 Framework: Introduction and Methodology, USA: ISACA, 2018.

[8] S. Lilis Griffith Toyner, "INFORMATION SYSTEM SECURITY EVALUATION USING COBIT 5 FRAMEWORK," *Journal of Information System Management (JOISM)*, pp. 147-157, 2023.

[9] W. S. A. A. A. I. J. M. E. Muhammad Yasin, "Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," *IEEE*, 2021.

[10] C. T. P. V. S. Kasma, S. Sutikno and K. Surendro, "Design of e-Government Security Governance System Using COBIT 2019 : (Trial Implementation in Badan XYZ)," in *International Conference on ICT For Smart Society (ICISS)*, 2019.

[11] H. Yubo, "IT Risk Control for Internet Finance Based on COBIT," in *2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE)*, 2020.

[12] S. S. Setiyowati, Setiyowati and Sri Siswanti. Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1., SATIN - Sains dan Teknologi Informasi, 2021.

[13] Y. N. H. S. Erika Nachrowi, "Evaluationof Governance and Management of Information Technology Services Using Cobit 2019 and ITIL4," *RESTI JOURNAL*, vol. 4, no. 4, pp. 764-774, 2020.

[14] F. H. S. Diah Sulistyowati, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," *INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION*, vol. 4, no. 4, pp. 225-230, 2020.

[15] M. Dr. Nursapia Harahap, Penelitian Kuantitatif, Medan: Wal ashri Publishing, 2020.

[16] ISACA, Introduction and Methodology, Schaumburg, IL USA: ISACA, 2018.

[17] D. Steuperaert, "COBIT 2019: A SIGNIFICANT UPDATE," *EDPACS*, vol. 59, no. 01, pp. 1-5, 2019.

[18] ISACA, Enabling Process COBIT 5, IL USA: ISACA, 2012.

[19] ISACA, COBIT 2019 Design and Objective, IL USA: ISACA, 2018.