Pengembangan Pengelolaan Keamanan dan Program Keamanan Siber Menggunakan Framework COBIT 2019

Stephanus Widjaja[1,*]
[1] Teknik Informatika, STMIK AKI, Pati, Indonesia
Email: [1,*]stephanuswidjaja@gmail.com

Abstrak—Perkembangan perguruan tinggi yang semakin pesat mengakibatkan perkembangan teknologi informasi yang digunakannya pun semakin pesat. Pengembangan teknologi informasi pada perguruan tinggi bertujuan untuk meningkatkan kualitas layanan pendidikannya. Dengan perkembangan teknologi informasi yang semakin pesat maka aliran data dan informasinya pun akan semakin besar. Hal inilah yang memerlukan perhatian lebih salah satunya di bidang keamanan sistem. Universitas AKI sebagai salah satu perguruan tinggi swasta yang berbasis teknologi pasti ingin membangun infrastruktur teknologi informasinya dengan baik. Salah satu fokus yang saat ini ditekankan oleh pihak manajemen ialah bagaimana membangun infrastruktur teknologi informasi yang aman. Penelitian ini dilakukan untuk menjawab kebutuhan manajemen akan infrastruktur teknologi informasi yang aman. Penelitian ini menggunakan *framework* COBIT 2019 dan *guidelines* IT Audit sebagai panduan evaluasi. Penelitian ini berfokus pada domain *Align, Plan and Organize* (APO) khususnya proses *Managed Security*. Metode penelitian yang digunakan meliputi pemilihan area fokus pengelolaan teknologi informasi, pembuatan instrumen evaluasi pengelolaan teknologi informasi, pelaksanaan evaluasi pengelolaan teknologi informasi, evaluasi hasil pengelolaan teknologi informasi, analisa kesenjangan (*gap*) pengelolaan teknologi informasi dan perumusan strategi perbaikan pengelolaan teknologi informasi. Hasil dari penelitian ini adalah tingkat kemampuan setiap aktivitas dari praktik manajemen pengelolaan keamanan sistem yang berada pada level 3 (*defined*), nilai kematangan dan tingkat kematangan pengelolaan keamanan sistem yang berada pada level 3 (*defined*) untuk semua komponen sistem tata kelola, kesenjangan (*gap*) antara komponen dalam pengelolaan keamanan sistem dan strategi perbaikan pengelolaan keamanan sistem.

Kata Kunci: evaluasi, pengelolaan keamanan, program keamanan siber, COBIT 2019

Abstract—The increasingly rapid development of higher education has resulted in the development of the information technology they use becoming increasingly rapid. The development of information technology in higher education aims to improve the quality of educational services. With the increasingly rapid development of information technology, data and information flow will also increase. This requires more attention, one of which is in the field of system security. AKI University, a technology-based private university, wants to build its information technology infrastructure well. One of the focuses currently emphasized by management is how to build a secure information technology infrastructure. This research was conducted to answer management's need for secure information technology infrastructure. This research uses the COBIT 2019 framework and IT Audit guidelines as evaluation guides. This research focuses on the *Align, Plan, and Organize* (APO) domain, especially the *Managed Security* process. The research methods used include selecting a focus area for information technology management, creating information technology management evaluation instruments, implementing information technology management evaluations, evaluating information technology management results, gap analysis in information technology management, and formulating strategies for improving information technology management. The results of this research are the level of capability for each activity of system security management practices which is at level 3 (defined), the maturity value and maturity level of system security management which are at level 3 (defined) for all components of the governance system, gaps between components in system security management and strategies for improving system security management.

Keywords: evaluation, security management, cybersecurity program, COBIT 2019

1. PENDAHULUAN

Perguruan tinggi baik swasta maupun negeri saat ini sedang mengalami perkembangan dan evolusi yang sangat pesat[1]. Evolusi perguruan tinggi terjadi diberbagai aspek atau bidang di dalamnya. Aspek yang paling besar mengalami evolusi iyalah aspek perkuliahan. Didorong pandemi yang terjadi di awal tahun 2020 membuat seluruh perguruan tinggi sadar sekaligus harus bekerja sangat keras untuk menjamin proses perkuliahannya tetap berjalan lancar dan berkualitas[1]. Penggunaan teknologi informasi (TI) menjadi salah satu jalan untuk mengatasi masalah yang ada. Masing-masing perguruan tinggi mengembangkan teknologi informasinya untuk memenuhi kebutuhannya, hal ini juga terjadi pada Universitas AKI (UNAKI). UNAKI secara teratur mengembangkan teknologi informasinya melalui unit pelaksana teknis teknologi informasi dan komunikasi (UPT TIK). Salah satu fokus pihak manajemen pada pengembangan teknologi informasi yaitu permasalahan keamanan sistem. Keamanan sistem menjadi fokus utama pihak manajemen dikarenakan banyaknya data dan informasi yang beredar di dalam proses bisnis UNAKI memerlukan pengamanan sesuai tingkatannya masing-masing. Agar dapat mengembangkan teknologi informasi yang memenuhi aspek keamanan sistem kita perlu terlebih dahulu mengetahui bagaimana pengelolaan teknologi informasi yang berjalan saat ini khususnya proses pengelolaan keamanan sistem.

Selain itu penerapan dan pengelolaan teknologi informasi memerlukan evaluasi secara berkala untuk mengetahui kebermanfaatannya. Evaluasi perlu dilakukan untuk setiap proses yang ada agar kita dapat mengetahui secara detail kekurangan yang ada. Dalam melakukan evaluasi penerapan dan pengelolaan teknologi informasi diperlukan sebuah *framework* sebagai acuan penilaian. Ada banyak *framework* tata kelola TI yang dapat digunakan, tetapi pemilihan *framework* perlu disesuaikan dengan tujuan evaluasi dan proses yang akan dievaluasi. Dalam penelitian ini menggunakan *framework* COBIT 2019 dengan fokus pada domain *Align, Plan and Organize (APO)* proses *Managed Security*[2][3][4]. Dasar pemilihan domain dan proses tersebut adalah kebutuhan manajemen terhadap keamanan sistem pada pengembangan infrastruktur teknologi informasinya. Untuk evaluasi yang bersifat teknis, penelitian ini menggunakan panduan audit teknis *IT Auditing Using Controls To Protect Information Assets*[5]. Penelitian ini berfokus pada proses pengelolaan keamanan teknologi informasi dan program keamanan siber. Penelitian ini bertujuan untuk:

1. Mengetahui efektivitas dan efisiensi penerapan dan pengelolaan teknologi informasi di UNAKI khususnya pada proses pengelolaan keamanan dan program keamanan siber.
2. Mengetahui tingkat kematangan (*maturity level*) proses pengelolaan keamanan.
3. Merumuskan strategi perbaikan untuk proses pengelolaan keamanan.

Framework COBIT 2019 digunakan sebagai kerangka kerja acuan untuk mengevaluasi Pusat Sistem Informasi (PSI) disebuah universitas di kota Kudus. Domain dan proses yang dievaluasi dalam penelitian ini meliputi EDM 04 optimalisasi sumber daya, APO 01 pengelolaan *framework* manajemen IT, APO 02 pengelolaan strategi, APO 07 pengelolaan sumber daya manusia, APO 11 pengelolaan kualitas, APO 12 pengelolaan resiko, APO 14 pengelolaan data, DSS 01 pengelolaan operasi, DSS 05 pengelolaan layanan keamanan, MEA 01 pengelolaan pemantauan kinerja dan kesesuaian, dan MEA 02 pengelolaan sistem kendali internal. Tahapan penelitian ini adalah identifikasi dan perumusan masalah, pengumpulan data, pemetaan domain COBIT 2019, pengukuran *maturity level*, analisis *gap* dan rekomendasi. Tingkat kematangan pada seluruh domain dan proses yang dievaluasi berada pada tingkat 3[6].

Implementasi *framework* COBIT 2019 pada evaluasi penggunaan teknologi informasi juga dilakukan oleh salah satu perguruan tinggi di Kalimantan Barat. Metode yang digunakan adalah metode *Action Research*. Metode pengumpulan data menggunakan studi literatur, observasi (pengamatan di objek), wawancara dan kuesioner. Proses yang dievaluasi adalah proses pengelolaan operasi (DSS 01) dengan praktek manajemen yang dievaluasi meliputi DSS 01.01 sampai DSS 01.07. Hasil dari penelitian ini yaitu tingkat kematangan, tingkat kesenjangan dan rekomendasi[7].

COBIT 2019 juga diimplementasikan untuk evaluasi pengelolaan TI pada perusahaan XYZ. Metode penelitiannya terdiri dari tiga tahap yaitu tahap perencanaan penelitian, tahap pengumpulan data dan tahap analisa data dan hasil. Tahap perencanaan penelitian meliputi identifikasi masalah, observasi, studi pustaka, penentuan domain, penentuan narasumber dan penentuan target level kapabilitas. Tahap pengumpulan data meliputi pembuatan pertanyaan dan melakukan wawancara. Tahap analisa data dan hasil meliputi perhitungan level kapabilitas, analisis kesenjangan dan pemberian rekomendasi. Penelitian ini menggunakan model deskriptif kualitatif. Hasil dari penelitian ini adalah terdapat lima proses prioritas teratas yaitu DSS 05 dengan nilai 50, DSS 03 dengan nilai 45, DSS 02 dengan nilai 30, BAI 09 dengan nilai 35 dan MEA 03 dengan nilai 30[8].

Penelitian mengenai keamanan informasi menggunakan framework COBIT 5 sebagai acuannya juga dilakukan pada kantor wilayah Kementerian Agama provinsi Lampung. Penelitian ini menggunakan metode pengumpulan data wawancara, dokumentasi, studi pustaka, kuesioner dan pengamatan lapangan. Hasil dari penelitian ini adalah nilai rata-rata kematangannya 3,3 untuk domain optimalisasi resiko (EDM 03), pengelolaan kerangka kerja manajemen TI (APO 01), pengelolaan sumber daya manusia (APO 07), pengelolaan resiko (APO 12), pengelolaan perubahan TI (BAI 06), pengelolaan operasi (DSS 01), pengelolaan permintaan layanan dan kejadian (DSS 02), pengelolaan permasalahan (DSS 03), pengelolaan layanan keamanan (DSS 05), pengelolaan pengawasan kinerja dan kepatuhan (MEA 01) dan pengelolaan sistem dan pengendalian internal (MEA 02). Pengelolaan yang sudah berjalan telah melaksanakan prosedur yang terstandarisasi tetapi belum mencapai tingkatan *optimized*[9].

2. METODE PENELITIAN

2.1 Pemilihan area fokus pengelolaan teknologi informasi

Pemilihan area fokus adalah pemilihan proses apa yang menjadi fokus pihak pimpinan untuk dikembangkan. Proses pemilihan area fokus dilakukan bersama dengan tim UPT TIK, wakil rektor bidang TI dan *stakeholder* terkait. Pemilihan area fokus juga memperhatikan kebutuhan kampus dan isu terkini yang ada.

2.2 Pembuatan instrument evaluasi pengelolaan teknologi informasi

1. Wawancara

Wawancara adalah teknik pengumpulan data dengan memberikan sejumlah pertanyaan langsung kepada narasumber yang berkompeten[10][11]. Pembuatan form interview berdasarkan aktivitas pada setiap praktik manajemen yang ada. Dalam penelitian ini terdapat 3 praktek manajemen dengan total pertanyaan 19 pertanyaan. Pemilihan narasumber berdasarkan kompetensinya[7][12]. Narasumber yang pilih untuk wawancara ialah kepala UPT TIK dan administrator sistem. Hasil interview memetakan level kemampuan untuk setiap aktivitas pada praktik manajemen pengelolaan keamanan.

2. Survey Kuesioner
   Survey kuesioner adalah teknik pengumpulan data dengan memberikan sejumlah pertanyaan dalam bentuk tertulis yang ditujukan kepada narasumber yang berkompeten[13]. Survey kuesioner dilakukan terhadap 5 narasumber yang berkompeten dalam pengelolaan keamanan yaitu wakil rektor 3 bidang teknologi informasi, kepala UPT TIK, administrator sistem dan 2 staf pengelola sistem. Hasil survey kuesioner menggambarkan nilai kematangan dan tingkat kematangan proses pengelolaan keamanan. Form kuesioner disusun berdasarkan 7 komponen sistem tata kelola yaitu
   1. Proses
   2. Struktur organisasi
   3. Prinsip, kebijakan dan kerangka kerja
   4. Informasi
   5. Budaya, etika dan perilaku
   6. Orang, keterampilan dan kompetensi
   7. Layanan, infrastruktur dan aplikasi
3. Test Sistem
   Test sistem dilakukan dengan pengujian teknis pada objek yang diteliti. Test sistem menggunakan panduan audit teknologi informasi pada bagian audit program keamanan siber[5]. Hasil test sistem menggambarkan secara teknis pengelolaan keamanan.
4. Studi Dokumen
   Studi dokumen dilakukan dengan mengumpulkan dokumen-dokumen terkait seperti standar operasional, form, dan catatan (log) yang terkait[14][15]. Hasil studi dokumen menggambarkan kesiapan dan kelengkapan dokumen terkait pengelolaan keamanan.

2.3 Evaluasi pengelolaan teknologi informasi

Evaluasi pengelolaan TI berdasarkan data yang diperoleh dari interview, kuesioner, test sistem dan studi dokumen. Evaluasi dikelompokan berdasarkan 7 komponen sistem tata kelola[16].

2.4 Analisa kesenjangan (*gap*) pengelolaan teknologi informasi

Analisa kesenjangan (*gap*) didapat dari selisih nilai kematangan saat ini dengan nilai kematangan yang dituju. Selisih ini yang digunakan untuk menentukan skala prioritas perbaikan[17][18].

2.5 Perumusan strategi perbaikan pengelolaan teknologi informasi

Perumusan strategi perbaikan pengelolaan TI disusun secara bertahap dari tingkat kematangan saat ini hingga tingkat kematangan yang dituju. Perumusan strategi perbaikan pengelolaan TI dikelompokan berdasarkan 7 komponen sistem tata kelola. Strategi perbaikan pengelolaan TI digunakan untuk pengembangan pengelolaan keamanan dan program keamanan siber.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Interview

Pelaksanaan interview dilakukan kepada kepala UPT TIK sebagai sebagai penanggung jawab operasional UPT TIK. Pertanyaan yang diajukan berdasarkan aktivitas proses pengelolaan keamanan (APO 13). Level kemampuan untuk setiap aktivitas pada praktek manajemen berdasarkan hasil interview disajikan melalui tabel 1:

Tabel 1. Level Kemampuan Aktivitas Pengelolaan Keamanan

Proses	Aktivitas	Level Kemampuan
APO 13.01 Membangun dan memelihara sistem manajemen keamanan informasi (ISMS)		
APO 13.01.01	Menentukan ruang lingkup dan Batasan sistem manajemen keamanan informasi (ISMS).	3
APO 13.01.02	Mendefinisikan ISMS, menyesuaikan dengan kebijakan kampus dan konteks dimana kampus beroperasi.	3

APO 13.01.03	Menyelaraskan ISMS dengan pendekatan yang dimiliki kampus (manajemen keamanan).	3
APO 13.01.04	Mendapatkan otorisasi manajemen untuk menerapkan, mengoperasikan dan mengubah ISMS.	3
APO 13.01.05	Mempersiapkan dan memelihara persyaratan penerapan yang menggambarkan ruang lingkup ISMS.	3
APO 13.01.06	Menentukan dan mengkomunikasikan peran dan tanggung jawab manajemen keamanan informasi.	3
APO 13.01.07	Mengkomunikasikan pendekatan ISMS.	3
APO 13.02 Mendefinisikan dan mengelola rencana manajemen resiko keamanan informasi dan privasi.		
APO 13.02.01	Merumuskan dan memelihara rencana penanganan resiko keamanan informasi.	3
APO 13.02.02	Mempertahankan inventaris komponen solusi untuk mengelola resiko keamanan.	3
APO 13.02.03	Mengembangkan proposal untuk menerapkan rencana penanganan resiko keamanan informasi.	2
APO 13.02.04	Proses pemberian masukan untuk desain dan pengembangan praktik manajemen dan solusi yang dipilih dari rencana penanganan resiko keamanan informasi.	3
APO 13.02.05	Pelaksanaan pelatihan keamanan informasi, privasi dan program kesadaran (awareness programs).	3
APO 13.02.06	Mengintegrasikan perencanaan, desain, penerapan, pemantauan prosedur keamanan informasi dan privasi serta pengendalian lainnya.	3
APO 13.02.07	Mengukur efektivitas praktik pengelolaan yang dipilih.	2
APO 13.03 Memantau dan meninjau sistem manajemen keamanan informasi (ISMS).		
APO 13.03.01	Peninjauan efektivitas ISMS secara rutin.	2
APO 13.03.02	Audit ISMS dilakukan sesuai jadwal yang direncanakan.	3
APO 13.03.03	Manajemen secara teratur melakukan peninjauan ruang lingkup ISMS serta melakukan perbaikan yang diperlukan.	3
APO 13.03.04	Pendokumentasian seluruh tindakan dan peristiwa yang berdampak pada kinerja ISMS.	2
APO 13.03.05	Proses pemberian masukan rencana pemeliharaan keamanan.	3

Dari tabel level kemampuan aktivitas pengelolaan keamanan terlihat level kemampuan secara umum berada dilevel 3 (*defined*) hal ini menggambarkan bahwa panduan atau standar yang dimiliki kampus telah mampu memberikan panduan pada seluruh aktivitas pengelolaan keamanan hingga mencapai tujuan yang diharapkan. Akan tetapi masih perlu menjadi perhatian adalah aktivitas yang memiliki level kemampuan 2 (*performed*) yaitu

1. APO 13.02.03 proses pengembangan proposal untuk menerapkan rencana penanganan resiko keamanan informasi. Dikarenakan struktur organisasi yang sederhana sehingga memungkinkan komunikasi yang intens antara unit dengan pimpinan. Hal ini menjadikan setiap permasalahan yang ada dapat langsung dikomunikasikan sehingga dapat segera terselesaikan.
2. APO 13.02.07 proses mengukur efektivitas praktik pengelolaan yang dipilih.
3. APO 13.03.01 proses peninjauan efektivitas ISMS secara rutin.
4. APO 13.03.04 proses pendokumentasian seluruh tindakan dan peristiwa yang berdampak pada kinerja ISMS. Proses ini sebenarnya sudah dilakukan dengan baik, terstruktur dan dapat diakses oleh pihak yang berwenang tetapi pendokumentasiannya belum tersistem secara khusus (belum ada sistem yang secara khusus).

3.2 Hasil Survey Kuesioner

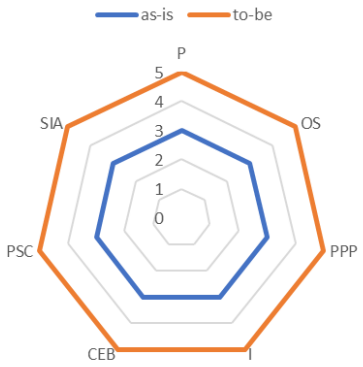
Survey kuesioner dilakukan dengan mengajukan pertanyaan tertulis kepada narasumber yang berkompeten untuk menjawab. Kuesioner terdiri dari 14 pertanyaan yang terbagi ke dalam 7 kelompok berdasarkan komponen sistem tata kelola. Masing-masing kelompok terdiri dari 2 pertanyaan yang mewakili kondisi saat ini (*as-is*) dan

kondisi yang diharapkan (*to-be*). Hasil survey kuesioner tingkat kematangan proses pengelolaan keamanan disajikan pada tabel 2 berikut:

Tabel 2. Tingkat Kematangan Proses Pengelolaan Keamanan

Attribute	***as-is***	***to-be***
Processes (P)	3	5
Organizational Structures (OS)	3	5
Principles, Policies and Procedures (PPP)	3	5
Information (I)	3	5
Culture, Ethics, and Behavior (CEB)	3	5
People, Skills and Competencies (PSC)	3	5
Service, Infrastructure, and Applications (SIA)	3	5

Dari hasil survey kuesioner di atas tergambar tingkat kematangan saat ini (*as-is*) untuk proses pengelolaan keamanan berada pada tingkat 3 (*defined*). Tingkat kematangan yang dituju (*to-be*) untuk proses pengelolaan keamanan berada pada tingkat 5 (*defined, measured and continuous improvement*). Tingkat kematangan pengelolaan keamanan secara keseluruhan tergambar juga dalam diagram radar berikut:



Gambar 1. Diagram Radar Tingkat Kematangan Proses Pengelolaan Keamanan

3.3 Hasil Test Sistem

Test sistem dilakukan pada program keamanan siber yang merupakan bagian dari proses pengelolaan keamanan. Test sistem berdasarkan master checklist yang terdapat pada panduan audit teknologi informasi[5]. Form test sistem terdiri dari 15 pertanyaan, yaitu:

1. Implementasi program keamanan siber di lingkungan kampus.
2. Penilaian manajemen resiko informasi, identifikasi dan pengelolaan resiko keamanan siber.
3. Penilaian cakupan program keamanan siber dan keterkaitannya dengan fungsi IT dalam lingkungan kampus.
4. Memastikan kebijakan keamanan TI yang ada memberikan persyaratan yang memadai untuk keamanan TI serta kebijakan untuk mengkomunikasikan dan memantaunya.
5. Memastikan fungsi kesadaran (awareness) dan komunikasi dalam tim TI serta metode pelatihan tim dan karyawan tentang resiko dan masalah keamanan TI.
6. Memastikan manajemen kerentanan berfungsi dengan baik pada lingkungan kampus serta memastikan seluruh tim TI menyadari ancaman dan kerentanan yang timbul serta cara mengidentifikasinya.
7. Evaluasi fungsi pemantauan keamanan oleh tim TI, pengumpulan catatan (*log*) serta pemrosesan peringatan dan kemampuan deteksi.

8. Evaluasi fungsi respon insiden dari tim TI.
9. Evaluasi tim TI dalam menjalankan fungsi lainnya.
10. Evaluasi kebijakan dan proses dalam penetapan kepemilikan data, klasifikasi data, melindungi data sesuai klasifikasinya dan penentuan siklus hidup data.
11. Proses TI kampus menangani kebijakan keamanan dan resiko keamanan.
12. Memastikan personel TI memiliki keterampilan dan pengetahuan yang diperlukan.
13. Memastikan matrik yang dikumpulkan sesuai dengan tujuan program keamanan kampus serta pelaporannya.
14. Penggunaan penyedia layanan pengelolaan keamanan dalam tim TI.
15. Organisasi dalam hal ini kampus memastikan efektivitas pengendalian keamanan TI.

Hasil dari test sistem program keamanan siber disajikan pada tabel 3 berikut:

Tabel 3. Hasil Test Sistem

No	Kegiatan	Hasil
1	Bagaimana implementasi program keamanan siber di lingkungan kampus?	Program keamanan sudah dijalankan dengan baik. Dengan menjalankan program keamanan yang sudah direncanakan sebelumnya.
2	Bagaimana penilaian manajemen resiko informasi, identifikasi dan pengelolaan resiko keamanan siber?	Sudah dilakukan penilaian manajemen resiko dengan melibatkan seluruh pemangku kepentingan. Penilaian meliputi manajemen resiko informasi, identifikasi dan pengelolaan resiko keamanan.
3	Bagaimana menilai cakupan program keamanan siber dan keterkaitannya dengan fungsi IT dalam lingkungan kampus?	Sudah jelas alur penilaian cakupan program keamanannya.
4	Bagaimana memastikan kebijakan keamanan IT yang ada memberikan persyaratan yang memadai untuk keamanan IT? Bagaimana kebijakan untuk mengkomunikasikannya dan memantaunya?	1. Kebijakan keamanan IT sudah memberikan persyaratan yang memadai untuk keamanan IT. 2. Sudah disosialisasikan dan dilakukan monitoring.
5	Bagaimana memastikan fungsi kesadaran (awareness) dan komunikasi dalam tim IT? Bagaimana metode pelatihan tim dan karyawan tentang resiko dan masalah keamanan IT?	1. Kesadaran dan komunikasi tim IT sudah baik. 2. Metode pelatihan sudah ada.
6	Bagaimana memastikan manajemen kerentanan berfungsi dengan baik pada lingkungan kampus? Bagaimana memastikan seluruh tim IT menyadari ancaman dan kerentanan yang timbul serta bagaimana mengidentifikasinya?	1. Sudah terdapat analisa dan evaluasi manajemen kerentanan. 2. Sudah dilakukan sosialisasi dan koordinasi seluruh tim IT terkait ancaman dan kerentanan.
7	Bagaimana evaluasi fungsi pemantauan keamanan oleh tim IT, pengumpulan log serta pemrosesan peringatan dan kemampuan deteksi?	Fungsi pemantauan keamanan yang dilakukan oleh tim IT sudah dilakukan evaluasi secara internal di UPT TIK.
8	Bagaimana evaluasi terhadap fungsi respon insiden dari tim IT?	Sudah ada evaluasi fungsi respon terhadap insiden tetapi harus rutin dilakukan pengecekan agar meminimalisir terjadinya human error.
9	Bagaimana evaluasi tim IT dalam menjalankan fungsi lainnya?	Sudah dilakukan evaluasi tim IT untuk fungsi lainnya.
10	Bagaimana evaluasi kebijakan dan proses dalam penetapan kepemilikan data, klasifikasi data, melindungi data sesuai klasifikasinya dan penentuan siklus hidup data?	Sudah dilakukan evaluasi kebijakan penetapan kepemilikan data, dll.
11	Bagaimana proses IT kampus menangani kebijakan keamanan dan resiko keamanan?	Proses IT kampus sudah direncanakan dengan baik.

12	Bagaimana memastikan personel IT memiliki keterampilan dan pengetahuan yang diperlukan?	Sudah ada identifikasi keterampilan dan pengetahuan yang dibutuhkan untuk mengatasi ancaman keamanan.
13	Bagaimana memastikan matrik yang dikumpulkan sesuai dengan tujuan program keamanan kampus serta bagaimana pelaporannya?	Sudah ada matrik sederhana yang digunakan secara internal.
14	Bagaimana penggunaan penyedia layanan pengelolaan keamanan dalam tim IT?	1. Tidak menggunakan pihak ketiga memberikan keuntungan tersendiri yaitu karakteristik keamanan IT tidak diketahui oleh pihak luar. 2. Tantangannya adalah UPT TIK dituntut untuk secara aktif melakukan update dan inovasi untuk mengembangkan keamanan IT kampus.
15	Bagaimana kampus memastikan pengendalian keamanan ITnya efektif?	Pengawasan dan evaluasi internal sudah dilakukan oleh UPT TIK bersama stakeholder terkait.

3.4 Analisa Kesenjangan (gap)

Analisa kesenjangan (*gap*) digunakan untuk menentukan skala prioritas perbaikan pada proses pengelolaan keamanan. Analisa kesenjangan dilakukan dengan mencari selisih nilai kematangan saat ini (*as-is*) dengan nilai kematangan yang dituju (*to-be*) dari setiap atribut. Selisih yang paling tinggi akan mendapatkan prioritas utama untuk dapat menjalankan strategi perbaikan yang ada. Meskipun demikian apabila memungkinkan implementasi strategi perbaikan secara paralel maka implementasi akan dilaksanakan secara paralel. Hasil analisa kesenjangan (*gap*) disajikan dalam tabel 4 berikut:

Tabel 4. Hasil Analisa Kesenjangan (*gap*)

Attribute	*as-is*	*to-be*	*gap*
Processes (P)	3,2	5	1,8
Organizational Structures (OS)	3,2	5	1,8
Principles, Policies and Procedures (PPP)	3	5	2
Information (I)	3	5	2
Culture, Ethics, and Behavior (CEB)	3	5	2
People, Skills and Competencies (PSC)	3	5	2
Service, Infrastructure, and Applications (SIA)	3	5	2

Dari hasil analisa kesenjangan (*gap*) dapat dirumuskan skala prioritas perbaikan untuk proses pengelolaan keamanan seperti tampak pada tabel 5 berikut:

Tabel 5. Skala Prioritas Perbaikan Pengelolaan Keamanan

No	Urutan Prioritas Perbaikan
1	*Principles, Policies and Procedures* (PPP)
2	*Information* (I)
3	*Culture, Ethics, and Behavior* (CEB)

4	*People, Skills and Competencies* (PSC)
5	*Service, Infrastructure, and Applications* (SIA)
6	*Processes* (P)
7	*Organizational Structures* (OS)

3.5 Strategi Perbaikan

Dari tabel 2 tingkat kematangan proses pengelolaan keamanan diketahui tingkat kematangan saat ini (*as-is*) berada pada level 3 dan tingkat kematangan yang dituju (*to-be*) berada di tingkat 5. Strategi perbaikan dirancang untuk dapat memperbaiki dan mengembangkan proses pengelolaan keamanan. Strategi perbaikan dirancang untuk 2 tingkatan yaitu dari tingkat 3 menuju tingkat 4 dan dari tingkat 4 menuju tingkat 5. Perancangan strategi perbaikan mengacu pada skala prioritas yang didapatkan dari analisa kesenjangan (*gap*). Strategi perbaikan dari tingkat 3 menuju tingkat 4, yaitu:

1. *Principles, Policies, and Procedures* (PPP)
    1) Membuat pedoman pengukuran pengelolaan rencana manajemen resiko keamanan informasi dan privasi.
    2) Membuat pedoman pengukuran sistem manajemen keamanan informasi (ISMS).
    3) Melakukan sosialisasi pedoman pengukuran tersebut.
2. *Information* (I)
    1) Pengukuran aliran informasi terkait rencana manajemen resiko keamanan informasi dan privasi serta sistem manajemen keamanan informasi (ISMS).
    2) Pengukuran kecepatan dan ketepatan aliran informasi terkait pengelolaan keamanan sistem.
3. *Culture, Ethics, and Behavior* (CEB)
   Pengukuran terkait budaya, etika dan perilaku individu maupun kelompok terkait pengelolaan keamanan sistem.
4. *People, Skills, and Competencies* (PSC)
    1) Analisa kebutuhan keterampilan dan kompetensi terkait manajemen resiko keamanan informasi dan privasi serta pengelolaan sistem manajemen keamanan informasi (ISMS).
    2) Implementasi hasil analisa kebutuhan keterampilan dan kompetensi tersebut.
    3) Melakukan pengukuran hasil implementasi pelatihan keterampilan dan kompetensi tersebut.
5. *Service, Infrastructure, and Applications* (SIA)
    1) Analisa kebutuhan layanan, infrastruktur dan aplikasi terkait pengelolaan rencana manajemen resiko keamanan informasi dan privasi serta pengelolaan sistem manajemen keamanan informasi (ISMS).
    2) Melakukan pengukuran kinerja layanan, infrastruktur dan aplikasi yang diimplementasikan.
6. *Processes* (P)
    1) Analisa proses-proses terkait pengelolaan rencana manajemen resiko keamanan informasi dan privasi serta sistem manajemen keamanan informasi (ISMS).
    2) Implementasi hasil analisa proses tersebut.
7. *Organizational Structures* (OS)
   Pengukuran kinerja seluruh pihak yang terlibat dalam pengelolaan keamanan sistem.

Setelah mengimplementasikan strategi perbaikan dari tingkat 3 menuju tingkat 4 perlu dilakukan evaluasi terlebih dahulu untuk mengetahui apakah tingkat pengelolaan keamanan sudah berada di tingkat 4. Setelah mencapai tingkat 4 maka diimplementasikan strategi perbaikan dari tingkat 4 menuju tingkat 5, yaitu:

1. *Principles, Policies and Procedures* (PPP)
   Merancang rencana pengembangan pengelolaan rencana manajemen resiko keamanan informasi dan privasi serta pengelolaan sistem manajemen keamanan informasi (ISMS) berdasarkan hasil pengukuran yang telah dilakukan.
2. *Information* (I)

1) Merancang rencana pengembangan aliran informasi terkait rencana manajemen resiko keamanan informasi dan privasi serta sistem manajemen keamanan informasi (ISMS).
2) Meningkatkan kecepatan dan ketepatan pendistribusian informasi terkait rencana manajemen resiko keamanan informasi dan privasi serta sistem manajemen keamanan informasi (ISMS).

3. *Culture, Ethics, and Behavior* (CEB)
   Merancang rencana pengembangan budaya, etika dan perilaku individu maupun kelompok terkait pengelolaan keamanan sistem.
4. *People, Skills, and Competencies* (PSC)
   Merancang rencana pengembangan keterampilan dan kompetensi personel berdasarkan hasil pengukuran yang telah dilakukan.
5. *Service, Infrastructure, and Applications* (SIA)
   Merancang rencana pengembangan layanan, infrastruktur dan aplikasi pengelolaan keamanan sistem berdasarkan hasil pengukuran sebelumnya.
6. *Processes* (P)
   Merancang pengembangan proses pengelolaan keamanan sistem berdasarkan hasil pengukuran yang telah dilakukan.
7. *Organizational Structures* (OS)
   Mengembangkan strategi kerja untuk membuat kinerja pengelolaan keamanan sistem lebih efektif.

4. KESIMPULAN

Berdasarkan evaluasi dan pengembangan pada proses pengelolaan keamanan dan program keamanan siber dapat disimpulkan tingkat kematangan pengelolaan keamanan dan program keamanan siber saat ini (*as-is*) ada ditingkat 3 (*defined*) yang artinya seluruh aktivitas pada proses pengelolaan tersebut sudah terdefinisi dan didokumentasikan dengan baik. Tingkat kematangan pengelolaan keamanan dan program keamanan siber yang ingin dicapai (*to-be*) ada ditingkat 5 (defined, measured and continuous improvement) yang artinya seluruh aktivitas pada proses pengelolaan tersebut sudah terdefinisi dan didokumentasikan dengan baik. Dilakukan pengukuran secara rutin dan terjadwal, apabila ditemukan kekurangan atau kelemahan dapat segera diperbaiki.

Pada aktivitas praktik manajemen APO 13.02.03 mengembangkan proposal untuk menerapkan rencana penanganan resiko keamanan informasi level kemampuannya berada pada level 2. Hal ini perlu ditingkatkan dengan melengkapi prosesnya. Untuk setiap rencana penanganan resiko perlu digambarkan secara rinci kedalam proposal meskipun waktu penanganan tetap menjadi perhatian. Artinya pengembangan proposal tidak boleh menghambat penanganan resiko keamanan informasi. Pada aktivitas praktik manajemen APO 13.02.07 mengukur efektivitas praktik pengelolaan yang dipilih level kemampuannya berada pada level 2. Hal ini perlu ditingkatkan dengan mendokumentasikan secara lengkap latar belakang dan praktik pengelolaan yang diusulkan dan yang dipilih. Pengukuran efektivitas ini dapat memberikan gambaran perbandingan yang nyata antara usulan praktik pengelolaan yang ada. Penelitian ini dapat dikembangkan lagi untuk proses-proses yang lainnya misalkan proses pengelolaan data, pengelolaan sumber daya manusia, dan lain sebagainya. Pengembangan penelitian perlu memperhatikan fokus dan kebutuhan manajemen terkait pengembangan infrastruktur teknologi informasi.

REFERENCES

[1] A. M. Permana, A. Rahmanto, and P. Utari, "Perkuliahan Daring Di Era Covid-19: Solusi atau Evolusi?," in *Prosiding Seminar Nasional Unimus*, Semarang: Universitas Muhammadiyah Semarang, 2020, pp. 365–372. [Online]. Available: https://prosiding.unimus.ac.id/index.php/semnas/article/view/637/642

[2] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. Schaumburg: ISACA, 2018. [Online]. Available: https://www.isaca.org/resources/cobit

[3] ISACA, *COBIT 2019 Framework Introduction and Methodology*. Schaumburg: ISACA, 2018.

[4] ISACA, *COBIT 2019 Design Guide Designing an Information and Technology Governance Solution*. Schaumburg: ISACA, 2018.

[5] M. Kegerreis, M. Schiller, C. Davis, and B. Wrozek, *IT Auditing Using Controls to Protect Information Assets*, 3rd ed. New York: McGraw-Hill Education, 2020.

[6] K. Wabang, Y. Rahma, A. P. Widodo, and F. Nugraha, "Tata Kelola Teknologi Informasi Menggunakan COBIT

2019 Pada PSI Universitas Muria Kudus," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 7, no. 3, pp. 275–282, 2021, [Online]. Available: https://jurnal.stmikroyal.ac.id/index.php/jurteksi/article/view/1103

[7] M. Saleh *et al.*, "Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas," *JEPIN (Jurnal Edukasi dan Penelit. Inform.*, vol. 7, no. 2, pp. 204–209, 2021, [Online]. Available: https://jurnal.untan.ac.id/index.php/jepin/article/view/48228

[8] S. F. Bayastura, S. Krisdina, and A. P. Widodo, "ANALISIS DAN PERANCANGAN TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019 PADA PT. XYZ," *J. Inform. dan Komput.*, vol. 4, no. 1, pp. 68–75, 2021, doi: 10.33387/jiko.

[9] D. Darwis, N. Y. Solehah, and D. Dartnono, "Penerapan Framework COBIT 5 Untuk Audit Tata Kelola Keamanan Informasi Pada Kantor Wilayah Kementerian Agama Provinsi Lampung," *TELEFORTECH J. Telemat. Inf. Technol.*, vol. 1, no. 2, pp. 38–45, 2021.

[10] M. Ikhsan and D. M. K. Nugraheni, "Evaluasi Tata Kelola Teknologi Informasi pada Proses Pengelolaan Inovasi dan Pengelolaan Perubahan Teknologi Informasi Menggunakan COBIT 2019 di PT. XYZ," *J-COSINE (Journal Comput. Sci. Informatics Eng.*, vol. 6, no. 1, pp. 47–55, 2022, [Online]. Available: https://jcosine.if.unram.ac.id/index.php/jcosine/article/view/430

[11] T. M. Insani, Samsudin, and A. Ikhwan, "Implementasi Framework Cobit 2019 Terhadap Tata Kelola Teknologi Informasi Pada Balai Penelitian Sungei Putih," *J. Tek. Inform. Kaputama*, vol. 6, no. 1, pp. 50–60, 2022, [Online]. Available: https://jurnal-backup.kaputama.ac.id/index.php/JTIK/article/viewFile/674/518

[12] ISACA, *COBIT 2019 Implementation Guide Implementing and Optimizing an Information and Technology Governance Solution*. Schaumburg: ISACA, 2018. [Online]. Available: http://linkd.in/ISACAOfficial

[13] R. A. Setiawan and W. Wasilah, "Evaluasi Tata Kelola Dan Manajemen Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Dinas Komunikasi Dan Informatika Kabupaten Lampung Selatan," in *Prosiding Seminar Nasional Darmajaya*, Lampung: Institut Informatika dan Bisnis Darmajaya, 2022, pp. 8–15. [Online]. Available: https://jurnal.darmajaya.ac.id/index.php/PSND/article/view/3247%0Ahttps://jurnal.darmajaya.ac.id/index.php/PSND/article/download/3247/1437

[14] A. W. N. Putra, A. Sunyoto, and A. Nasiri, "PERENCANAAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI LABORATORIUM KALIBRASI MENGGUNAKAN COBIT 2019 (Studi Kasus: Laboratorium Kalibrasi BSML Regional II)," *J. Fasilkom*, vol. 10, no. 3, pp. 241–247, 2020, doi: 10.37859/jf.v10i3.2272.

[15] A. Q. A'yuni, A. H. Muhammad, and A. Nasiri, "Literature Review Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019," *J. Inf.*, vol. 9, no. 1, pp. 47–52, 2023, [Online]. Available: https://informa.poltekindonusa.ac.id/index.php/informa/article/view/247

[16] R. Fadhilah, I. Santosa, and L. Abdurrahman, "RENCANA AUDIT TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 2019 PADA UNIT ISTI UNIVERSITAS TELKOM," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 3, pp. 157–163, 2021, doi: 10.33387/jiko.

[17] E. Wulandari, L. H. Atrinawati, and M. G. L. Putra, "Perancangan Tata Kelola Teknologi Informasi dengan Menggunakan Framework Cobit 2019 pada PT XYZ Balikpapan," *DoubleClick J. Comput. Inf. Technol.*, vol. 5, no. 2, pp. 127–138, 2022, doi: 10.47080/simika.v5i1.1423.

[18] S. D. Putra, H. Herman, and A. Yudhana, "AUDIT TATA KELOLA ACADEMIC INFORMATION SYSTEM MENGGUNAKAN FRAMEWORK COBIT 2019," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 3, pp. 467–474, 2023, doi: 10.25126/jtiik.20231036361.