Evaluasi Kapabilitas Sitem Keamanan Informasi Pusat Teknologi dan Pangkalan Data Universitas X Menggunakan Process Assessment Model Framework Cobit 5 (Domain DSS05)

Hariani[1)], Nur Afif[2)], Wahyuddin Saputra[3)] Andi Muhammad Nur Hidayat[4)]

[1,2,3,4] Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Alauddin Makassar
[1,2,3]Jl. H.M. Yasin Limpo No. 36 Samata, Kab Gowa, Sulawesi Selatan, Indonesia
E-mail: hariani.kasim@uin-alauddin.ac.id[1)], nur.afif@uin-alauddin.ac.id[2)] , wahyuddin.saputra@uin-alauddin.ac.id[3)], andi.nurhidayat@uin-alauddin.ac.id[4]

Abstrak – Kontrol keamanan aset informasi yang lemah adalah masalah yang harus dicegah dan perlu diatasi untuk menghindari pihak yang tidak bertanggungjawab dapat mencuri dan mengganggu jalannya aktivitas yang berkaitan dengan pengelolaan data dan informasi. Salah satu instansi yang membutuhkan keamanan terhadap perlindungan aset informasi adalah UPT Pusat Teknologi dan Pangkalan Data Universitas X. Divisi ini merupakan unit pelaksana yang bertugas menyiapkan dukungan fasilitas penyelenggaraan sistem informasi dan berfungsi sebagai pusat data dan informasi akademik yaitu penerima, pengolah, dan pendistribusi Informasi. Penelitian ini menggunakan Framework COBIT 5 dan berfokus pada domain DSS05 untuk mengukur capablitas level pada UPT tersebut, hasil yang diperoleh UPT Pusat Teknologi dan Pangkalan Data pada Universitas X hampir sepenuhnya telah menerapkan proses subdomain DSS05 pada level 1 yaitu *Performed Process* dan mencapai tujuan yang diharapkan. Nilai capability level berada pada skala *F-Fully achieved* dengan skor sebesar 87%. Meskipun demikian, masih terdapat GAP pada beberapa proses yaitu dari DSS05.1-DSS5.7. agar bisa melangkah ke level berikutnya sebaiknya instansi melakukan perbaikan berdasarkan rekomendasi yang diberikan agar skala pada tiap proses DSS05 keseluruhan bisa mencapai *F-Fully achieved*.

Kata Kunci: Keamanan Informasi, Audit, COBIT 5, DSS05

PENDAHULUAN

Kemajuan TI atau SI di era globalisasi berkembang sangat pesat. Teknologi informasi menjadi kebutuhan bagi organisasi sebagai alat komunikasi, pengolahan data dan informasi serta sebagai upaya meningkatkan efektivitas kinerja organisasi. Kontrol keamanan aset informasi yang lemah adalah masalah yang harus dicegah dan perlu diatasi untuk menghindari pihak yang tidak bertanggungjawab dapat mencuri dan mengganggu jalannya aktivitas yang berkaitan dengan pengelolaan data dan informasi. Salah satu instansi yang membutuhkan keamanan terhadap perlindungan aset informasi adalah UPT Pusat Teknologi dan Pangkalan Data Universitas X. Divisi ini merupakan unit pelaksana yang bertugas menyiapkan dukungan fasilitas penyelenggaraan sistem informasi dan berfungsi sebagai pusat data dan informasi akademik yaitu penerima, pengolah, dan pendistribusi Informasi.

UPT Pusat Teknologi dan Pangkalan Data Universitas X merupakan organisasi pendidikan yang telah menerapkan TI dalam proses operasionalnya seperti sistem informasi akademik, sistem informasi keuangan, sistem informasi penerimaan mahasiswa baru, serta sistem informasi kepegawaian. Keberadaan sistem informasi dalam organisasi perlu dipelihara dan diawasi dengan baik sehingga dapat dipastikan bahwa sistem organisasi selaras dengan tujuan bisnis organisasi. Untuk memastikan bahwa proses-proses bisnis terhindar dari insiden-insiden yang berkaitan dengan keamanan informasi maka setiap perusahaan memerlukan suatu penerapan tata kelola TI (IT Governance) yang berkaitan dengan keamanan informasi.

Tata kelola keamanan teknologi informasi merupakan kebutuhan primer bagi setiap instansi publik maupun non-publik dalam Revolusi Industri 4.0. Revolusi Industri 4.0 hadir dalam kehidupan masyarakat dengan membawa tren otomasi dan internet of things. Era dimana pemanfaatan teknologi, big data, dan cloud computing mendukung penerapan otomasi dan membangun hubungan untuk bertukar informasi melalui jaringan. Ancaman dan gangguan keamanan cyber adalah tanggung jawab bersama setiap instansi publik. Instansi perlu membangun komitmen dan budaya kesadaran keamanan informasi mulai dari tingkatan top level management sampai dengan pegawai teknis. Seluruh pihak dalam instansi harus berkontribusi secara optimal dan proporsional sesuai

dengan perannya masing-masing. Keamanan informasi yang baik hanya dapat dicapai melalui penerapan sejumlah upaya-upaya teknis yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai.

Berdasarkan data dari Security Report, Check Point (2018), terdapat sebanyak 64% Lembaga Publik di seluruh dunia bermasalah dengan keamanan teknologi informasi. Salah satu penyebabnya adalah belum optimalnya penerapan tata kelola keamanan teknologi informasi. Hal ini perlu disikapi serius oleh instansi publik untuk meningkatkan perbaikan di aspek tata kelola keamanan teknologi informasi. Solusi teknis memang dapat memecahkan permasalahan, namun tanpa adanya perbaikan tata kelola akan menjadi sia-sia. Salah satu cara untuk memastikan hal tersebut adalah dengan melakukan audit sistem informasi. Audit sistem informasi dapat dilakukan dengan menggunakan berbagai framework seperti Cobi, ITIL, COSO, dan sebagainya.

Cobit atau Control Objectives for Information and related Technology merupakan salah satu framework yang digunakan untuk melakukan audit sistem informasi. Hal-hal yang perlu diaudit menurut Cobit dibagi ke dalam 4 fokus utama yang disebut domain. Keempat domain Cobit tersebut di antaranya adalah Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), serta Monitor and Evaluate (ME). Domain PO menjelaskan mengenai proses perencanaan yang dilakukan organisasi, AI menjelaskan proses implementasi dari perencanaan tersebut sehingga menjadi sebuah layanan, DS menjelaskan proses pelayanan kepada pengguna sistem, ME menjelaskan proses pengawasan dan evaluasi terhadap perencanaan, implementasi, serta pelayanan yang diberikan kepada pengguna sistem.

COBIT 5 dipilih untuk menangani permasalahan tata kelola keamanan teknologi informasi karena menyajikan kerangka kerja yang komprehensif dalam membantu instansi mencapai tujuan yang berkaitan dengan pengelolaan keamanan informasi dan aset teknologi yaitu subdomain DSS05 (*Manage Security Service*). COBIT 5 bersifat generik dan bermanfaat untuk instansi dari semua ukuran, baik komersial ataupun sektor publik (ISACA, 2012).

LANDASAN PUSTAKA

Framework COBIT 5

Suatu teknik yang dilakukan dengan melakukan tahapan ilmiah yang dikerjakan oleh peneliti untuk mengumpulkan data dan informasi dengan tujuan untuk menjawab rumusan masalah yang di teliti. Kerangka kerja (Framework) yang digunakan untuk tata kelola TI (IT Governance) ada banyak sekali, salah satu IT Governance yang banyak diterapkan adalah COBIT (Control Objectives for Information and related Technology). COBIT (Control Objectives for Information and Related Technology) ialah instrumen panduan general (best practice) guna manajerial teknologi informasi, yang dirancang oleh Information System and Control Association (ISACA), dan IT Governance Institute (ITGI) pada tahun 1996. Pada tahun 2012, ISACA menerbitkan COBIT 5, yang adalah struktur pekerjaan untuk IT Governance manajemen perusahaan TI. COBIT 5 menghubungkan COBIT 4.1, Val IT dan Risk IT menjadi kesatuan struktur pekerjaan yang berlaku sebagai struktur kerja perusahaan yang selaras dan bisa dikelola dengan TOGAF dan ITIL. COBIT 5 merupakan framework baru, yang mengombinasikan tata laksana dan teknik pengelolaan perusahaan di mana mempunyai pedoman praktik, model dan alat analisis yang secara umum diperoleh guna berkontribusi dalam peningkatan performa tata kelola TI

COBIT memiliki 5 (lima) kerangka kerja utama yang dijelaskan sebagai berikut :

1. Evaluate, Direct, and Monitor (EDM): Domain ini mencakup terhadap proses pengelolaan yang memiliki keterkaitan dengan pengelolaan sasaran stakeholder, nilai pengiriman, optimisasi resiko dan sumber daya, yang mencakup praktek dan aktivitas yang ditujukan terhadap proses evaluasi pilihan strategi, pemberian pengarahan IT, dan proses monitorisasi outcome.
2. Align, Plan and Organise (APO): Domain ini mencakup strategi dan taktik, domain ini juga berfokus terhadap proses identifikasi cara terbaik pengkontribusian IT dalam mencapai sasaran bisnis. Realisasi dari visi strategi harus direncanakan, dikomunikasikan, dan dikelola untuk prespektif yang berbeda. Pengorganisasian yang benar dan infrastruktur teknologi harus ditempatkan di tempat yang benar.
3. Build, Acquire, and Implement (BAI): Domain ini berperan dalam pemberian solusi dan menyediakan pelayanan. Dalam perealisasian strategi IT, solusi IT perlu diidentifikasi, dikembangkan atau didapatkan, begitupun diimplementasikan dan

diintegrasikan pada proses bisnis. Perubahan dan maintenance dari sistem yang ada juga pada lingkup domain ini, untuk memastikan solusi sesuai dengan tujuan bisnis.

4. Deliver, Service and Support (DSS): Domain DSS berfokus terhadap aktual delivery and support of required services, yang temasuk service delivery, pengelo laan atas keamanan dan kontinuitas, layanan bantuan untuk user, serta manajemen atas data dan fasilitas operasional.
5. Monitor, Evaluate and Assess (MEA): berperan dalam tindakan monitoring semua proses sehingga dapat memastikan pengarahan yang diberikan ditaati. Semua proses IT harus diperiksa secara regular tiap waktu untuk memastikan kebutuhan kualitas dan ketaatan dengan kebutuhan pengendalian. Domain mengajukan manajemen kinerja, monitor dari internal, ketaaatan dan tata kelola

RACI Chart

Framework pada COBIT 5 menggunakan diagram RACI dalam menentukan tanggung jawab atau peran suatu proses terhadap setiap *stakeholder*. Diagram ini sebagai alat ukur dalam mengidentifikasi peran dan tanggung jawab seorang karyawan pada sebuah proses bisnis untuk suatu organisasi. Terdapat empat klasifikasi peran dalam diagram RACI menurut ISACA pada tahun 2012 seperti yang terlihat pada tabel di bawah ini:

Tabel 1. RACI Chart

Peran	Keterangan
R(esponsible)	Orang yang bertanggung jawab dan memiliki peran utama untuk memastikan tiap aktivitas berhasil terlaksana.
A(ccountable)	Orang yang bertanggung jawab dan mempunyai wewenang dalam pengambilan keputusan pada pelaksanaan aktivitas tertentu.
C(onsulted)	Orang yang memberikan masukan dan pendapat dalam suatu aktivitas (konsultan).
I(nformed)	Orang yang bertanggung jawab dalam menerima informasi untuk mengawasi aktivitas yang sedang dilakukan (Informan).

Capability Model

Penentuan *capability* level pada *Process assessment model* (PAM) pada COBIT ditentukan berdasarkan Sembilan atribut proses di awali oleh PA yang dijelaskan dalam ISO/IEC 15504-2:2003 sebagai berikut:

Tabel 2. Capability Level dan Process Attributes

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work product management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimizing process
PA 5.1	Process innovation
PA 5.2	Process optimization

1. Level 0 (*incomplete)*: tidak mengimplementasikan proses disebabkan bukti pencapaian sistematis dari tujuan proses yang dimiliki hanya terdiri dari sedikit atau tidak ada.
2. Level 1 (*performed*): pengimplementasian proses mencapai tujuan.
3. Level 2 (*managed*): pengimplementasian proses telah terkelola (terencana, diawasi, dan disesuaikan)
4. Level 3 (*established*): pengimplementasian proses menggunakan proses yang terdefinisi dan mampu mencapai hasil.
5. Level 4 (*predictable*): pengimplementasian proses saat ini berjalan dengan batasan yang terdefinisi dalam mencapai hasil.
6. Level 5 (*optimizing*): pengimplementasian proses yang dapat diprediksi akan ditingkatkan untuk memenuhi tujuan bisnis organisasi saat ini.

Penilaian proses untuk mencapai kemampuan pada tingkat 1 dilakukan dengan mengevaluasi hasil deskripsi proses secara detail kemudian diklasifikasikan menjadi empat kategori seperti pada tabel dibawah:

Tabel 3. Rating Levels

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

Sumber: ISO/IEC 15504-2:2003 dalam COBIT 5 Process Assessment Model.

Proses tersebut dapat dijelaskan sebagai berikut:

a. N (*Not achieved*) tidak ada atau hanya sedikit bukti atas pencapaian atribut proses dengan rentang nilai berkisar 0-15%.
b. P (*Partially achieved*) terdapat beberapa bukti mengenai pendekatan dan pencapaian atribut suatu proses dengan rentang nilai 15-50%.
c. L (*Large achieved*) terdapat bukti atas pendekatan sistematis dan pencapaian signifikan pada proses walaupun terdapat kelemahanyang tidak signifikan yang memiliki rentang nilai 50-85%.
d. F (*Fully achieved*) terdapat bukti lengkap atas pendekatan sistematis dan pencapaian penuh pada atribut proses dengan rentang nilai 85-100%.

Domain DSS05

Fokus pada domain ini yaitu pengiriman, pelayanan dan pendukungan terhadap pengelolaan operasional, permintaan, penanganan masalah, layanan keamanan, aturan keberlanjutan bisnis serta proses bisnis pada organisasi. Terdapat 6 proses pada domain DSS yang meliputi: (1) DSS01 *Manage Operations*; (2) DSS02 *Manage Service Requests and Incidents*; (3) DSS03 *Manage Problems*; (4) DSS04 *Manage Continuity*; (5) DSS05 *Manage Security Services*; dan (6) DSS06 *Manage Business Process Controls*.

Pada bagian proses DSS05 terkait *Manage security services* memiliki tujuan untuk melindungi informasi organisasi dalam mempertahankan tingkat resiko keamanan yang diterima organisasi sesuai kebijakan kemanan. Terdapat tujuan lain yaitu membangun, memelihara peran keamanan informasi, hak akses, monitoring kemanan, memperkecil insiden dan dampak bisnis dari kerentanan keamanan informasi operasional, (ISACA, 2012).

PENELITIAN TERKAIT

Penelitian ini ditinjau dari penelitian sebelumnya, berikut beberapa penelitian terkait mengenai tata kelola dan manajemen keamanan informasi.

Penelitian yang dilakukan (Imany et al., 2019) dengan menggunakan kerangka kerja COBIT 5 dengan fokus pada proses APO13 tentang pengelolaan keamanan dan DSS05 terkait pengelolaan layanan. Hasil penelitian, kedua menunjukkan proses telah mencapai level 2 (*Managed Process*), dengan tingkat pencapaian yang diinginkan perusahaan berada pada level 3 (*Established Process*). Hasil tersebut memiliki kesenjangan (*gap level*) sebesar 1 level pada masing-masing proses. Dari hasil tersebut terdapat beberapa saran dalam penelitian ini untuk meningkatkan hasil diantaranya adalah menggunakan proses lain dari COBIT 5 yang berkaitan dengan keamanan informasi seperti EDM03 (*Ensure Risk Optimisation*), APO12 (*Manage Risk*), BAI06 (*Manage Changes*). Selain itu, penelitian selanjutnya dapat mengembangkan penelitian ini dengan menggunakan kerangka kerja atau standar lain yang berkaitan dengan keamanan informasi seperti ISO/IEC 27001, ITIL (*Information Technology Infrastructure Library*) *For Information Security*, ISO 31000 dan kerangka kerja lainnya.

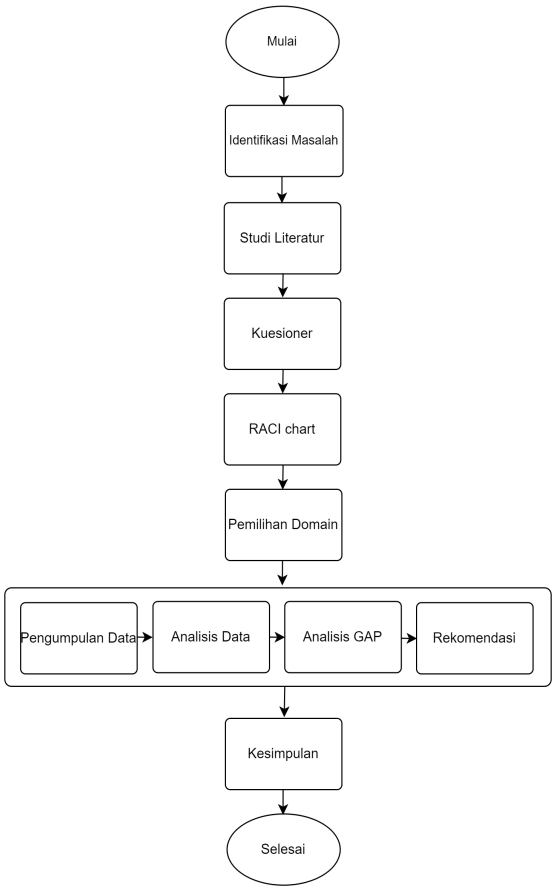
Penelitian yang dilakukan (Nurhuda et al., 2021) mengenai Audit Pendataan Keluarga menggunakan Pendekatan *Framework* COBIT 5 pada Domain DSS memperoleh hasil dari 6 proses terpilih pada domain DSS terdapat 4 proses yang mencapai level 1 (*performed*) dan 2 proses yang berhasil mencapai level 2 (*managed process*). Tingkat kemampuan manajemen TI yang diharapkan berada pada level 3 sehingga GAP muncul di semua domain yang bermakna saat ini organisasi belum sepenuhnya mengimplementasikan proses yang ditetapkan untuk mencapai tujuan proses. Dari seluruh rangkaian penelitian tersebut dapat disimpulkan bahwa diperoleh nilai level kapabilitas sebesar 1,33 dan terdapat GAP sebesar 1,67 untuk mencapai level yang diharapkan. Untuk mengatasi kekurangan-kekurangan tersebut maka diberikan beberapa rekomendasi perbaikan untuk hasil yang lebih maksimal diantaranya meningkatkan kapabilitas proses sehingga BKKBN Propinsi Jawa Barat dapat mencapai tingkat kapabilitas yang diharapkan.

Penelitian yang dilakukan oleh (Agung et al., 2019) untuk mengukur tingkat kapabilitas sistem informasi akademik terhadap ketercapaian visi dan misi universitas. Meneliti dampak yang terjadi pada universitas terkait tingkat kapabilitas sistem informasi akademik. Penelitian ini berfokus pada keefektifan, keefisienan, unit fungsional teknologi informasi pada sistem informasi akademik, integritas, *saveguarding assets*, *reliability, confidentiality, availabilty* dan *security*. Penelitian ini menggunakan *framework*

COBIT 5 pada domain *Deliver, Service & Support* (DSS) dengan hasil tata kelola Sistem Informasi Akademik sudah dilakukan walaupun masih belum berjalan secara optimal karena belum mencapai pada tingkat kematangan yang diharapkan. Domain DSS06 (Manage business process controls) memiliki hasil index level minimum sedangkan domain DSS04 (Manage continuity) memiliki hasil index level maksimum adalah. Dari hasil tersebut maka direkomendasikan solusi dalam hal peningkatan kapabilitas sistem informasi akademik pada universitas tersebut.

METODOLOGI PENELITIAN

Penelitian ini merujuk pada metode kualitatif *Scientific Research in Information Systems* (Recker, 2016) dan metode *Self-Assessment* Cobit 5. Adapun kerangka fikir penelitian dapat dilihat pada gambar dibawah:



Gambar 1. Kerangka Penelitian

Penelitian ini dikerjakan dengan beberapa tahapan secara runut, tahap pertama dimulai dengan melakukan identifikasi masalah pada pusat data centre Universitas X, selanjutnya tahap observasi dengan melakukan Interview pada kepala UPT untuk mengetahui kondisi sistem di lapangan. Tahapan selanjutnya, mencari referensi dan mempelajari literatur terkait untuk menunjang penelitian. Sumber literatur diperoleh dari jurnal ilmiah, buku dan website yang terpercaya. Hasil studi literatur dapat mengetahui penelitian serupa dari peneliti terdahulu, selanjutnya penulis mengikuti kerangka dan alur yang digunakan untuk mengidentifikasi domain yang digunakan pada penelitian ini. Tahapan berikutnya adalah penyusunan kuesioner. Kuesioner dibuat berdasarkan kerangka cobit 5 dengan melihat setiap proses dan point-point aktivitas dari domain yang dipilih. Selanjutnya menentukan *RACI Chart* berdasarkan struktur jabatan pada UPT Pusat Data Centre Universitas X, hal ini bertujuan untuk memetakan pembagian kuesioner berdasarkan peran dan jabatan pemangku kepentingan pada UPT tersebut. Tahapan selanjutnya, pemilihan domain yang akan digunakan dengan menyesuaikan proses bisnis yang selaras dengan visi misi lembaga, proses tersebut berfokus pada domain DSS05.

Tahapan yang sangat penting selanjutnya yaitu pengumpulan data. Tahapan ini harus sesuai dengan prosedur dan panduan dari kerangka Cobit 5 yang digunakan. Karena, jika terjadi kesalahan dalam proses ini akan menyebabkan data tidak kredibel dan tidak bisa dipertanggungjawabkan. Data yang telah dikumpulkan, selanjutnya akan dianalisis untuk menentukan capability level sehingga diketahui nilai domain yang menunjukkan kondisi sistem keamanan saat ini dan kondisi sistem keamanan yang diharapkan. Kesenjangan yang ditemukan pada tingkat kapabilitas disebut dengan gap. Hasil informasi gap tersebut nantinya sebagai acuan untuk mencapai level tertinggi sesuai yang diharapkan di akan datang. Berdasarkan temuan hasil analisis gap akan disarankan sejumlah rekomendasi untuk memperbaiki tata kelola sistem kemanan sistem Informasi saat ini sehingga visi misi yang diharapkan bisa tercapai.

HASIL DAN PEMBAHASAN

Studi kasus akan memfokuskan pada proses yang mengacu pada prinsip COBIT 5 agar membantu organisasi mencapai tujuan yang diinginkan.

A. Analisis RACI Chart

Seperti yang telah dijelaskan sebelumnya, *RACI Chart* merupakan metode pemetaan peran dan tanggungjawab dari organisasi. RACI Chart pada penelitian ini akan dipetakan sesuai dengan struktur yang ada pada Pusat Teknologi dan Pangkalan Data Universitas X. tabel 3 berikut memberikan gambaran RACI Chart sesuai dengan peran pada UPT tersebut.

Tabel 4. RACI Chart Organisasi

	Komponen	Peran sesuai COBIT 5	Jabatan
DSS05 RACI Chart	**R**	Head IT Operations	Kepala UPT
		Head Development	Divisi Data Centre
		Chief Information Officer	Divisi Pengembangan dan Pelatihan Sistem
		Information Security Manager	Divisi Internet dan Jaringan
	A	Chief Information Security Officer	Divisi Multimedia dan WEB

B. Analisis Kuesioner

Penelitian ini menggunakan capability level pada framework COBIT 5 untuk mengukur jawaban responden yang telah dikumpulkan dari kuesioner sesuai dengan pemetaan *RACI Chart*. Terdapat 5 responden yang memberikan jawaban melalui kuesioner sesuai dengan kapabilitas masing-masing dimana pernyataan kuesioner dibuat sesuai dengan panduan COBIT 5 pada domain DSS05. Contoh hasil analisis dapat dilihat pada tabel 4 berikut.

Tabel 5. Contoh Analisis Kuesioner

Sub Domain	Pertanyaan	Responden					Persetujuaan		Presentase	Rata-rata	Skala %	Level
		1	2	3	4	5	dilakukan	Tidak				
DSS05.1	BPs										92%	Fully Achieved (F)
	1	1	1	1	1	1	5	0	100%	93%		
	2	0	1	1	1	1	4	1	80%			
	3	1	1	1	1	1	5	0	100%			
	4	1	1	1	1	1	5	0	100%			
	5	1	1	1	1	1	5	0	100%			
	6	0	1	0	1	1	4	1	80%			
	Jumlah	**4**	**6**	**5**	**6**	**6**	**28**	**2**	**93%**			
	WPs											
	1	1	1	1	1	0	4	1	80%	90%		
	2	1	1	1	1	1	5	0	100%			
	Jumlah	**2**	**2**	**2**	**2**	**1**	**9**	**1**	**90%**			

C. Capability Level DSS05

Tingkat capability level ditentukan berdasarkan analisis data dari kuesioner dan interview yang dilakukan, tujuannya untuk melihat kondisi sistem saat ini. Analisis dilakukan menggunakan panduan COBIT 5 domain DSS05. Tingkat capability level pada organisasi saat ini dapat dilihat pada tabel 6 berikut.

Tabel 6. Penilaian Capability level DSS05

Sub Domain	Proses	Skala	Pencapaian
DSS05.1	Perlindungan Terhadap Malware	92%	**F**
DSS05.2	Pengelolaan Jaringan dan Keamanan Konektivitas	95%	**F**
DSS05.3	Pengelolaan Keamanan Endpoint	80%	**L**
DSS05.4	Pengelolaan Identitas Pengguna dan Akses Logical	79%	**L**
DSS05.5	Pengelolaan Akses Fisik ke Aset TI	93%	**F**
DSS05.6	PengelolaanDokume Penting dan Perangkat Keluaran	79%	**L**
DSS05.7	Memonitor Infrastruktur untuk Kegiatan yang Berhubungan dengan Keamanan	88%	**F**
Jumlah		**87%**	**F**

Tabel 7. Capaian Capability Level domain DSS05

Proses **Manage Service Security**

DSS05	Level 0	Level 1.1	Level 2		Level 3	
		PA.1.1	PA.2.1	PA.2.2	PA3.1	PA.3.2
Presentase	100 %	87%				
Rating by Criteria	F	F				
Keterangan:	N (Not Achieved, 0%-15%), P (Partially Achieved, >15%-50%), L (Largelly Achieved, >50%- 85%), F (Fully Achieved, >85%-100%)					

Capaian capability level pada domain DSS05 seperti terlihat pada tabel 7. Pada tabel menjelaskan bahwa Level 1 berada pada rating *fully achieved* atau memperoleh skor 87% yang berarti bahwa organisasi sudah menjalankan proses DSS05 untuk *Performed Process* hampir seluruhnya sudah mencapai tujuan. Sementara target organisasi yaitu berada pada level 3 *(Established process)* maka ada kesenjangan yang terjadi sekitar 2 level.

D. Analisis GAP

Untuk mengetahui perbandingan tingkat kapabilitas saat ini dan tingkat kapabilitas yang diharapkan maka digunakan analisis GAP. Jika hasil analisis menunjukkan mempunyai level yang sama maka proses dianggap sudah berjalan dengan baik. Namun, jika hasil analisis menunjukkan ada kesenjangan maka diperlukan rekomendasi-rekomendasi untuk meningkatkan proses yang sedang berjalan. Tabel berikut menjelaskan hasil analisis GAP yang diperoleh.

Tabel 8. Hasil analisis GAP

Proses	**Capability Level**	**Targeted Level**	**Gap**
DSS05-Manage Service Security	1	3	2

Hasil analisis menunjukkan pencapaian saat ini (*as is*) berada pada level 1 sementara target yang ingin dicapai (*to be*) berada pada level 3 yaitu *Established Process*. sehingga ada kesenjangan sebanyak 2 level. Untuk mengatasi hal tersebut dibutuhkan sejumlah rekomendasi untuk perbaikan proses.

E. Rekomendasi

Agar tercapai proses yang diinginkan maka beberapa rekomendasi dapat diterapkan untuk meningkatkan nilai capability level, diantaranya:

1. Rekomendasi Proses DSS05.01

   UPT Pusat Teknologi dan Pangkalan Data pada Universitas X harus melakukan instalasi dan mengaktifkan *tools* perlindungan pada semua aset dan fasilitas device yang dimiliki agar terlindung dari perangkat lunak yang bisa membahayakan sistem, baik secara otomatis maupun semi-otomatis. Selanjutnya, instansi sebaiknya mendukung staf untuk mengikuti pelatihan tentang malware dan mengadakan kerjasama ke beberapa vendor terkait serta mengeluarkan kebijakan bagaimana mencegah perangkat lunak yang berbahaya dalam bentuk dokumen.

2. Rekomendasi Proses DSS05.02

   UPT Pusat Teknologi dan Pangkalan Data pada Universitas X sebaiknya melakukan Penetration Testing pada sistem secara berkala kemudian hasilnya di dokumentasikan untuk dijadikan acuan dan dipelajari jika ada *trouble* sistem dikemudian hari.

3. Rekomendasi Proses DSS05.03

   UPT Pusat Teknologi dan Pangkalan Data pada Universitas X sebaiknya membuat dan mengadakan dokumen tentang kebijakan keamanan untuk perangkat endpoint.

4. Rekomendasi Proses DSS05.04

   UPT Pusat Teknologi dan Pangkalan Data pada Universitas X sebaiknya melakukan identifikasi secara unik untuk pengguna sistem baik pengguna internal, eksternal dan yang hanya sementara. Selanjutnya, mengidentifikasi aktivitas pengguna baik berupa aplikasi, infrastruktur, sistem operasi, pengembangan dan pemeliharaan sistem.

   Rekomendasi selanjutnya, sebaiknya instansi mengadakan dokumen mengenai hak akses pengguna yang disetujui dan dokumen hasil ulasan akun pengguna.

5. Rekomendasi Proses DSS05.05

   UPT Pusat Teknologi dan Pangkalan Data pada Universitas X sebaiknya memberi batasan akses ke situs IT yang masuk dalam klasifikasi sensitif dengan menetapkan pembatasan perimeter, seperti pagar, dinding, dan perangkat keamanan pada pintu interior dan eksterior. Selanjutnya, memastikan perangkat seperti CCTV dan alarm jika terjadi akses yang tidak sah.

   Rekomendasi selanjutnya, instansi memberikan dukungan untuk mengikuti pelatihan keamanan fisik secara berkala dan mengadakan dokumen mengenai permintaan akses yang disetujui.

6. Rekomendasi Proses DSS05.06

   UPT Pusat Teknologi dan Pangkalan Data pada Universitas X sebaiknya membuat prosedur untuk

mengatur penerimaan, penggunaan, penghapusan dan pembuangan yang dituangkan dalam formulir khusus baik di dalam dan di luar instansi. Selanjutnya mengamankan informasi yang sensitif jika ada penggantian inventaris baru.

Rekomendasi selanjutnya, mengadakan dokumen mengenai inventaris dokumen penting dan perangkat sistem serta mengadakan dokumen mengenai hak akses khusus. A,

7. Rekomendasi Proses DSS05.07

   UPT Pusat Teknologi dan Pangkalan Data pada Universitas X sebaiknya melakukan peninjauan aktifitas log secara berkala, membuat dokumen yang berisi log insiden yang pernah terjadi dan dokumen mengenai karakteristik dari insiden yang pernah terjadi.

KESIMPULAN DAN SARAN

Berdasarkan hasil audit diatas menggunakan Framework COBIT 5, maka dapat disimpulkan bahwa UPT Pusat Teknologi dan Pangkalan Data pada Universitas X hampir sepenuhnya telah menerapkan proses subdomain DSS05 sampai pada level 1 yaitu *Performed Process* dan mencapai tujuan yang diharapkan. Nilai capability level berada pada skala *F-Fully achieved* dengan skor sebesar 87%. Agar bisa melangkah ke level berikutnya sebaiknya instansi melakukan perbaikan berdasarkan rekomendasi yang diberikan agar skala bisa mencapai 90% keatas.

DAFTAR PUSTAKA

Agung, H., Mulia, U. B., Andry, J., & Mulia, U. B. (2019). *AUDIT SISTEM INFORMASI AKADEMIK PADA UNIVERSITAS XYZ AUDIT SISTEM INFORMASI AKADEMIK PADA UNIVERSITAS XYZ MENGGUNAKAN*. *August*.

COBIT Self-assessment Guide: Using COBIT 5.

ISACA. (2012). COBIT 5: Enabling Process

Imany, Y. D., Hayuhardhika, W., Putra, N., & Herlambang, A. D. (2019). Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(6), 5926–5935.

Recker, J. (2016). *Scientific Research in Information Systems : A Beginner ' s Guide*. *January 2012*.

M., Nurhuda, A. M., Philipus, E., & Gunawan, I. (2021). *Audit Sistem Pendataan Keluarga Menggunakan Pendekatan Framework COBIT 5 Pada Domain DSS (Studi Kasus : BKKBN Propinsi Jawa Barat) Auditing of Family Data System Using COBIT 5 Framework Approach in DSS Domain (Case Study : BKKBN of West Java Province)*. *10*(1), 78–87.

Process Assessment Model (PAM): Using COBIT ® 5.