ANALISIS TINGKAT KEAMANAN SISTEM AMS PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU MENGGUNAKAN COBIT 5 DENGAN DOMAIN DSS05

, Satrianansyah[1] Kurnia Adha[2], Novi Lestari[3*]
Fakultas Komputer, Program Studi Sistem Informasi, Universitas Bina Insan, Lubuklinggau[1,2]
Fakultas Komputer, Program Studi Rekayasa Sistem Komputer, Universitas Bina Insan, Lubuklinggau[3]
Email : satrianansyah@univninainsan.ic.id[1], kurniaadha12@gmail.com[2]
novi_lestari@univbinainsan.ac.id[3]

Abstrak

Academic Management System (AMS) Universitas Bina Insan adalah sistem yang sangat penting penggunannya di Universitas Bina Insan, maka dari itu untuk keamanan informasinya harus diperhatikan oleh perguruan tinggi. Informasi ini dapat berupa data mahasiswa, data dosen, jadwal perkuliahan, data mata kuliah, pengisian KRS, pengecekan nilai dan pengumuman akademik. Penelitian ini akan menggunakan metode COBIT 5 dengan domain DSS05 sebagai standar kontrol keamanan teknologi informasi. Tujuan dari Domain DSS05 ini adalah untuk melindungi informasi perusahaan dan menjaga tingkat resiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan serta menetapkan dan memelihara peran keamanan informasi dan hak akses dan melakukan pemantauan keamanan. Tujuan proses ini adalah untuk meminimalkan dampak bisnis dari kerentanan keamanan informasi operasional dan insiden. Pada kondisi saat ini (As is) memperoleh nilai 2,143 atau bisa dikatakan berada di tingkat kemampuan level 2 yaitu Repeatable But Invinitive. Artinya keamanan sistem di Universitas Bina insan belum ada standarisasi prosedur untuk pelatihan secara formal ataupun komunikasi dan tanggung jawab bergantung pada individu. Tingkat kepercayaan pada kemampuan individu sangat tinggi, sehingga kesalahan yang sama sering kali terjadi. Sedangkan, untuk kondisi yang diharapkan (to be) memperoleh nilai 4,286 dengan tingkat kematangan level 4 yang dimana pada tahap ini harus diterapkan Managed and Measurable.

Kata kunci: AMS; Keamanan; COBIT 5; DSS05; CMMI

Abstract

The Academic Management System (AMS) of Bina Insan University is a very important system for its use at Bina Insan University, therefore, for information security, universities must pay attention to it. This information can be in the form of student data, lecturer data, lecture schedules, course data, filling out KRS, checking grades and academic announcements. This study will use the COBIT 5 method with the DSS05 domain as the information technology security control standard. The purpose of this DSS05 Domain is to protect company information and maintain an acceptable level of information security risk by the company in accordance with security policies as well as establish and maintain information security roles and access rights and perform security monitoring. The purpose of this process is to minimize the business impact of operational information security vulnerabilities and incidents. In the current condition (As is) it gets a value of 2.143 or it can be said to be at the level of ability level 2, namely Repeatable But Invinitive. This means that system security at Bina Insan University does not yet have standardized procedures for formal training or communication and responsibility depends on the individual. The level of confidence in individual abilities is very high, so the same mistakes often occur. Meanwhile, for the expected condition (to be) the score is 4,286 with a maturity level of level 4 which at this stage must be applied Managed and Measurable.

***Keywords**: AMS; Security; COBIT 5; DSS05; CMMI*

I. PENDAHULUAN

Sistem informasi adalah sebuah sistem pengolahan data (SPD), yang terdiri dari komponen-komponen komunikasi yang digunakan dalam sistem organisasi data [1]. Sistem informasi akademik (SIA) adalah *software* yang digunakan untuk menyediakan informasi dan pengolahan administrasi yang berhubungan dengan kegiatan akademis [2]. Dengan penggunaan *software* seperti ini diharapkan kegiatan administrasi akademis dapat dikelola dengan baik dan informasi yang diperlukan dapat diperoleh dengan mudah dan cepat. Tetapi, dengan adanya perkembangan teknologi sering kali disalahgunakan dan menyebabkan terjadinya ancaman. Sebuah sistem informasi sangat berperan penting untuk perkembangan suatu lembaga atau institusi. Universitas Bina Insan Lubuklinggau telah menerapkan sistem informasi akademik. *Academic Management System* (AMS) adalah sistem informasi akademik yang dalam kegiatan administrasinya dilakukan secara online, sistem ini digunakan untuk mengetahui pengolahan data dosen dan mahasiswa, pengisian nilai, pengisian rencana hasil studi (KRS) dan jadwal kuliah. Sistem ini juga dapat berfungsi sebagai pendukung untuk analisis data dalam menentukan keputusan kampus. Perguruan tinggi Universitas Bina Insan menggunakan *Academic Management System* untuk mempermudah proses pengolah data akademik dan data-data lainnya. Pengguna sistem informasi akademik ini yaitu mahasiswa, dosen dan admin. *Academic Management System* (AMS) Universitas Bina Insan adalah sistem sangat penting yang harus diperhatikan oleh perguruan tinggi. Informasi baik berupa data mahasiswa, data dosen, jadwal perkuliahan, data mata kuliah, pengisian KRS, pengecekan nilai dan pengumuman akademik, wajib dilindungi dengan keamanan informasi. Keamanan informasi adalah suatu keharusan yang harus ada pada sebuah sistem. Sebelum memberikan solusi keamanan pada sebuah sistem, terlebih dahulu harus melakukan analisis tingkat keamanan pada *Academic Management System* (AMS) Universitas Bina Insan, sebatas mana tingkat level keamanan pada sistem tersebut. Penelitian ini dilakukan karena sebelumnya belum ada penelitian tentang analisis tingkat keamanan pada sebuah sistem *Academic Management System* (AMS) Universitas Bina Insan.

Demi melindungi sebuah sistem informasi tersebut maka harus dilakukan analisis tentang tingkat level keamanan yang sudah diterapkan pada sistem tersebut. Penelitian ini akan menggunakan metode COBIT 5 sebagai standar kontrol keamanan teknologi informasi. COBIT 5 *(Control Objectives for Information and Related Technology)* adalah suatu acuan standar praktek manajemen teknologi informasi dan kumpulan dokumentasi praktek terbaik (*best practices)* untuk tata kelola TI yang dapat membantu pengguna, manajemen dan auditor untuk menjembatani pemisah *(gap)* antara permasalahan-permasalahan teknis, kebutuhan pengendalian dan risiko [3]. Sedangkan untuk mencapai standar level pencapaian diperlukan CMMI pada keamanan teknologi informasi. *Capability Maturity Model Integration* (CMMI) adalah sesuatu model pendekatan untuk menilai skala kemampuan dan kematangan sebuah organisai perangkat lunak [4]. Dengan adanya model COBIT 5 dan CMMI diharapkan akan dapat membantu menentukan analisis tingkat level keamanan pada *Academic Management System* Universitas Bina Insan. Untuk menghindari pembahasan agar tidak menyimpang dari permasalah yang ada, maka penelitian ini dibatasi hanya menganalisa tingkat level keamanan pada *Academic Management System* (AMS) Universitas Bina Insan Lubuklinggau menggunakan standar *framework* COBIT 5, dengan fokus pada domain yang terpilih. Dan penggunaan metode CMMI sebagai penentuan kematangan tingkat level keamanan sistem.

Hasil penelitian terbaik sebelumnya yang sesuai dengan penelitian ini adalah

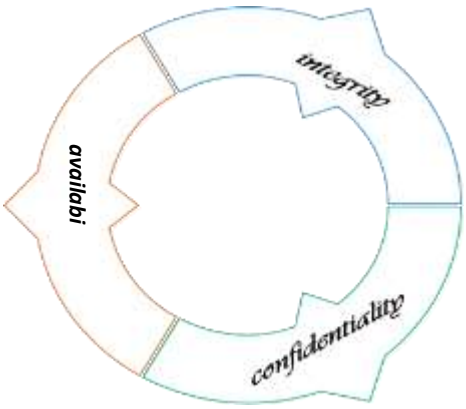
penelitian yang dilakukan oleh Rusydi Umar, Imam Riadi, Eko Handoyo Universitas Ahmad Dahlan (2018) yang berjudul "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan *Capability Maturity Model Integration* (CMMI)". Hasil penelitian ini menunjukkan bahwa COBIT 5 memberikan standar yang baik dalam kontrol keamanan teknologi informasi dan CMMI memberikan standar level pencapain yang baik dalam penilaian keamanan teknologi informasi. Kombinasi *framework* COBIT 5 dan CMMI mampu memberikan solusi penilaian tingkat keamanan teknologi dengan optimal. Persamaan penelitian terdahulu dengan yang sekarang adalah terletak pada kombinasi 2 metode antara COBIT 5 dan CMMI. Sedangkan perbedanya adalah tentang sistem yang diteliti [3].

Sistem informasi harus memberikan keamanan, kerahasiaan dan integritas data yang diolah kinerja sistem informasi agar dapat dimanfaatkan secara optimal dan aman. Analisis ini dilakukan guna untuk mengetahui kualitas keamanan sistem sehingga dapat dipertimbangkan, ditingkatkan dan memastikan keberlanjutan sistem keamanan tersebut, meminimalkan resiko yang mungkin terjadi dan memaksimalkan kegunaan pada sistem tersebut. Tujuan lainnya adalah untuk mengatasi segala masalah dan kendala baik secara teknis maupun secara non-teknis yang dapat berpengaruh dalam kinerja sistem. Dan sebelumnya belum ada penelitian tentang analisis tingkat level keamanan pada *Academic Management System* (AMS) Universitas Bina Insan. Sistem informasi akademik sebagai manajemen akademik perlu memastikan keamanan, privasi dan integritas data yang diolah, sistem informasi juga menjadi bagian penting yang harus diperhatikan agar sistem informasi dapat dimanfaatkan secara optimal. Penelitian ini akan dapat membantu memberikan solusi ataupun saran untuk keamanan sistem kedepannya.

II. TINJAUAN PUSTAKA

Audit keamanan adalah suatu mekanisme atau proses yang mempunyai dasar pada kebijakan pada suatu standar keamanan dalam menentukan keadaan dari perlindungan yang ada serta untuk memverifikasi apakah perlindungan yang sudah ada berjalan dengan baik ataupun belum . Tujuan utama dari audit keamanan adalah untuk memberikan gambaran dalam perlindungan sesuai dengan kebijakan ataupun aturan dan standar keamanan yang telah ditetapkan serta memverifikasi apakah perlindungan yang sudah berjalan dengan baik ataukah belum [5].

Keamanan informasi merupakan cara yang dapat kita gunakan dalam mencegah penipuan (cheating) atau, paling tidak untuk mendeteksi adanya sebuah penipuan pada sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki bentuk fisik. Keamanan informasi adalah cara atau straegi yang dapat digunakan dalam mengamankan aset informasi dari ancaman-ancaman yang mungkin ada. Secara tidak langsung keamanan informasi dapat menjamin keberlanjutan dari suatu bisnis serta mengurangi risiko-risiko yang terjadi dan dapat mengoptimalkan pengembalian investasi [6].



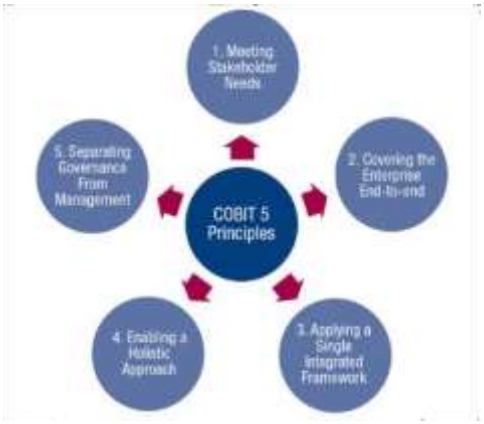
Gambar 1. Aspek Keamanan Informasi
Sumber : [3]

1. *Confidentiality* adalah keamanan informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu.

2. *Integrity* adalah keamanan informasi seharusnya menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan atau ancaman lain yang menyebabkan berubahnya informasi dari aslinya.
3. *Availability* adalah keamanan informasi seharusnya menjamin pengguna dapat mengakses informasi kapan pun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan.

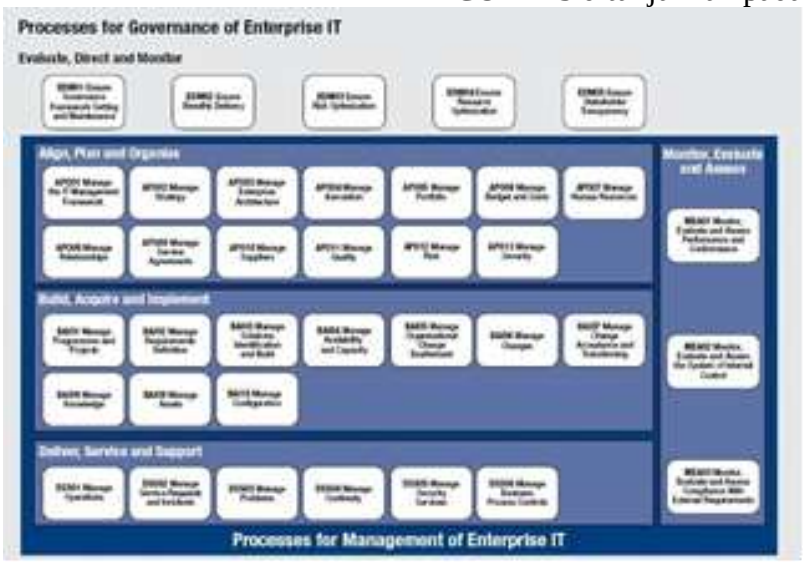
COBIT 5 adalah kerangka yang dapat membantu perusahaan dalam mencapai tujuannya dalam tata kelola serta memanajemen TI perusahaan. Secara umum COBIT 5 dapat membantu perusahaan dalam menciptakan nilai optimal dari sebuah TI dengan cara menjaga keseimbangan antara mendapatkan keuntungan dan mengoptimalkan tingkat resiko dan penggunaan sumber daya yang ada [7].

COBIT 5 memiliki lima prinsip dasar seperti ditunjukkan pada gambar 2.



Gambar 2. Prinsip-prinsip COBIT 5
Sumber : [7]

COBIT 5 mengidentifikasi seperangkat enabler tata kelola dan manajemen yang mencakup 37 proses. Di area tata kelola (governance), ada lima proses di domain Evaluate, Direct and Monitor (EDM). Ada empat domain yang didefinisikan di area manajemen (management): Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); Monitor, Evaluate and Assess (MEA). Berikut merupakan domain dan proses (sub domain) dalam COBIT 5 ditunjukkan pada gambar 3.



Gambar 3. COBIT 5 *process reference* model [8]

Deliver, Service, and Support yang biasa dikenal dengan singkatan DSS merupakan salah satu domain di *framework* COBIT 5. Domain ini merupakan perluasan dari domain *Deliver and Support* (DS) pada versi COBIT sebelumnya, yakni COBIT 4.1. Domain DSS menitik beratkan pada

proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan, dan pengelolaan data yang sedang berjalan. Domain DSS terdiri dari 6 sub proses dan 38 sub-sub proses, serta 204 aktivitas yang dilakukan pada domain ini [9].

Deliver, Service and Support (DSS) domain ini mempunyai 6 proses sebagai berikut:

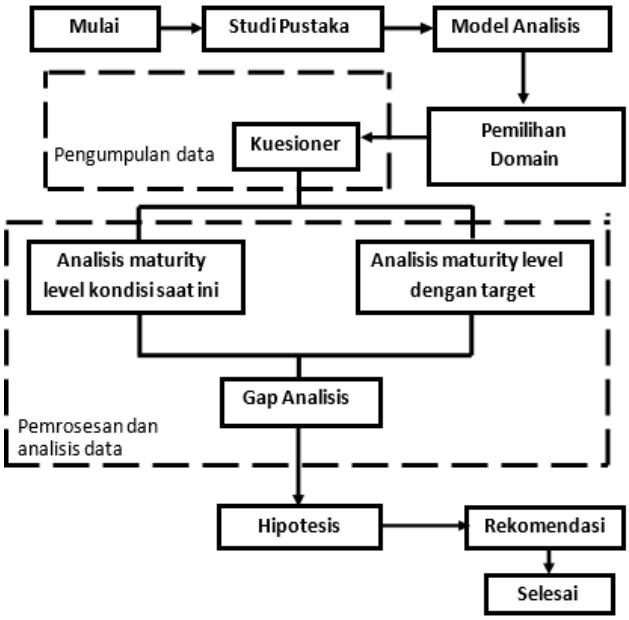
1. DSS01: *Manage operations.*
2. DSS02: *Manage service request and incidents.*
3. DSS03: *Manage Problem.*
4. DSS04: *Manage continuity.*
5. DSS05: *Manage security services.*
6. DSS06: *Manage business process controls.*

Dalam penelitian ini penulis menggunakna domain DSS05: *Manage security services*, dimana *process goals and matrics* dari metode COBIT 5 dengan domain DSS05 yaitu sebagai berikut:

1. DSS05.01 Protect against malware
   Melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama patch keamanan dan pengendalian virus terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dan perangkat lunak perusak (mis, virus, worm, spyware, spam).
2. DSS05.02 Manage network and connectivity security
   Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas.
3. DSS05.03 Manage endpoint security
   Pastikan titik akhir (misal, laptop, desktop, server, dan perangkat seluler dan jaringan seluler atau perangkat lunak lainnya) dijamin pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang ditetapkan dari informasi yang diproses, disimpan atau dikirim.
4. DSS05.04 Manage user identity and logical access
   Pastikan semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis mereka dan berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis.
5. DSS05.05 Manage physical access to IT assets
   Tentukan dan terapkan prosedur untuk memberi, membatasi dan mencabut akses kebangunan, bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses kebangunan, bangunan dan area harus dibenarkan, disahkan, dicatat dan dipantau. Ini harus berlaku untuk semua orang yang memasuki tempat itu, termasuk staf, staf sementara, klien, vendor, pengunjung atau pihak ketiga lainnya.
6. DSS05.06 Manage sensitive documents and output device
   Manatapkan pengamanan fisik, praktik akuntansi dan pengolahan persedian yang tepat atas aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau token keamanan.
7. DSS05.07 Manage the infrastructure for security-related events
8. Menggunakan alat deteksi intrusi, memantau infrastruktur untuk akses yang tidak sah dan memastikan bahwa setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian secara umum.

III. METODOLOGI PENELITIAN

3.1 Kerangka penelitian



Gambar 4. Tahapan Penelitian

Kerangka berpikir digunakan untuk menjelaskan pola antar teori dan objek dalam penelitian. Pemikiran dimulai dari latar belakang penelitian, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian. Konsep tersebut kemudian merujuk pada studi pustaka sebagai dasar yang akan digunakan sebagai acuan penelitian, adapun studi pustaka yang dibutuhkan adalah literatur dan penelitian relevan. Setelah studi pustaka kemudian metode analisis, analisa yang dilakukan menggunakan analisa kuantitatif berdasar kan pengolahandata dari standar COBIT 5 dan dikombinasikan dengan metode CMMI. Pemilihan domain yang digunakan pada COBIT 5 yaitu domain Deliver, Service and Support (DSS) dengan sub-domain DSS05 dan dikombinasikan dengan kriteria pada capability level CMMI, kemudian pengumpulan data kuesioner dan menyebarkan kuesioner dengan membuat daftar pertanyaan berdasarkan standar yang termuat dalam COBIT 5 tentang instruksi pelaksanaan manajemen keamanan.

Setelah itu analisis maturity level atau analisis tingkat kematangan keamanan saat ini pada AMS Universitas Bina Insan dan menganalisis kesenjangan (gap) dengan menghitung maturity saat ini dengan target. Kemudian memberikan hipotesis dari penelitian yang akan dilakukan. Dan menyusun rekomendasi tata kelola keamanan Academic Management System (AMS) Universitas Bina Insan Lubuklinggau.

Kerangka berpikir digunakan untuk menjelaskan pola antar teori dan objek dalam penelitian. Pemikiran dimulai dari latar belakang penelitian, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian. Konsep tersebut kemudian merujuk pada studi pustaka sebagai dasar yang akan digunakan sebagai acuan penelitian, adapun studi pustaka yang dibutuhkan adalah literatur dan penelitian relevan. Setelah studi pustaka kemudian metode analisis, analisa yang dilakukan menggunakan analisa kuantitatif berdasar kan pengolahandata dari standar COBIT 5 dan dikombinasikan dengan metode CMMI. Pemilihan domain yang digunakan pada COBIT 5 yaitu domain *Deliver, Service and Support* (DSS) dengan sub-domain DSS05 dan dikombinasikan dengan kriteria pada *capability level* CMMI, kemudian pengumpulan data kuesioner dan menyebarkan kuesioner dengan membuat daftar pertanyaan berdasarkan standar yang tersaji dalam COBIT 5 tentang perintah pelaksanaan manajemen keamanan.

Setelah itu analisis *maturity level* atau analisis tingkat kematangan keamanan saat ini pada AMS Universitas Bina Insan dan menganalisis kesenjangan (gap) dengan menghitung *maturity* saat ini dengan target. Kemudian memberikan hipotesis dari penelitian yang akan dilakukan. Dan menyusun rekomendasi tata kelola

keamanan *Academic Management System* (AMS) Universitas Bina Insan Lubuklinggau.

3.2 Metode COBIT 5

Disetiap domain COBIT memiliki beberapa pembahasan yang sudah ditetapkan pada metode tersebut dan memiliki variabel yang didalamnya sudah terdapat aktivitas atau pernyataan dari setiap sub-domain. Dibawah ini akan memberi penjelasan apa saja yang ada di dalam domain DSS.

Deliver, Service and Support (DSS) domain ini mempunyai 6 proses sebagai berikut:

1. DSS01: *Manage operations.*
2. DSS02: *Manage service request and incidents.*
3. DSS03: *Manage Problem.*
4. DSS04: *Manage continuity.*
5. DSS05: *Manage security services.*
6. DSS06: *Manage business process controls.* DSS06: Manage business process controls.

Pada penelitian ini akan berfokus pada domain DSS dengan sub-domain DSS05 yang membahas tentang keamanan sistem informasi.

3.3 Metode Capability Maturity Model Integration (CMMI)

Metode ini digunakan untuk proses penilaian dari skala kemampuan dan kematangan pada sebuah sistem. Pada skala kemampuan atau *capability level* digunakan untuk alur proses penilaian secara berjenjang. Penilaian tersebut didasarkan pada kuesioner yang ditentukan dari standar COBIT 5 dan dinilai dengan menggunakan tingkat kemampuan pada CMMI. Dibawah ini merupakan acuan penilaian *capability level* yang akan digunakan untuk menjawab semua pernyataan dari kuesioner yang sudah dibuat yaitu sebagai berikut :

a. Level 0: Tidak lengkap (*Incomplete*): Pendekatan tidak lengkap untuk memenuhi maksud dari area praktek.
b. Level 1: Dilakukan (*Performed*): Pendekatan awal untuk memenuhi maksud dari area praktik.
c. Level 2: Dikelola (*Managed*): Berlaku praktik level 1. Praktik yang sederhana, tetapi lengkap yang membahas maksud penuh dari area praktik.
d. Level 3: Ditetapkan (*Defined*): Dibangun pada praktik level 2. Menggunakan standar organisasi dan menyesuaikan untuk mengatasi karakteristik proyek dan pekerjaan. Berfokus pada pencapaian tujuanproyek dan kinerja organisasi.
e. Level 4: Dikelola secara kuantitatif (*Quantitatively Managed*): Dibangun pada praktik level 3. Menggunakan teknik kuantitatif statistik dan lainnya untuk memahami variasi kinerja dan mendeteksi, memperbaiki, atau memprediksi area fokus untuk mencapai kualitas dan tujuan kinerja proses.
f. Level 5: Mengoptimalkan (*Optimizing*): Dibangun pada praktik level 4. Menggunakan teknik kuantitatif statistik dan lainnya untuk mengoptimalkan kinerja dan peningkatan untuk mencapai kualitas dan tujuan kinerja proses

IV. HASIL DAN PEMBAHASAN

4.1 Hasil

1 *Maturity Level*

Dari hasil penelitian diatas dapat ditetapkan nilai keseluruhan dengan tingkatan *maturity level* dari keseluruhan aktivitas yang dilakukan dalam DSS05 dengan persamaan sebagai berikut:

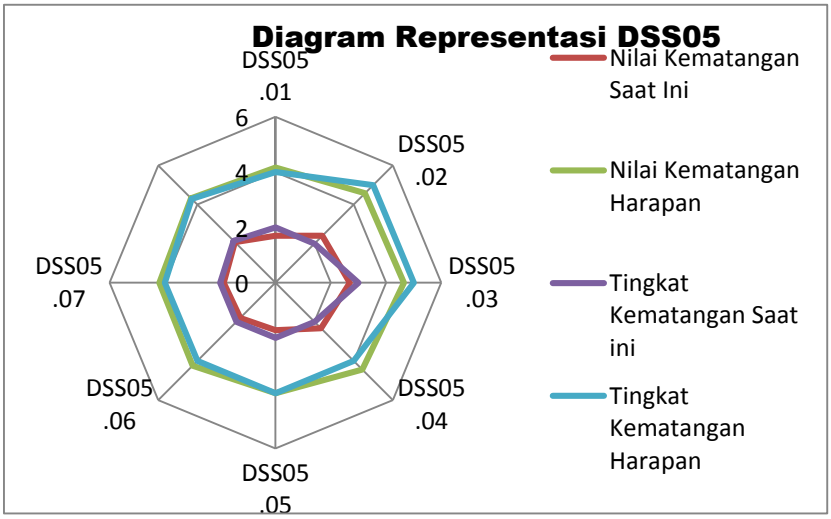
$$Maturitly\ evel\ DSS05 = \frac{\Sigma\ \text{Maturity level}}{Banyak\ proses}$$

Tabel 1 Hasil rekapitulasi keseluruhan data *maturity level*

No	Sub Proses	Nilai Kematangan		Tingkat Kematangan	
		Saat Ini	Harapan		
1	DSS05.01	1,7	4,167	2	4
2	DSS05.02	2,4	4,578	2	5
3	DSS05.03	2,689	4,644	3	5
4	DSS05.04	2,325	4,45	2	4
5	DSS05.05	1,714	4	2	4
6	DSS05.06	1,8	4,24	2	4
7	DSS05.07	1,88	4,2	2	4
Rata-rata		2,073	4,326	2,143	4,286

Dari tabel di atas dapat disimpulkan bahwa pada proses DSS05 (*Manage security services*) tentang keamanan *Academic Management System* di Universitas Bina Insan untuk kondisi saat ini (*as is*) memperoleh nilai 2,073 atau bisa dikatakan berada di tingkat kemampuan level 2 yaitu *Repeatable But Invinitive*. Artinya pada proses DSS05 (*Manage security services*) pada *Academic Management System* di Universitas Bina insan sudah adanya proses yang dikembangkan dengan adanya prosedur yang sama dan digunakan oleh banyak orang dalam menyelesaikan tugas. Dan juga belum ada penetapan prosedur untuk pelatihan secara resmi ataupun komunikasi dan tangung jawab bergantung pada individu. Tingkat kepercayaan pada kemampuan individu sangat tinggi, sehingga kesalahan yang sama sering kali terjadi.

Sedangkan, untuk kondisi yang diharapkan (*to be*) pada proses DSS05 (*Manage security services*) tentang keamanan *Academic Management System* di Universitas Bina Insan memperoleh nilai 4,326 dengan tingkat kematangan level 4 yang dimana pada tahap ini harus diterapkan *Managed and Measurable*. Artinya pada keamanan sistem menggunakan proses DSS05 (*Manage security services*) di Universitas Bina Insan diharapkan terdapat adanya manajemen, memonitor dan mengukur kepatuhan dengan prosedur dan mengambil tindakan terhadap proses yang tampaknya tidak dapat bekerja secara efektif.



Gambar 5. Diagram representasi DSS05

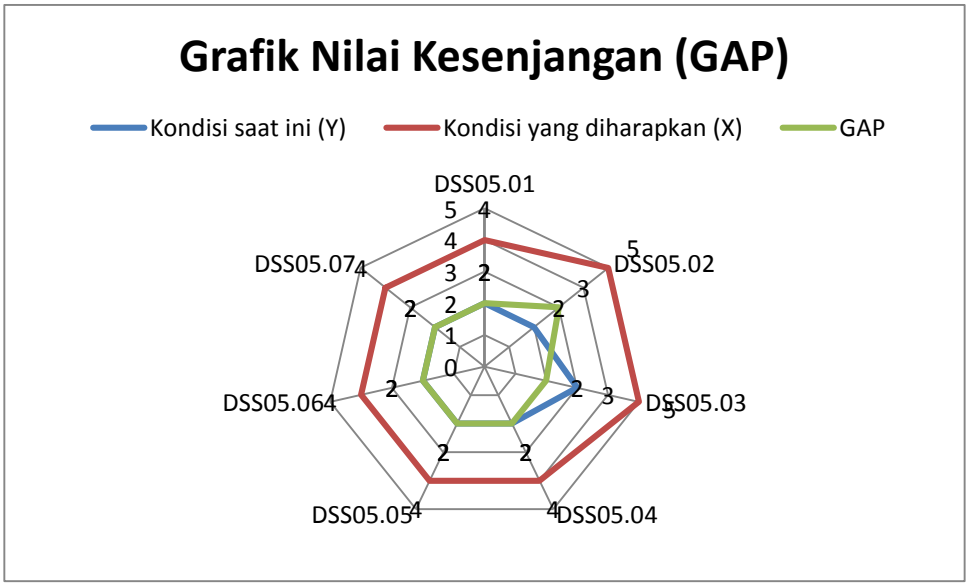
2 Nilai Kesenjangan (GAP)

$$\text{Tingkat kesenjangan} = X - Y$$

Keterangan :
X = Tingkat kematangan yang diharapkan (*to-be*)
Y = Tingkat kematangan saat ini (*as is*)

Tabel 2 Nilai kesenjangan (GAP)

No	Sub Proses	Tingkat Kematangan		GAP	*Maturity level*
		Y	X		
1	DSS05.01	2	4	**2**	*Repeatable but invinitve*
2	DSS05.02	2	5	**3**	*Define Process*
3	DSS05.03	3	5	**2**	*Repeatable but invinitve*
4	DSS05.04	2	4	**2**	*Repeatable but invinitve*
5	DSS05.05	2	4	**2**	*Repeatable but invinitve*
6	DSS05.06	2	4	**2**	*Repeatable but invinitve*
7	DSS05.07	2	4	**2**	*Repeatable but invinitve*
Rata-rata		2,143	4,286	**2,143**	*Repeatable but invinitve*



Gambar 6. Grafik nilai kesenjangan (GAP)

4.2 Pembahasan

Pada topik pembahasan ini akan menjelaskan hasil penelitian yang didapatkan dari perhitungan tingkat level kematangan (*maturity level*) pada *Academic Management System* di Universitas Bina Insan Lubuklinggau. Dari hasil rekapitulasi keseluruhan perhitungan setiap sub domain DSS05 maka dapat diketahui hasil temuan, gap (kesenjangan) dan rekomendasi. Pada bagian berikutnya akan menjelaskan setiap hasil temuan, gap dan rekomendasi dalam bentuk tabel.

1. Temuan, Gap dan Rekomendasi Proses DSS05

Tabel 3 Temuan, Gap dan Rekomendasi DSS05.01

DSS05.01 - *Protect against malware*		
Nilai Kesenjangan Tingkat 2		
Temuan	**GAP**	**Rekomendasi**
Adanya perlindungan perangkat lunak terhadap malware (perangkat lunak perusak) menggunakan *software* proteksi dengan menggunakan konfigurasi yang aman.	Belum ada standarisasi prosedur pelatihan secara formal dan komunikasi dalam memelihara dan perbaikan sistem untuk melindungi sistem informasi dari malware (perangkat lunak perusak).	Universitas Bina Insan direkomendasikan untuk memberikan pelatihan yang baik, memanajemen, memonitoring dan menghitung kepatuhan dengan prosedur dan mengambil tindakan terhadap proses yang tidak dapat bekerja secara efektif.

Tabel 4 Temuan, Gap dan Rekomendasi DSS05.02

DSS05.02 - *Manage network and connectivity security*		
Nilai Kesenjangan Tingkat 3		
Temuan	**GAP**	**Rekomendasi**
Adanya langkah-langkah seperti menetapkan mekanisme penyaringan jaringan, menerapkan mekanisme terpercaya untuk penerimaan informasi yang aman, memelihara kebijakan untuk keamanan konektivitas.	Mekanisme yang ditetapkan belum diterapkan secara teratur dan prosedur yang digunakan pada sistem keamanan Universitas Bina Insan belum memadai tetapi digubakan pada praktek.	Universitas Bina Insan direkomendasikan untuk menerapkan secara teratur mekanisme yang telah ditetapkan, menyediakan keperluan untuk meningkatkan efektivitas dan kualitas dan menyempurnakan ketingkat praktek yang baik.

Tabel 5 Temuan, Gap dan Rekomendasi DSS05.03

DSS05.03 - *Manage endpoint security*		
Nilai Kesenjangan Tingkat 2		
Temuan	**GAP**	**Rekomendasi**
Memastikan alat-alat seperti laptop, deskop, server, dan perangkat komputer lainnya dijamin pada tingkat yang memenuhi persyaratan keamanan.	Belum adanya standarisasi alat-alat jaringan mengenai pengolahan dan persyaratan keamanan yang ditetapkan dari pihak informasi keamanan pada Universitas Bina Insan.	Universitas Bina Insan direkomendasikan untuk menyediakan peralatan guna meningkatkan efektivitas dan kualitas, membuat organisasi cepat berdaptasi. Dan teknologi informasi digunakan secara terintegritas untuk mengotomatisasi alur kerja.

Tabel 6 Temuan, Gap dan Rekomendasi DSS05.04

DSS05.04 - *Manage user identity and logical access*		
Nilai Kesenjangan Tingkat 2		
Temuan	**GAP**	**Rekomendasi**

Semua pengguna di Universitas Bina Insan memiliki wewenang untuk menggunakan sistem informasi akademik sesuai dengan kebutuhan dan koordinasi dengan tim ICT tersebut.	Tingkat kepercayaan pada pengguna sangat tinggi, sehingga kesalahan yang sama sering kali terjadi.	Universitas Bina Insan direkomendasikan untuk memonitoring dan mengukur kepatuhan setiap pengunjung dengan prosedur. Dan melakukan pelatihan secara formal kepada semua pengunjung terkhusus kepada tim yang mengelola sistem tersebut.

Tabel 7 Temuan, Gap dan Rekomendasi DSS05.05

DSS05.05 - *Manage physical access to IT assets*		
Nilai Kesenjangan Tingkat 2		
Temuan	**GAP**	**Rekomendasi**
Tim ICT Universitas Bina Insan menerapkan prosedur untuk mencabut akses ke sistem, membatasi dan memberi. Input ke sistem harus dipantau, dicatat, disahkan dan dibenarkan berlaku untuk semua orang yang memasuki sistem tersebut.	Belum adanya standarisasi penerapan seperti yang dijelaskan pada temuan tersebut.	Universitas Bina Insan direkomendasikan untuk menerapkan prosedur dan mengambil tindakan terhadap akses yang akan masuk kedalam sistem.

Tabel 8 Temuan, Gap dan Rekomendasi DSS05.06

DSS05.06 - *Manage sensitive documents and output devices*		
Nilai Kesenjangan Tingkat 2		
Temuan	**GAP**	**Rekomendasi**
Tim ICT Universitas Bina Insan melakukan pengolahan persediaan seperti inventaris dokumen dan perangkat *output* yang sensitif, dan melakukan rekonsiliasi reguler.	Belum adanya standarisasi pengolahan dokumen dan perangkat pengeluaran sensitif.	Universitas Bina Insan direkomendasikan untuk mengatur manajemen kerja pada data dokumen penting dalam sistem informasi akademik tersebut

Tabel 9 Temuan, Gap dan Rekomendasi DSS05.07

DSS05.07 - *Manage the infrastructure for security-related events*		
Nilai Kesenjangan Tingkat 2		
Temuan	**GAP**	**Rekomendasi**
Tim ICT Universitas Bina Insan secara teratur melakukan peninjauan log peristiwa untuk kejadian potensial.	Belum adanya standarisasi dalam melakukan peninjauan log peristiwa untuk kejadian potensial.	Universitas Bina Insan direkomendasikan untuk menerapkan prosedur dalam mencatat semua peristiwa yang terjadi pada sistem tersebut.

Dari hasil temuan, gap dan rekomendasi dapat diketahui bahwasannya pada sistem keamanan yang ada pada *Academic Management System* perlu di

perbaiki lagi dan dikembangkan sesuai dengan rekomendasi yang diberikan pada setiap sub domain DSS05. Hal ini dilakukan untuk memperbaiki dan membantu proses keamanan pada AMS di Universitas Bina Insan agar mencapai tingkat level keamanan yang paling optimal atau sangat baik.

V. KESIMPULAN

Berdasarkan rangkuman skripsi yang telah dijelaskan dalam halaman sebelumnya terkait analisis tingkat level keamanan *Academic Management System* Universitas Bina Insan, maka didapatkan kesimpulan sebagai berikut.

Dari hasil rekapitulasi keseluruhan perhitungan menggunakan rumus *maturity level* yang sudah ditetapkan maka dapat diketahui bahwasannya tingkat level keamanan pada *Academic Management System* (AMS) Universitas Bina Insan Lubuklinggau melalui sub domain yang digunakan yaitu DSS05 pada kondisi saat ini (*As is*) memperoleh nilai 2,143 atau bisa dikatakan berada di tingkat kemampuan level 2 yaitu *Repeatable But Invinitive*. Artinya keamanan sistem di Universitas Bina insan belum ada standarisasi prosedur untuk pelatihan secara formal ataupun komunikasi dan tanggung jawab bergantung pada individu. Tingkat kepercayaan pada kemampuan individu sangat tinggi, sehingga kesalahan yang sama sering kali terjadi. Sedangkan, untuk kondisi yang diharapkan (*to be*) memperoleh nilai 4,286 dengan tingkat kematangan level 4 yang dimana pada tahap ini harus diterapkan *Managed and Measurable*. Dapat di artikan bahwa pada keamanan sistem menggunakan proses DSS05 (*Manage security services*) di Universitas Bina Insan diharapkan terdapat adanya mengambil tindakan, mengukur kepatuhan dengan prosedur, memonitor dan memanajemen proses yang tampaknya tidak dapat bekerja secara efektif.

Nilai kesenjangan antara tingkat kematangan 2 dengan tingkat kematangan 4 terdapat nilai *gap* sebesar 2,143. Hal tersebut menunjukkan bahwa Universitas Bina Insan harus memenuhi standarisasi untuk melakukan pelatihan secara formal dan komunikasi yang bagus bagi tim pengelola sistem keamanan tersebut.

VI. DAFTAR PUSTAKA

[1] Y. Anggraini, D. Pasha, and A. Setiawan, "Sistem Informasi Penjualan Sepeda Berbasis Web Menggunakan Framework Codeigniter (Studi Kasus : Orbit Station)," *J. Teknol. dan Sist. Inf.*, vol. 1, no. 2, pp. 64–70, 2020.

[2] R. Pinanjar, "SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK CODEIGNITER PADA SMKN 1 TRIMURJO," Universitas Teknokrat Indonesia, 2019.

[3] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019, doi: 10.21456/vol9iss1pp47-54.

[4] S. Samsinar, R. Sinaga, and R. Afriany, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 (Studi Kasus: STIKES Garuda Putih Jambi)," *J. Media Inform. Budidarma*, vol. 5, no. 1, p. 138, 2021, doi: 10.30865/mib.v5i1.2573.

[5] R. Gunawan and D. Tjahjadi, "Audit Sistem Informasi Akademik Berbasis Web Menggunakan Framework Cobit 5.0 Pada Domain Apo13 Dan Dss05 (Studi Kasus: SIAT STMIK ROSMA

KARAWANG)," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 13, no. 3, pp. 29–40, 2018, doi: 10.35969/interkom.v13i3.35.

[6] A. Ramadhani, "Keamanan Informasi," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, p. 39, 2018, doi: 10.30999/n-jils.v1i1.249.

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

[8] ISACA, *A Business Framework for the Governance and Management of Enterprise IT*, United Sta. ISACA, 2012.

[9] K. C. Johanes Fernandes Andry, *Audit Menggunakan Cobit 4.1 dan Cobit 5 dengan Case Study*. Yogyakarta: Teknosain, 2018.