

Kajian Keamanan Sistem Informasi Akademik Menggunakan *Framework* COBIT 5

Yonal Supit^{a,1,*}, Edy Irwansyah^{b,2}

^aUniversitas Bina Nusantara, Jakarta-Indonesia

^bUniversitas Bina Nusantara, Jakarta-Indonesia

¹Email yonal.supit@binus.ac.id, ²Email eirwansyah@binus.edu

*Penulis koresponden

Diterima	Direvisi	Disetujui	Dipublikasikan
19/3/2024	23/3/2024	1/4/2024	22/5/2024

ABSTRACT

This study examines the security of academic information systems using the COBIT 5 Framework. Key issues are uncertainty in protecting student and staff data, the potential for cyberattack vulnerabilities, and non-compliance with international security standards. The goal is to evaluate the security level of the system and suggest improvement recommendations according to COBIT 5 principles. Research methods include Renstar IT policy analysis, system audits, and interviews with IT personnel and related academic communities. Data is analyzed quantitatively to identify weaknesses and opportunities for improvement. The COBIT 5 framework is used as a security assessment framework. The results highlight the need for improvement, including access management, activity monitoring, and continuous improvement plans. Using COBIT 5, substantial measures such as strengthening access controls and developing disaster recovery plans can be identified. The research emphasizes the importance of a structured approach in improving the security of academic information systems, with COBIT 5 as a useful tool. With the right measures, system security can be enhanced to protect the integrity, confidentiality, and availability of critical data for educational institutions. In conclusion, these measures demonstrate how important COBIT 5 implementation is in addressing information security challenges in academic environments.

KEYWORDS

1. Security
2. Information System
3. COBIT 5
4. Evaluation
5. Maturity Level

ABSTRAK

Kajian ini memeriksa keamanan sistem informasi akademik dengan menggunakan Framework COBIT 5. Permasalahan utama adalah ketidakpastian dalam melindungi data mahasiswa dan staf, sangat berpotensi terhadap kerentanan serangan siber, dan ketidaksesuaian dengan standar keamanan internasional. Tujuannya adalah mengevaluasi tingkat keamanan sistem dan memberikan saran rekomendasi perbaikan sesuai prinsip-prinsip COBIT 5. Metode penelitian mencakup analisis kebijakan Renstar TI, audit sistem, dan wawancara dengan personel IT serta civitas akademik terkait. Data dianalisis secara kuantitatif untuk mengidentifikasi kelemahan dan peluang perbaikan. Framework COBIT 5 digunakan sebagai kerangka kerja penilaian keamanan. Hasilnya menyoroti perlunya peningkatan, termasuk manajemen akses, pemantauan aktivitas, dan rencana perbaikan berkelanjutan. Dengan menggunakan COBIT 5, langkah-langkah substansial seperti penguatan kontrol akses dan penyusunan rencana pemulihan bencana dapat diidentifikasi. Penelitian ini menekankan pentingnya pendekatan terstruktur dalam meningkatkan keamanan sistem informasi akademik, dengan COBIT 5 sebagai alat yang berguna. Dengan tindakan yang tepat, keamanan sistem dapat ditingkatkan untuk melindungi integritas, kerahasiaan, dan ketersediaan data penting bagi institusi pendidikan. Kesimpulannya, langkah-langkah ini menunjukkan betapa pentingnya implementasi COBIT 5 dalam menangani tantangan keamanan informasi di lingkungan akademik.

KATA KUNCI

1. Keamanan
2. Sistem Informasi
3. COBIT 5
4. Evaluasi
5. Tingkat Kematangan

This is an open access article under the CC-BY-SA license.



1 PENDAHULUAN

Di era *system* digital digital ini, Sistem Informasi Akademik (SIA) peristiwa yang pokok buat hukum pembelajaran untuk mengurus serta sediakan data terikat layanan mahasiswa, layanan akademik, serta administrasi institusi dengan teknik realistik. akan tetapi, keberhasilan serta keberlanjutan SIA tidak semata-mata terkait pada fungsionalitasnya namun pula amat terikat dengan keamanan sistem data itu. ancaman keamanan data sejenis akses tidak , agresi malware, manipulasi data diri, serta kendala layanan mampu mudarat integritas, kerahasiaan, serta ketersediaan data yang dielola oleh SIA. Oleh gara-gara itu, riset ini bertekad guna menjalankan tinjauan mendalam keamanan SIA dengan menggunakan pendekatan *Framework* COBIT 5.

Dimasa sekarang, sebagian besar bisnis bergantung sepenuhnya pada informasi seperti data keuangan agar bisnis perbankan dapat bertahan dan menjadi lebih kompetitif (Knapp et al., 2006). Menurut thycotic, 62 % dari seluruh ancaman siber berdampak pada usaha kecil dan menengah, dan 60 % di antaranya mengalami masalah yang sangat serius sehingga berdampak pada penutupan usaha pasca serangan tersebut (Thycopic Software Ltd., 2017). 53% serangan menyebabkan \$500.000 atau lebih (Cisco Systems Inc., 2018) sebaliknya kerugian rata-rata disebabkan akibat dari pelanggaran data adalah \$3,86 juta (Ponemon Institute LLC, 2018). Tidak hanya kerugian finansial yang menjadi risiko namun juga dampak hukum dan reputasi (Tu & Yuan, 2014). Oleh karena itu, setiap organisasi perlu menjaga keamanan dan kerahasiaan informasi dan teknologi yang menjadi penyebab utama dari serangan yang merugikan bisnis [1].

Untuk mengidentifikasi serta mengatasi ancaman keamanan, penting untuk memahami layanan keamanan informasi yang terus berkembang pesat. Serangan-serangan yang sering terjadi seperti *phishing*, *malware*, dan serangan *DDoS* dapat mengakibatkan kerugian finansial serta berdampak pada buruknya reputasi perusahaan, serta ketidakstabilan operasional. Selain itu, dalam konteks SIA, informasi yang berkaitan dengan data mahasiswa, hasil ujian, dan proses akademik menjadi target yang sangat bernilai bagi para pelaku kejahatan. Oleh karena itu, mengidentifikasi

dan mengevaluasi potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan data di SIA menjadi langkah awal yang penting dalam menjaga keamanan Sistem Informasi Akademik.

Pemanfaatan Framework COBIT 5 dalam analisis keamanan SIA memberikan pendekatan yang lengkap serta teratur. COBIT 5, selaku kerangka aktivitas manajemen serta pengawasan teknologi data, menawarkan arahan yang kokoh buat mengatur akibat, meyakinkan keamanan, serta memaksimalkan harga dari pemodal teknologi data. Dengan menggunakan prinsip-prinsip COBIT 5, penelitian ini menyurvei daya guna tata Kelola TI terhadap kondisi keamanan SIA. penilaian ini meliputi prosedur rekognisi, penghitungan, serta penindakan akibat yang barangkali timbul terikat dengan keamanan data. Audit kepada proses-proses kunci dalam SIA bakal jadi bagian integral dari analisis ini.

Melalui implementasi COBIT 5, prosedur audit hendak berfokus pada pengukuran kapabilitas dan kematangan terhadap kontrol keamanan yang telah diidentifikasi oleh *framework* COBIT. Hal ini meliputi pengukuran efektivitas kontrol, penilaian kepatuhan terhadap kebijakan keamanan yang ada, dan identifikasi potensi area perbaikan. Dengan demikian, kajian ini tidak hanya akan mengidentifikasi kekurangan keamanan tetapi juga memberikan wawasan tentang implementasi *best practices* dalam manajemen keamanan SIA. Hasil kajian ini diharapkan dapat memberikan rekomendasi konkret untuk meningkatkan keamanan SIA. Rekomendasi perbaikan dan peningkatan akan didasarkan pada temuan audit, evaluasi manajemen risiko, dan analisis potensi ancaman keamanan. Selain itu, rekomendasi tersebut akan diarahkan pada penerapan *best practices* COBIT 5 yang sesuai dengan konteks SIA.

Penerapan rekomendasi ini diharapkan dapat meningkatkan tingkat keamanan SIA, mengurangi risiko, dan memberikan dasar yang kokoh bagi kelangsungan operasional lembaga pendidikan. Secara keseluruhan, kajian keamanan SIA menggunakan framework COBIT 5 bertujuan untuk memberikan kontribusi positif terhadap pengelolaan keamanan informasi dilembaga pendidikan. Dengan mengintegrasikan pendekatan COBIT 5, penelitian ini akan meningkatkan landasan yang kokoh untuk mengatasi ancaman-ancaman keamanan yang dihadapi oleh SIA. Keberhasilan implementasi rekomendasi yang dihasilkan dari kajian ini akan mencerminkan komitmen lembaga pendidikan untuk melindungi integritas, kerahasiaan, dan ketersediaan data yang menjadi bagian krusial dari Sistem Informasi Akademik. Teknologi Informasi di suatu perguruan tinggi merupakan sebuah konsep yang menjawab kebutuhan organisasi akan jaminan pengembalian investasi TI yang diinvestasikan. Tanpa tata kelola TI, risiko investasi TI dan kegagalan layanan dapat terjadi. Sebagian besar tata kelola TI pada perguruan tinggi masih belum dilakukan secara maksimal [2].

Penggunaan tata kelola teknologi informasi pada suatu institusi, termasuk perguruan tinggi, memerlukan bantuan beberapa *tools* berupa kerangka tata kelola teknologi informasi yang komprehensif, yang bertujuan untuk memberikan pedoman bagi para pemimpin dalam mengelola informasinya [3, p. 5]. Banyak sekali faktor yang mempengaruhi keamanan informasi, di antaranya adalah risiko, organisasi, kebiasaan, pelatihan, pilihan tata kelola, kerangka kerja, teknologi/infrastruktur, sumber daya manusia, proses, informasi, aplikasi/layanan, kebijakan/prinsip dan manajemen [4].

Hadirnya teknologi informasi telah mengubah cara berbisnis saat ini dalam lingkungan yang kompetitif. Harmonisasi antara bisnis dan TI melahirkan skema tata kelola teknologi informasi (ITG). ITG adalah sub-bagian tata kelola Institusi untuk mengarahkan dan mengendalikan semua aktivitas Institusi yang terkait dengan TI. Perihal memastikan apabila seluruh kegiatan itu selaras dengan strategi Institusi, memberikan nilai, mempertimbangkan risiko, mengelola sumber daya, dan mengelola kinerja. Beberapa kerangka kerja diusulkan untuk pengelolaan dan pengendalian TI, misalnya. ITIL, PMbok, COSO, ISO 27001, CMMI, Six Sigma. Kerangka kerja paling komprehensif yang memberikan pengendalian dalam bentuk tata kelola dan manajemen terhadap seluruh aktivitas utama terkait TI adalah *Control Objectives for Information and Technology* (COBIT) [5, p. 5].

Pengawasan yang efektif memungkinkan manajemen untuk memanfaatkan seluruh sumber daya Institusi secara efektif, untuk melengkapi tanggung jawabnya dan untuk mengoptimalkan keandalan dan pemanfaatan informasi yang diperoleh. Pengawasan internal memainkan peran besar dalam membantu manajer organisasi meningkatkan keandalan data, mendeteksi dan mengontrol

aktivitas Institusi, mencegah kesalahan dan membantu audit internal dan eksternal dalam melakukan control TI [6].

2 METODE PENELITIAN

2.1 Alat Penelitian

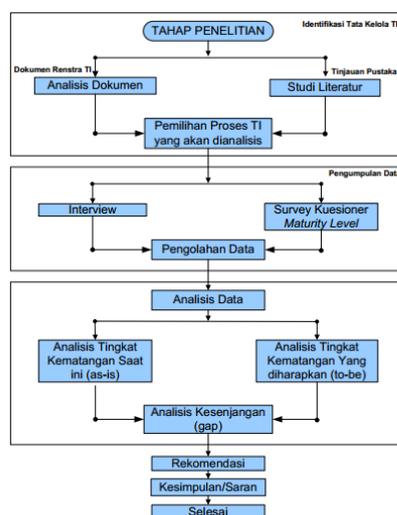
Dalam penelitian ini alat yang digunakan untuk menganalisa tata kelola TI di Perguruan Tinggi agar bisa memadai dalam penggunaannya dalam rangka pengembangan TI adalah COBIT 5 yang dikeluarkan oleh ISACA dan ITGI (*the IT Governance Institute*). COBIT merupakan sebuah kerangka kerja penilaian SI yang bersifat generik, artinya COBIT bisa diimplementasikan diberbagai bentuk organisasi bisnis termasuk lembaga pendidikan tinggi, namun penggunaannya harus disesuaikan dengan tujuan dan kondisi organisasi. Selain itu COBIT dapat digunakan untuk memeriksa pengelolaan (audit) seluruh sumber daya TI, sehingga dapat diketahui faktor apa saja yang menghambat dan mendukung pengembangan TI di Perguruan Tinggi. Tahap selanjutnya adalah proses pengolahan data setelah data diolah lalu dilakukan analisis data sesuai dengan domain yang dipilih menggunakan *framework* COBIT. Hasil analisis data diharapkan dapat mengetahui kesenjangan (*gap*) kondisi saat ini dan tujuan yang akan dicapai (*to-be*) dalam melaksanakan tata kelola TI yang baik guna mengembangkan TI Perguruan Tinggi. Dari hasil temuan analisis akan diberikan rekomendasi peningkatan pencapaian sesuai *framework* COBIT 5. Dan Tahap akhir adalah pembuatan kesimpulan dari hasil analisis penelitian yang sudah dilakukan.

2.2 Tahapan Penelitian

Pertama yang dilakukan sebelum melakukan penelitian ini adalah melakukan perumusan masalah mengumpulkan permasalahan yang ditemukan dan disatukan dalam suatu pertanyaan penelitian. Selanjutnya pertanyaan penelitian ini digunakan sebagai pedoman, penentuan arah atau fokus dari penelitian, kemudian dilanjutkan dengan perbandingan *literatur review* jurnal-jurnal atau penelitian-penelitian terdahulu yang mendukung proses penelitian ini, lalu dilakukan formulasi dari permasalahan yang ada, formulasi ini dalam bentuk pertanyaan yang kemudian akan diuji melalui penelitian. Tahap selanjutnya setelah diformulasikan permasalahan lalu dilakukan pengumpulan data yang dibutuhkan dalam penelitian ini, cara pengumpulan data dalam penelitian ini dengan melakukan observasi langsung ke objek penelitian melalui interview dan penyebaran kuesioner kepada masing-masing responden.

2.3 Alur Proses Penelitian

Dalam penelitian ini setiap tahapan akan disesuaikan dengan kerangka kerja COBIT. Berdasarkan tahap-tahap yang ada pada COBIT diharapkan dapat mengetahui tingkat kematangan dan kapabilitas dari tata kelola Teknologi Informasi. Secara lengkap tahapan penelitian digambarkan pada Gambar 1.



Gambar 1 Tahapan Proses Penelitian

2.3.1 Metode Pengumpulan Data

Pada penelitian ini menggunakan metode kuesioner dengan narasumber yang telah ditentukan sesuai dengan domain dan *control objective* yang digunakan untuk tata kelola Teknologi Informasi pada. Data yang diperoleh dari kuesioner merupakan data mentah yang berisi jawaban dari setiap responden, lalu hasil dari kuesioner tersebut diolah untuk mendapatkan nilai kapabilitas dari masing-masing proses pengolahan ini dengan menghitung persentase untuk setiap proses jawaban yang diperoleh. Kapabilitas proses pada suatu sistem merupakan ukuran semakin baik sistem tersebut maka semakin baik pula hasil yang dicapai. Dalam suatu sistem, tingkat kemampuan proses perlu ditingkatkan. Karena semakin tinggi tingkat kapabilitas sistem maka semakin baik pula pengelolaan dan prosedur dalam sistem tersebut. Untuk itu diperlukan suatu kerangka kerja yang dapat mengukurnya sebelum dan sesudah pengembangan sistem dilaksanakan. Menurut [7] Penentuan jumlah responden ditentukan berdasarkan rumus Slovin yang ditunjukkan pada Persamaan 1 dan 2 berikut:

Persamaan 1

$$n = \frac{N}{1 + N \cdot e} \quad (1)$$

Dimana:

n = jumlah sampel minimal

N = jumlah populasi

e = margin error

Persamaan 2

$$N = \frac{(0 * y^0) + (1 * y^1) + \dots + (n * y^n)}{Z} \quad (2)$$

Dimana:

N = tingkat pencapaian

Z = jumlah responden.

n = level kapabilitas

Persamaan 3

Menurut [8] Pengolahan dilakukan dengan menghitung persentase untuk setiap proses jawaban yang diperoleh dengan membagi frekuensi dengan jumlah atribut, kemudian dikalikan 100%.

$$P = \frac{f}{n} \times 100\% \quad (3)$$

Dimana:

P = Persentase

f = Frekuensi dari atribut yang terpenuhi

n = Jumlah pertanyaan atau atribut

2.3.2 Metode Pengolahan Data

Data yang diperoleh dari hasil kuesioner merupakan data mentah yang berisi jawaban dari setiap responden. Tujuan pengolahan data adalah untuk menyederhanakan seluruh data dan kemudian disajikan dalam bentuk yang lebih sistematis. Data yang diperoleh bersifat kuantitatif sehingga perlu diolah untuk proses penarikan kesimpulan.

2.3.3 Metode Analisis Penilaian Tingkat Kematangan

Setelah melakukan perhitungan maka selanjutnya melakukan perhitungan Rata-rata Nilai Maturity Level dengan formula sebagai berikut: [9].

$$\text{Rata-rata Nilai Maturity Level} = \frac{\sum \text{Nilai Maturity Tiap Responden}}{\sum \text{Responden}} \quad (4)$$

2.3.4 Uji Validitas dan Reliabilitas

Uji validitas dan reliabilitas untuk instrumen penelitian berdasarkan kriteria bahwa satu set pertanyaan-pertanyaan dalam kuesioner dapat diterima jika memiliki koefisien validitas lebih besar

dari atau sama dengan 0,3 dan realitas yang lebih besar dari atau sama dengan 0,7 sebagaimana yang ditunjukkan pada Tabel 1. berikut ini [10].

Tabel 1. Kriteria Uji Reliabilitas dan Validitas

Kriteria	Reliabilitas	Validitas
Baik	0,80	0,50
Diterima	0,70	0,30
Kriteria	Reliabilitas	Validitas
Rendah	0,60	0,20
Jelek	0,50	0,10

2.3.5 Process Assessment (PA)

PA dapat dinilai berdasarkan interval seperti pada tabel 2 sebagai berikut: [11].

Tabel 2 Kategori Persentase

Singkatan	%Dicapai	Keterangan
N (<i>Not Achieved</i>)	0 - 15%,	Tidak dicapai: Ada sedikit bukti atau tidak ada sama sekali pencapaian atribut ditetapkan dalam proses yang dinilai.
P (<i>Partially Achieved</i>)	>15% - 50%	Sebagian dicapai: Ada beberapa bukti dari pendekatan, beberapa pencapaian, dan atribut ditetapkan dalam proses yang dinilai. Beberapa aspek Pencapaian atribut mungkin tidak terduga.
L (<i>Largely Achieved</i>)	>50% - 85%	Sebagian besar tercapai: Ada bukti dari pendekatan sistematis, pencapaian yang signifikan, atribut yang ditetapkan dalam proses yang dinilai.
F (<i>Fully Achieved</i>)	>85% - 100%	Sepenuhnya tercapai: Ada bukti dari pendekatan lengkap dan sistematis, pencapaian penuh, atribut ditetapkan dalam proses yang dinilai.

Jika suatu proses telah mencapai full Achieved, maka dapat dilakukan ringkasan pencapaian tingkat kapabilitas agar mudah untuk memahami posisi tingkat suatu proses.

Tabel 3. Identifikasi Ringkasan Pencapaian Tingkat Kapabilitas [12].

Tujuan Proses	Deskripsi Tujuan dari Proses									
	Tingkat									
	0	1	2	3	4	5				
<i>Rating berdasarkan persentase</i>		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
<i>Rating berdasarkan tingkat</i>										

Sebuah penilaian yang dapat mengatasi seluruh proses COBIT yang berkaitan dengan tujuan bisnis yang spesifik untuk TI dapat menggunakan alat penilaian menyediakan pemetaan terkait dengan tujuan bisnis dan tujuan TI.

2.3.6 Metode Analisis

Metode analisis data pada penelitian ini dilakukan dengan beberapa tahap, yaitu:

1. Pemetaan Tingkat Kematangan

Pengolahan data dilakukan untuk mengetahui Tingkat Kematangan dari setiap Kontrol Proses Pada tahap ini dilakukan pemetaan tingkat kematangan tata kelola Teknologi Informasi menggunakan alat ukur model kematangan yang diadopsi dari standar COBIT.

2.3.7 Model Penilaian Proses (PAM)

PAM merupakan suatu model yang bertujuan untuk menilai kemampuan proses dengan satu atau beberapa model referensi proses. Skala enam tingkat kemampuan proses yang ditetapkan dalam skala ordinal yang dimulai dari tidak lengkap hingga optimalisasi. Tingkatan-tingkatan tersebut dapat dijelaskan sebagai berikut: [11].

Tabel 4. Model Penilaian Proses

Indeks Kematangan	Tingkat Kematangan
4,51 – 5,00	5-dioptimalisasi
3,51 – 4,50	4-diatur
2,51 – 3,50	3-ditetapkan
1,51 – 2,50	2-dapat diulang
0,51 – 1,50	1-inisialisasi
0,00 – 0,50	0-tidak ada

2.4 Rekomendasi Hasil Analisis

Dengan diketahuinya nilai kapabilitas saat ini dan kondisi yang ingin dicapai dari hasil identifikasi tingkat kapabilitas maka akan didapat gap (kesenjangan). Untuk menutup kesenjangan tersebut pada tahapan ini diberikan langkah-langkah yang berisi rekomendasi sasaran kendali untuk menutup kesenjangan yang ada untuk mencapai kondisi yang diharapkan. Pada tahapan ini, dilakukan penarikan kesimpulan atas penelitian yang dilakukan. Setelah mendapatkan kesimpulan selanjutnya akan disusun sebuah laporan penelitian yang dijalankan yang kemudian dapat dijadikan masukan dan saran kepada pihak Perguruan Tinggi terkait keamanan sistem informasi akademik. Dengan diketahuinya tingkat kapabilitas tata kelola keamanan Sistem Informasi dari hasil identifikasi analisis data, dapat diketahui atribut-atribut yang diisyaratkan tetapi belum dilaksanakan, sehingga dapat diberikan rekomendasi berdasarkan praktik terbaik (*best practice*) dalam COBIT 5.

3 HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Perancangan model tata kelola ini diawali dengan pengumpulan data, visi, misi, sasaran institusi serta renstra TI. Selanjutnya dilakukan analisis sesuai dengan tujuan organisasi untuk mengetahui penanggung jawab aktifitas dan ekspektasi dari pengelola siacad dan user yang terdiri dari jajaran manajemen institusi dan dosen, terhadap proses-proses pada setiap domain yang akan dianalisis tingkat kematangannya sesuai panduan COBIT 5, yaitu EDM (Evaluate Direct and Monitor), APO (Align Plan and Organize), BAI (Build Acquire and Implement), DSS0 (Deliver Support and Service).

3.2 Manajemen Tata Kelola Sistem Informasi

Dalam menerapkan tata kelola TI, diperlukan sebuah model standar tata kelola yang representatif dan menyeluruh yang mencakup masalah perencanaan, implementasi, operasional dan pengawasan terhadap seluruh proses TI maka perlu melakukan pemetaan terkait dengan tata kelola TI sebagai berikut:



Gambar 2. Alur Manajemen Tata Kelola SI

3.3 Pemetaan Tujuan Institusi dengan enterprise goals COBIT 5

Langkah awal yang harus dilakukan agar dapat memetakan tujuan TI adalah mengidentifikasi tujuan institusi. COBIT 5 menyediakan dimensi kartu keseimbangan yang mengkategorikan 17 tujuan perusahaan ke dalam empat (4) dimensi yaitu: Keuangan, Pelanggan, Proses Bisnis Internal, Belajar dan Bertumbuh. Hasil dari empat (4) tujuan perusahaan yang sudah diidentifikasi akan dipetakan kedalam tujuan terkait TI dalam COBIT 5.

Tabel 5. Identifikasi Tujuan Institusi

Dimensi Kartu Nilai Keseimbangan	No	Tujuan Institusi	Tujuan Renstra TI
Keuangan	1	Nilai pemangku kepentingan dan investasi bisnis	
	2	Portofolio dari produk dan layanan yang kompetitif	
	3	Mengelola risiko bisnis (menjaga aset)	Peningkatan Sumber Daya SI
	4	Kepatuhan terhadap hukum dan peraturan eksternal	
	5	Transparansi keuangan	
Pelanggan	6	Budaya layanan yang berorientasi pada pelanggan	Peningkatan Sistem Keamanan SI
	7	Kelangsungan dan ketersediaan layanan bisnis	
	8	Respon tangkas terhadap perubahan lingkungan bisnis	
	9	Strategi pengambilan keputusan berdasarkan perubahan informasi	
Proses Bisnis Internal	10	Optimasi biaya penyampaian layanan	
	11	Optimasi fungsionalitas proses bisnis	Peningkatan Layanan SI
	12	Optimasi biaya proses bisnis	
	13	Mengelola program perubahan bisnis	
	14	Produktivitas operasional dan staf	Peningkatan Kompetensi SDM bidang TI.
Belajar dan Bertumbuh	15	Kepatuhan terhadap kebijakan internal	
	16	Karyawan yang mempunyai keahlian dan motivasi	
	17	Budaya inovasi produk dan bisnis	

3.4 Pemetaan Enterprise Goals Terkait Tujuan TI

Tabel 6. Pemetaan Tujuan Institusi dengan Tujuan Terkait TI

			Tujuan Institusi			
			Mengelola risiko bisnis (Menjaga aset)	Budaya layanan yg berorientasi pada pelanggan	Optimasi fungsionalitas proses bisnis	Produktivitas Operasional dan Staf
	No	Tujuan terkait Teknologi Informasi	3	6	11	14
Keuangan	1	Penyelarasan Strategi TI dan Bisnis	S	P	P	
	2	Kepatuhan TI dan Dukungan untuk kpatuhan dengan hukum dan peraturan Eksternal	S			
	3	Komitmen manajemen eksekutif untuk pengambilan keputusan terkait TI	S		S	
	4	Mengelola risiko bisnis terkait TI	P			
	5	Menyadari keuntungan dari investasi memungkinkan TI dan portofolio layanan		S	S	S
	6	Tranparansi biaya TI, keuntungan dan risiko	S			

Pelanggan	7	Penyampaian layanan TI sejalan dengan persyaratan Bisnis	S	P	P	
	8	Penggunaan aplikasi, informasi dan solusi teknologi mencukupi	S	S	P	P
Internal	9	Ketangkasan TI	S	S	P	S
	10	Keamanan informasi, infrastruktur pengolahan dan aplikasi	P			
	11	Optimasi aset TI, sumber daya dan kemampuan			S	S
	12	Memungkinkan dan mendukung proses bisnis dengan menggabungkan aplikasi dan teknologi dalam proses bisnis	S	S	P	S
	13	Menyampaikan program penyampaian keuntungan, tepat waktu, tepat biaya dan memenuhi standar persyaratan dan kualitas	S	S		
	14	Ketersediaan informasi yang bisa diandalkan dan digunakan untuk pengambilan keputusan	S		S	
	15	Kepatuhan TI terhadap kebijakan internal	S			
Belajar dan Bertumbuh	16	Karyawan yang kompeten dan termotivasi bisnis dan TI		S		
	17	Pengetahuan, Keahlian dan inisiatif untuk inovasi bisnis		S	S	

Pemetaan hanya memilih proses yang berkategori primer, hasil dari pemetaan ini mendapatkan 10 proses yang berkategori primer dalam COBIT 5 seperti yang ditunjukkan pada tabel 4.2.

3.5 Identifikasi Responden

Dalam penelitian ini, ada sejumlah responden yang dilibatkan untuk mendapatkan informasi yang diperlukan terkait tata kelola TI, unsur-unsur tersebut dipetakan dalam tabel pemetaan responden berikut ini:

Tabel 7. Pemetaan Responden

Proses pada Cobit 5		Responden
EDM03	Memastikan Optimasi Risiko	<ul style="list-style-type: none"> • Ketua PT • Wakil Ketua PT • Ketua Program Studi • Kepala LP2M • BAUK/BAAK • Dosen dan Staff • Kepala IT
APO12	Mengelola Risiko	<ul style="list-style-type: none"> • Ketua PT • Wakil Ketua PT • Ketua Program Studi • Kepala LP2M • BAUK/BAAK • Dosen dan Staff • Kepala IT
APO13	Mengelola Keamanan	<ul style="list-style-type: none"> • Ketua PT • Wakil Ketua PT • Ketua Program Studi • Kepala LP2M • BAUK/BAAK • Dosen dan Staff • Kepala IT
BAI06	Mengelola Perubahan	<ul style="list-style-type: none"> • Ketua PT • Wakil Ketua PT • Ketua Program Studi • Kepala LP2M • BAUK/BAAK • Dosen dan Staff • Kepala IT

DSS05	Mengelola Layanan Keamanan	<ul style="list-style-type: none"> • Ketua PT • Wakil Ketua PT • Ketua Program Studi • Kepala LP2M • BAUK/BAAK • Dosen dan Staff • Kepala IT
-------	----------------------------	---

3.6 Pemetaan Berdasarkan Jenis Kelamin

Pada penelitian ini terdapat 31 orang responden, 25 orang adalah laki-laki (80,65%) dan 6 orang adalah perempuan (19,35%).

Tabel 8. Latar Belakang Pendidikan Responden

Jenis Kelamin	Jumlah	Prosentase (%)
Laki-Laki	25	80,65
Perempuan	6	19,35
Jumlah	31	100

3.7 Pemetaan Berdasarkan Latar Belakang Pendidikan

Pada latar belakang pendidikan responden terdapat 1 orang berpendidikan doktor (S3) yaitu 3%, 19 orang lainnya berpendidikan magister (S2) yaitu 61%, 8 orang lainnya berpendidikan (S1) 26%, dan 3 orang lainnya berpendidikan Diploma 10%.

Tabel 9. Latar Belakang Pendidikan Responden

No	Pendidikan	Jumlah	Prosentase (%)
1	S3	1	3%
2	S2	19	61%
3	S1	8	26%
4	Diploma	3	10%
	Jumlah	31	100%

3.8 Analisis Data Kuesioner

Data yang diperoleh dari hasil kuesioner responden merupakan data mentah yang belum diolah. Setelah data kuesioner dikumpulkan lalu dilakukan pengolahan untuk mendapatkan tingkat kevalidan angket dari masing-masing proses:

1. EDM03 Memastikan Optimasi Risiko

Tabel 10. Hasil Uji Validasi Angket

No. Soal	rhitung	rtabel 5% (N=31)	Keterangan
1	0,781**	0,355	Valid
2	0,812**		Valid
3	0,771**		Valid
4	0,799**		Valid
5	0,728**		Valid
6	0,640**		Valid
7	0,777**		Valid

Tabel 11. Hasil Uji Reabilitas Angket

Variabel	nilai_alpha	r tabel 5% (N=31)	Keterangan
EDM03	0,910	0,355	Reliabel

2. APO12 Mengelola Risiko

Tabel 12. Hasil Uji Validasi Angket

No. Soal	rhitung	rtabel 5% (N=31)	Keterangan
1	0,758**	0,355	Valid
2	0,798**		Valid
3	0,650**		Valid

4	0,803**		Valid
5	0,852**		Valid
6	0,875**		Valid
7	0,776**		Valid
8	0,893**		Valid
9	0,780**		Valid
10	0,841**		Valid
11	0,679**		Valid
12	0,722**		Valid
13	0,553**		Valid
14	0,687**		Valid
15	0,726**		Valid

Tabel 13. Hasil Uji Reabilitas Angket

Variabel	nilai alpha	r tabel 5% (N=31)	Keterangan
APO12	0,965	0,355	Reliabel

3. APO13 Mengelola Keamanan

Tabel 14. Hasil Uji Validasi Angket

No. Soal	rhitung	rtabel 5% (N=31)	Keterangan
1	0,694**	0,355	Valid
2	0,807**		Valid
3	0,565**		Valid
4	0,657**		Valid
5	0,793**		Valid
6	0,717**		Valid
7	0,675**		Valid
8	0,712**		Valid
9	0,615**		Valid
10	0,736**		Valid
11	0,742**		Valid
12	0,580**		Valid
13	0,786**		Valid
14	0,698**		Valid
15	0,780**		Valid

Tabel 15. Hasil Uji Reabilitas Angket

Variabel	nilai alpha	r tabel 5% (N=31)	Keterangan
APO13	0,942	0,355	Reliabel

4. BAI06 Mengelola Perubahan

Tabel 16. Hasil Uji Validasi Angket

No. Soal	rhitung	rtabel 5% (N=31)	Keterangan
1	0,821**	0,355	Valid
2	0,867**		Valid
3	0,854**		Valid
4	0,922**		Valid
5	0,921**		Valid
6	0,821**		Valid

Tabel 17. Hasil Uji Reabilitas Angket

Variabel	nilai alpha	r tabel 5% (N=31)	Keterangan
BAI06	0,944	0,355	Reliabel

5. DSS05 Mengelola Layanan Keamanan

Tabel 18. Hasil Uji Validasi Angket

No. Soal	rhitung	rtabel 5% (N=31)	Keterangan
1	0,464**	0,355	Valid
2	0,592**		Valid
3	0,582**		Valid
4	0,429*		Valid
5	0,630**		Valid
6	0,679**		Valid
7	0,643**		Valid
8	0,681**		Valid

9	0,760**		Valid
10	0,612**		Valid
11	0,730**		Valid
12	0,766**		Valid
13	0,643**		Valid
14	0,603**		Valid
15	0,719**		Valid
16	0,720**		Valid
17	0,607**		Valid
18	0,780**		Valid
19	0,496**		Valid
20	0,371*		Valid

No. Soal	rhitung	rtabel 5% (N=31)	Keterangan
21	0,477**	0,355	Valid
22	0,674**		Valid
23	0,782**		Valid
24	0,509**		Valid
25	0,603**		Valid
26	0,676**		Valid
27	0,637**		Valid
28	0,668**		Valid
29	0,603**		Valid
30	0,676**		Valid
31	0,658**		Valid
32	0,736**		Valid

Tabel 19. Hasil Uji Reabilitas Angket

Variabel	nilai alpha	r tabel 5% (N=31)	Keterangan
DSS05	0,968	0,355	Reliabel

Penjelasan Tabel: Uji Validasi: Tujuan untuk mengetahui tingkat kevalidan angket. Dasar pengambilan keputusan: $r_{hitung} > r_{tabel}$ = valid dan $r_{hitung} < r_{tabel}$ = tidak valid dimana $r_{tabel} = N$ (jumlah data) = 31 = Nilai Signifikan (5%) 0,355.

Uji Reabilitas: Tujuan untuk mengetahui konsistensi angket. Dasar pengambilan keputusan : $nilai\ alpha > r_{tabel}$ = konsisten dan $nilai\ alpha < r_{tabel}$ = tidak konsisten dimana $r_{tabel} = N$ (jumlah data) = 31 = Nilai Signifikan (5%) 0,355.

3.9 Capaian Proses Pada Setiap Domain

Untuk mengetahui seberapa besar tingkat kesenjangan (gap) mengenai tata kelola keamanan Sistem Informasi Akademik di Perguruan Tinggi maka diharapkan setiap proses TI dapat ditingkatkan tidak hanya sekedar diimplementasikan saja, namun proses–proses TI yang sudah diimplementasikan dapat ditingkatkan lagi sehingga dapat memberikan manfaat keamanan terhadap pengelolaan layanan Sistem Informasi yang ada di Perguruan Tinggi untuk tujuan jangka panjang dari institusi tersebut, berdasarkan hasil dari penyebaran kuesioner didapat nilai rata–rata untuk setiap proses.

Tabel 20. Daftar Capaian Proses COBIT 5

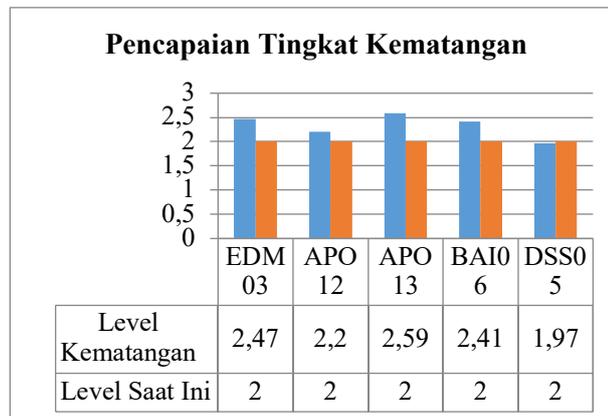
Nama Proses	Kondisi saat ini	Target	Gap
EDM03- Memastikan Optimasi Risiko	2	3	1
APO12 - Mengelola Risiko	2	3	1
APO13 - Mengelola Keamanan	2	3	1
BAI06 - Mengelola Perubahan	2	3	1
DSS05 - Mengelola Layanan Keamanan	2	3	1

3.10 Pengolahan Data

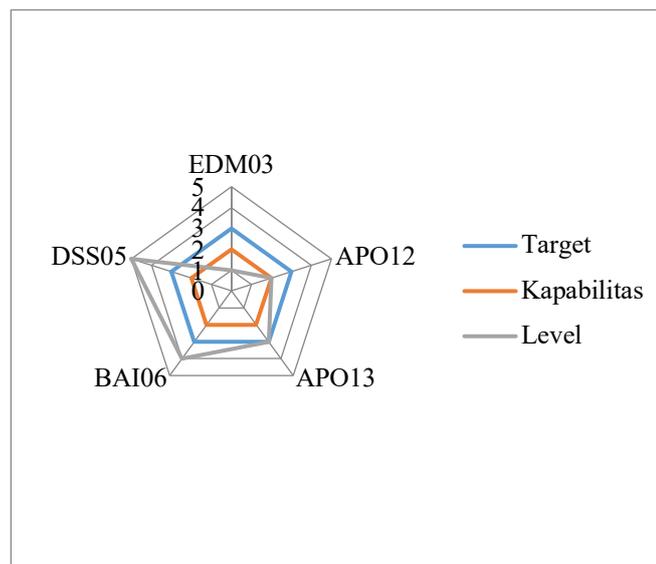
Hasil nilai perhitungan kuesioner *maturity* model yang didapatkan dari beberapa responden tersebut akan dilakukan pembulatan sehingga diperoleh tingkat kedewasaan tertentu untuk setiap proses TI yang dianalisis.

Tabel 21. Hasil Perhitungan Tingkat Kematangan

Total Responden 1-31	Nilai <i>Maturity Level</i>
EDM.03 Memastikan Optimasi Risiko	2,47
APO.12 Mengelola Risiko	2,20
APO.13 Mengelola Keamanan	2,59
BAI.06 Mengelola Perubahan	2,41
DSS.05 Mengelola Layanan Keamanan	1,97
Nilai rata-rata <i>Maturity Level</i>	2,32



Gambar 3. Hasil Tingkat Kematangan



Gambar 4. Diagram Tingkat Kapabilitas

3.11 Ringkasan Hasil Pengukuran Tingkat Kapabilitas

Dari hasil penilaian tingkat kapabilitas pada semua manajemen domain pada setiap *level*, belum ada yang mencapai tingkat kapabilitas *level 2*, karena untuk dapat melanjutkan ke *level* berikutnya harus mencapai kategori F (*Full Achieved*) dengan rentang nilai > 85-100%.

Tabel 22. Ringkasan Nilai Tingkat Kapabilitas Setiap Domain

<i>Governance/ Management Domain</i>	<i>Outputs</i>	<i>Score</i>
EDM03	Mengelola Optimasi Risiko	33,3%
APO12	Mengelola Risiko	25,5%
APO13	Mengelola Keamanan	33%
BAI06	Mengelola Perubahan	50%
DSS05	Mengelola Layanan Keamanan	36%
Rata-rata nilai tingkat kapabilitas		36%

3.12 Rekomendasi Perancangan Tata Kelola Keamanan TI

Dengan memperhatikan hasil yang telah diperoleh dalam penelitian ini yaitu kondisi tingkat kapabilitas TI dan hasil analisis kesenjangan yang ada di Perguruan Tinggi, maka dapat direkomendasikan sebuah perancangan keamanan tata kelola TI.

4 KESIMPULAN

Berdasarkan hasil pengukuran tingkat kematangan dan tingkat kapabilitas pengelolaan keamanan sistem informasi, maka dapat ditarik kesimpulan sebagai berikut:

1. Perlu menerapkan tata kelola TI, sebagaimana yang disyaratkan oleh COBIT sehingga dapat mengukur kelemahan pada penerapan TI agar dapat mencegah sedini mungkin dari ancaman keamanan.
2. Perlu menerapkan standar penilaian keamanan Sistem Informasi akademik agar meminimalisir ancaman keamanan.
3. Perlu peningkatan SDM dibidang TI agar keamanan lebih terkontrol.
4. Manajemen pengelolaan Sistem Informasi akademik belum terlalu memperhatikan tata kelola TI, hal ini terbukti dari lima proses domain yang diukur semuanya masih berada pada kapabilitas tingkat 1.
5. Memerlukan pedoman pengelolaan tata kelola TI yang melingkupi EDM03 (Memastikan Optimasi Risiko), APO12 (Mengelola Risiko), APO13 (Mengelola Keamanan), BAI06 (Mengelola Perubahan) dan DSS05 (Mengelola Layanan Keamanan) dalam memantau keamanan Sistem Informasi.
6. Hasil pengukuran tingkat kapabilitas dari setiap proses belum ada yang mencapai kapabilitas tingkat 2.
7. Untuk dapat meningkatkan kapabilitas tata kelola TI sesuai dengan target yang diinginkan, pengelola dapat melakukan perbaikan pada setiap domain proses yang saat ini masih berada pada kapabilitas tingkat 1.
8. Hasil pengukuran menunjukkan bahwa tata kelola manajemen keamanan TI belum sepenuhnya memenuhi standar keamanan yang akan dicapai.

5 KONTRIBUSI PENELITIAN

Penelitian ini memberikan kontribusi yang signifikan dalam meningkatkan keamanan sistem informasi akademik melalui penerapan Framework COBIT 5. Dengan menganalisis masalah keamanan yang ada, menetapkan tujuan yang jelas, dan menggunakan metode penelitian yang tepat, penelitian ini memberikan wawasan yang berharga tentang tingkat keamanan sistem informasi di lingkungan Perguruan Tinggi. Kontribusinya terletak pada identifikasi kelemahan yang spesifik dan penyediaan rekomendasi konkret untuk meningkatkan keamanan, termasuk penguatan kontrol akses, peningkatan pemantauan aktivitas, dan penyusunan rencana pemulihan bencana yang efektif. Dengan demikian, penelitian ini tidak hanya memberikan pemahaman mendalam tentang masalah keamanan sistem informasi, tetapi juga memberikan panduan praktis untuk mengatasi tantangan tersebut dan meningkatkan keamanan secara keseluruhan.

UCAPAN TERIMA KASIH

Terima kasih yang sebesar-besarnya kepada semua pihak yang telah berkontribusi dalam penelitian ini tentang keamanan sistem informasi akademik dengan menggunakan Framework COBIT 5. Saya ingin mengucapkan terima kasih kepada pembimbing dan tim penelitian atas bimbingan, dukungan, dan wawasan yang berharga mereka selama proses penelitian ini. Tidak lupa juga kepada pihak institusi pendidikan yang telah memberikan akses dan dukungan dalam pengumpulan data. Ucapan terima kasih juga untuk semua responden yang telah berpartisipasi dalam wawancara dan memberikan masukan yang berarti. Tanpa kontribusi dan dukungan dari semua pihak yang terlibat, penelitian ini tidak akan mencapai kesuksesan yang sama. Terima kasih atas segala bantuan, dorongan, dan kerjasama yang telah diberikan. Semoga hasil penelitian ini dapat memberikan manfaat yang berkelanjutan dalam upaya meningkatkan keamanan sistem informasi akademik bagi institusi pendidikan dan masyarakat luas.

DAFTAR PUSTAKA

- [1] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Comput. Secur.*, vol. 92, p. 101747, May 2020, doi: 10.1016/j.cose.2020.101747.
- [2] G. Morris William Tangka, A. Tanny Liem, and J. Yuan Mambu, "Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, Manado, Indonesia: IEEE, Oct. 2020, pp. 1–5. doi: 10.1109/ICORIS50180.2020.9320803.
- [3] B. Widjajanto, D. Agustini Santoso, and N. Riiati, "Alignment Model of Quality Assurance System of Higher Education And Performance Measurement Based on on Framework CobiT 5," in *2018 International Seminar on Application for Technology of Information and Communication*, Semarang: IEEE, Sep. 2018, pp. 207–213. doi: 10.1109/ISEMANTIC.2018.8549728.
- [4] S. Hartono, R. Tjahyadi, and C. Cassandra, "Analysis of Trouble Ticket System Using COBIT 5 Framework (A Case Study Approach)," in *2019 International Conference on Information Management and Technology (ICIMTech)*, Jakarta/Bali, Indonesia: IEEE, Aug. 2019, pp. 420–425. doi: 10.1109/ICIMTech.2019.8843709.
- [5] U. Noor and A. Ghazanfar, "A survey revealing path towards service life cycle management in COBIT 5," in *2016 Eleventh International Conference on Digital Information Management (ICDIM)*, Porto, Portugal: IEEE, Sep. 2016, pp. 68–73. doi: 10.1109/ICDIM.2016.7829754.
- [6] Fitroh, S. P. Nur Amalia, and S. Ratnawati, "Assessment of The Effectiveness of Internal Controls in an Organization Based on COBIT 5 Framework Case Study: State-Owned Enterprises," in *2019 7th International Conference on Cyber and IT Service Management (CITSM)*, Jakarta, Indonesia: IEEE, Nov. 2019, pp. 1–5. doi: 10.1109/CITSM47753.2019.8965409.
- [7] N. F. Saragih, C. Sagala, I. S. Dumayanti, I. K. Jaya, E. Rajagukguk, and A. Gea, "Evaluation of Employee Attendance System Using COBIT 5 Framework," in *2019 International Conference of Computer Science and Information Technology (ICoSNIKOM)*, Medan, Indonesia: IEEE, Nov. 2019, pp. 1–4. doi: 10.1109/ICoSNIKOM48755.2019.9111589.
- [8] B. Bugin, "Metodologi penelitian kualitatif." [Online]. Available: https://scholar.google.com/scholar?cluster=10451811250019784556&hl=en&as_sdt=2005&sciodt=2007
- [9] Y. A. Susanto, W. W. Winarno, and E. Pramono, "Perancangan Tata Kelola Keamanan Jaringan Dengan Framework Cobit Dan Iso 27001:2005".
- [10] H. Nugroho and K. Surendro, "Main and support enablers of vocational higher education governance," in *2014 2nd International Conference on Information and Communication Technology (ICoICT)*, Bandung, Indonesia: IEEE, May 2014, pp. 276–281. doi: 10.1109/ICoICT.2014.6914079.
- [11] P. Kusumah, S. Sutikno, and Y. Rosmansyah, "Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC)," *Proc. - 2014 Int. Conf. ICT Smart Soc. Smart Syst. Platf. Dev. City Soc. GoeSmart 2014 ICISS 2014*, pp. 1–6, 2014, doi: 10.1109/ICTSS.2014.7013193.
- [12] Isaca, P. Copy, and R. R. Sabilillah, "COBIT Self-assessment Guide: Using COBIT 5," 2013.