JIKA (Jurnal Informatika) Universitas Muhammadiyah Tangerang *P ISSN : 2549-0710*
Tangerang, April 2025, Vol 9, No.2 pp 159-168 *E ISSN : 2722-2713*

ANALISIS KEAMANAN SIBER KAMPUS MENGGUNAKAN FRAMEWORK COBIT 2019 PADA DOMAIN (DSS)

Eko Handoyo[1)], M. Cahyo Kriswantoro[2)], Bayu Anugrah [3)]

[1,3] Teknik Komputer Fakultas Sains Teknologi dan Pendidikan, Universitas Muhammadiyah Lamongan,
[2] Informatika Medis Fakultas Sains Teknologi dan Pendidikan, Universitas Muhammadiyah Lamongan,
Jl. Raya Plalangan Plosowahyu Km 02 Lamongan,
Co Responden Email: eko_handoyo@umla.ac.id

Article history
Received 25 Nov 2024
Revised 19 Feb 2025
Accepted 13 Apr 2025
Available online 30 May 2025

Keywords
COBIT,
Cyber,
DSS,
Security,
Maturity.

Abstract

The development of information technology is currently advancing rapidly. Information security aims to ensure the confidentiality, integrity and availability of information owned. The many information security threats that have a major impact on institutions require a cybersecurity risk assessment. The campus is one of the implementations of cyber in the scope of education with a lot of data and information that needs to be ensured. The COBIT 2019 Framework is a framework for directing organizations to cybersecurity activities and security assessments. The focus of this cybersecurity is on the domain (DSS). The maturity level has a good level of assessment, and is expected to provide recommendations related to findings in the audit process. This study aims to help provide an analysis of the right security assessment used in improving campus cybersecurity. The object of this research is on cyber services on campus, starting with collecting data related to campus cyber services to providing recommendations. The results of this study, the DSS domain achievement value of 3.50 indicates a maturity level at defined. This level means that the institution has implemented the defined process and all teams understand how the process should run.

Riwayat
Diterima 25 Nov 2024
Revisi 19 Feb 2025
Disetujui 13 Apr 2025
Terbit online 30 Mei 2025

Kata Kunci
COBIT,
DSS,
Keamanan,
Maturity,
Siber.

Abstrak

Perkembangan teknonogi informasi saat ini maju dengan pesat Keamanan informasi bertujuan agar informasi yang dimiliki terjamin kerahasiaannya (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*). Banyaknya ancaman keamanan informasi yang berdampak besar pada institusi perlu dilakukanan penilaian resiko keamanan siber. Kampus yang menjadi salah satu penimplementasian siber dalam ruang lingkup pendidikan dengan banyaknya data dan informasi yang perlu dipasikan keamananya. *Fremwork* COBIT 2019 merupakan kerangka kerja untuk mengarahkan organisasi pada aktivitas keamanan siber dan asesemen keamanan. Fokus keamanan siber ini terdapat pada domain *(DSS). Maturity level* memilki tingkat penilaian yang baik, dan diharpkan bisa memberikan rekomendasi terkait temuan pada proses audit. Penelitian ini bertujuan membantu memberikan analisis penilaian keamannan yang tepat digunakan dalam perbaikan *cybersecurity* kampus. Objek penelitian ini berada pada layanan siber di kampus, dimulai dengan penggumpulan data terkait dengan layanan siber kampus sampai dengan pemberian rekomendasi. Hasil dari penelitian ini domain DSS nilai ketercapaian 3,50 menunjukkan *maturity level* pada *defined*. Level ini berarti dinyatakan institusi telah menjalankan proses yang sudah didefinisikan dan semua tim paham bagaimana proses seharusnya berjalan.

PENDAHULUAN

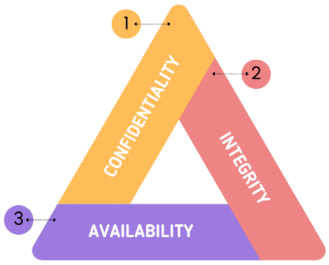
Pesatnya perkembangan digitalisasi dalam dunia global makin masif dan memberikan dapak seknifikan dalam berbagai bidang kehidupan(Handoyo et al., 2024). Bidang pendidikan juga ikut menjadi bagian penting dalam proses digitalisasi ini, tidak hanya melelui pemikiran dan penelitian saja anak tetapi juga proses implentasinya juga (Sopandi et al., 2024). Sektor pendidikan yang paling

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

banyak berperan dalam digitalisasi ini adalah kampus, dimana kampus menjadi salah satu pendidikan tinggi yang di tuntut untuk mampu megimplimentaikan teknolgi digitan dengan cepat, tepat dan efisien(Niqotaini et al., 2024; Riadi, Yanto, et al., 2020).

Istilah Perguruan Tinggi yang digunakan untuk lapisan ke-2, identik dengan istilah Perguruan Tinggi yang disebut dalam Peraturan Pemerintah No.30 th 1990, yaitu organisasi satuan pendidikan, yang menyelenggarakan pendidikan di jenjangpendidikan tinggi, penelitian dan pengabdian kepada Masyarakat (Nursanjaya, 2019). Sistem ini bertujuan untuk mendukung penyelenggaraan pendidikan, sehingga kampus dapat menyediakan layanan informasi yang lebih baik dan efektif kepada civitas akademika, baik didalam/diluar kampus melalui internet (Budhy & Hendra, 2021).

Perguruan tinggi yang mengimplemitasikan perkembangan teknologi dengan sumber daya data yang begitu banyak tentu akan menibulkan acanaman dalam sistem keamanannya (Wattimury & Faza, 2023). Adanya ancaman keamanan ini menuntut sistem keaman yang handal untuk memberika terjamin kerahasiaannya (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*) (Handoyo & Aprillya, n.d. 2024). Seperti pada gambar 1.



Gambar 1. Triangle keamanan

COBIT 2019 menawarkan standar yang dapat digunakan dalam untuk mengevaluasi keanadalan sistem(Saputra & Redo, 2021). COBIT 2019 dapat merumuskan strategi TI, merumuskan proses TI beserta aktivitas-aktivitasnya, serta mengukur tingkat kapabilitas tata kelola TI agar menjadi lebih efektif dan optimal (Ilmiah & Grafis, 2023). Pembaruan pada COBIT 2019 didasari oleh COBIT 5, sumber otoritatif lain serta ke depannya akan didukung oleh komunitas pengguna. Rangkaian produk COBIT 2019 terbuka dan dirancang untuk kostumisasi. COBIT 2019 menyediakan beberapa publikasi di antaranya adalah (Haster & Hartomo, 2022)

1. ***Introduction and Methodology***
   Dokumen ini memperkenalkan konsep kunci COBIT 2019, termasuk prinsip tata kelola, struktur kerangka kerja, dan metodologi untuk mengintegrasikan teknologi informasi (TI) dengan tujuan bisnis. Fokusnya adalah pada penciptaan nilai melalui TI, pengelolaan risiko, dan keselarasan strategis antara IT dan bisnis.
   a. Perbedaan dengan COBIT 5 : Prinsip yang Diperbarui: COBIT 2019 menambahkan dua prinsip baru dalam sistem tata kelola: penerapan sistem yang dinamis dan penyesuaian dengan kebutuhan organisasi. Prinsip kerangka kerja juga diperluas mencakup "keterbukaan, fleksibilitas, dan keselarasan dengan standar lain".
   b. Pendekatan Evolutif: Logo COBIT 2019 menekankan evolusi berkelanjutan, berbeda dengan COBIT 5 yang bersifat statis.

2. ***Governance and Management Objectives***
   Dokumen ini merinci 40 tujuan inti tata kelola dan manajemen TI, yang mencakup domain seperti Evaluate, Direct, and Monitor (EDM) dan Align, Plan, and Organize_(APO). Setiap tujuan dikaitkan dengan proses, komponen tata kelola (seperti struktur organisasi, kebijakan, dan SDM), serta referensi ke standar lain (misalnya ITIL, ISO 27001).
   a. Perbedaan dengan COBIT 5: Penambahan Tujuan: COBIT 2019 menambahkan 3 tujuan baru, seperti APO14 (Managed Data) dan BAI11 (Managed Projects), yang sebelumnya digabung dalam COBIT 5.
   b. Perubahan Terminologi: Enabler pada COBIT 5 diubah menjadi komponen tata kelola (misalnya budaya organisasi dan infrastruktur), memperluas cakupan implementasi.

3. ***Designing an Information and Technology Governance Solution***
   Panduan ini membantu organisasi merancang solusi tata kelola TI yang disesuaikan dengan kebutuhan unik

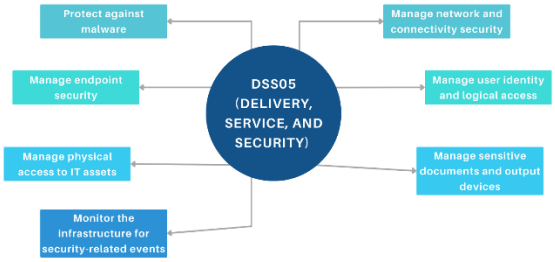
Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

mereka. Fokusnya pada faktor desain, seperti konteks organisasi (ukuran, industri), strategi (peran TI dalam bisnis),dan taktik (pilihan teknologi seperti cloud atau DevOps). Alur kerja yang disediakan mencakup identifikasi prioritas dan penyesuaian komponen tata kelola.

a. Perbedaan dengan COBIT 5: Faktor Desain: Konsep ini baru diperkenalkan di COBIT 2019 untuk memandu kustomisasi, sementara COBIT 5 lebih bersifat generik.
b. Alat Pendukung: COBIT 2019 menyediakan toolkit Excel untuk memfasilitasi proses desain, yang tidak ada di versi sebelumnya.

4. ***Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution***
Panduan implementasi ini menyediakan peta jalan bertahap untuk menerapkan solusi tata kelola TI, termasuk analisis kesenjangan, priorisasi inisiatif, dan pengukuran kematangan proses. Panduan ini juga menekankan optimasi berkelanjutan melalui siklus *plan-do-check-act.*
   a. Perbedaan dengan COBIT 5: Integrasi dengan *Design Guide*: COBIT 2019 menghubungkan implementasi dengan faktor desain, sedangkan COBIT 5 tidak memiliki pendekatan terstruktur untuk kustomisasi.
   b. Penekanan pada Keberlanjutan: COBIT 2019 menambahkan konsep peningkatan kapabilitas secara iteratif, berbeda dengan pendekatan linier COBIT 5.

Framework COBIT 2019 pada domain DSS05 (*Delivery, Service, and Security*) adalah sebuah proses pada COBIT 5 dengan fokus mengelola layanan keamanan pada organisasi untuk mempertahankan risiko keamanan informasi berada pada batas aman yang telah ditentukan dan membahas secara detail memelihara dan menjalankan prosedur dan tugas operasional tidak hanya konsisten, tapi juga meyakinkan(Riadi, Riyadi Yanto, et al., 2020). DSS05 terdiri dari 7 sub-proses, seperti pada Gambar 2.



Gambar 2. DSS05

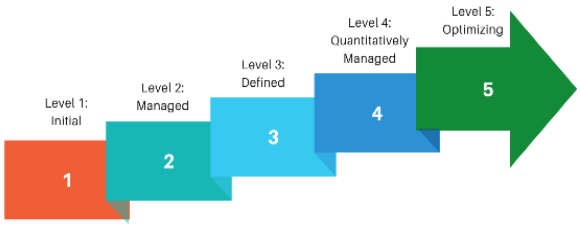
1. ***Protect against malware*** **(DSS05.01)**
Melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama patch keamanan dan pengendalian virus terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (Virus, worm, spyware, spam).
2. ***Manage network and connectivity security*** **(DSS05.02)**
Menggunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas.
3. ***Manage end point security*** **(DSS05.03)**
Memastikan titik akhir (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. ***Manage user identity and logical access*** **(DSS05.04)**
Memastikan 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. ***Manage physical access to IT assets*** **(DSS05.05)**
Menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut akses ke bangunan, bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses ke 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.

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

6. ***Manage sensitive documents and output devices*** **(DSS05.06)**
   Menetapkan pengamanan fisik, praktik akuntansi dan pengelolaan persediaan yang tepat atas sistem TI yang dapat dinegosiasikan, printer tujuan khusus atau token keamanan.

7. ***Monitor the infrastructure for security-related events*** **(DSS05.07)**
   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.

DSS05 melaksanakan beberapa akativitas sebanyak 49 aktivitas. Aktivitas Salah satu alat pengukur dari kinerja suatu system teknologi informasi adalah model kematangan (*maturity level*), jenis kematangan digunakan untuk mengontrol proses-proses teknologi informasi dengan metode penilaian dengan tujuan agar organisasi dapat mengetahui tingkat kematangan teknologi informasi saat ini danorganisasi dapat terus menerus selaras dan berusaha meningkatkan levelnya sampai tingkat tertinggi agar aspek governance terhadap teknologi informasi berjalan dengan lancar(Setyadi & Priyatiningsih, 2021) (Umar et al., 2019), seperti pada gambar 3.



Gambar 3. *Maturity level*

1. ***Initial***
   Secara umum, organisasi yang berapa pada level 1 adalah organisasi yang belum menjalankan CMMI. Tidak terdapatnya proses yang standar dalam pengembangan IT, banyak perubahan yang bersifat ad-hoc (begitu terdapat defect, langsung dilakukan perbaikan tanpa melihat penyebab utama secara menyeluruh) dan sangat sesdikit yang dilakukan oleh sistem.

2. ***Managed Level***
   Ini adalah organisasi telah memiliki beberapa proses yang sering digunakan dalam setiap proyek pengembangan, tetapi tidak terdapat keseragaman secara menyeluruh. Proses sudah mulai berjalan secara konsisten, akan tetapi tidak menyeluruh pada semua lini organisasi.

3. ***Defined Level 3***
   Ini adalah yang paling umum didasarkan oleh hampir seluruh organisasi pada saat telah mengimplementasikan CMMI. Pada level ini, semua lini organisasi menjalankan proses yang sudah didefinisikan pada level organisasi dan semua tim paham bagaimana proses seharusnya berjalan.

4. ***Quantitatively Managed***
   Pada level ini, organisasi semakin advance, mulai menerapkan konsep kuantifikasi pada setiap proses, dan selalu diawasi serta dikontrol.

5. ***Optimizing***
   Ini adalah level puncak dalam model CMMI. Pada level ini suatu organisasi telah mencapai seluruh spesifik dan sudah melewati seluruh level yang ada di Level 2, 3, 4, dan 5. Level ini fokus kepada peningkatan proses secara berkesinambungan melalui inovasi teknologi dan optimasi proses senantiasa dipantau dan dianalisis.

Kontribusi hasil penelitian ini sebagai solusi upaya peninggkatan keamaan siber kampus yang optimal(Isnaini & Suhartono, 2022). Hal ini diharapkan dapat membantu pengambilan kebijakan oleh pemangku kepetingakan (Rektor) dalam pengembanggan teknlogi infomasi yang aman bagi civitas.

METODE PENELITIAN

A. Tahapan Penelitian

Penelitian ini diperlukan data dan informasi yang lengkap guna mendukung tahapan pengujian yang akan dilakukan. Metode pengumpulan data yang digunakan adalah seperti pada gambar 4.

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

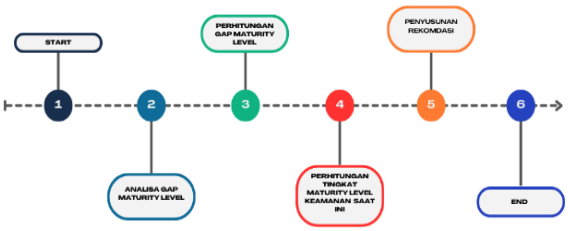
Gambar 4. Tahapan Penelitian

Metode pengumpulan data yang digunakan adalah sebagai berikut(Hadari Nawawi & Barat, n.d.):

1. Studi Kasus Metode Metode ini dilakukan dengan mengumpulkan, membaca serta mempelajari data yang berasal dari berbagai media seperti buku, jurnal, karya tulis atau artikel yang terkait dengan penelitian.
2. Observasi merupakan metode pengumpulan data dengan melakukan pengamatan langsung pada lapangan penelitian. Pada penelitian ini, peneliti melakukan pengamatan langsung pada layanan Sistem Informasi kampus di perguruan tinggi untuk mengumpulkan kebutuhan pengujian.
3. Wawancara: Peneliti melakukan wawancara secara langsung kepada narasumber yang berwenang tehadap layanan akademik di perguruan tinggi.
4. Kuesioner metode ini dilakukan pengumpulan data dengan *Fremework* COBIT 2019.
5. Rekomendasi Merupakan proses pemberian keputusan dari hasil analisis penelitian.

B. *Fremwork* COBIT 2019

Metode yang digunakan dalam penelitian ini adalah metode COBIT 2019 yang telah di kombinasikan dengan *Maturity level* (Lim & Fianty, n.d.)seperti pada gambar 5.



Gambar 5. Proses Framwork COBIT 2019

a) Perhitungan *Maturity Level* adalah melakukan perhitungan data yang telah didapatkan dari kuesioner untuk dilakukan perhitungan sehingga didapatkan *Maturity Level* keamanan sistem informasi akademik saat ini.
b) Perhitungan *Gap Maturity Level* proses ini adalah menghitung kondisi ideal yang diinginkan dan menentukan jarak (gap) antara *Maturity Level* saat ini (existing) dan *Maturity Level* rekomendasi (target).
c) Analisis *Gap Maturity Level* proses ini merupakan penetuan *Maturity Level* pada proses keamanan dengan standar yang sudah disedikan.
d) Penyusunan rekomendasi tata kelola keamanan TI berdasarkan gap analysis. Proses ini merupakan proses penyusunan rekomendasi kepada institusi berdasarkan nilai *gap analysis*.

HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan ini dijelaskan secara lengkap tahapan penelitian yang dilakukan. Seperti pada bagian sebelumnya, penelitian ini memiliki lima tahap. Pada bagian ini akan dibahas hasil yang diperoleh pada setiap tahapan:

A. Pengumpulan data

Proses pengumpulan data dilakukan dengan cara observasi, diskusi non formal, mengulas sistem yang berjalan saat ini melalui wawancara dan mempelajari dokumen-dokumen yang berkaitan dengan penelitian ini. Pengumpulan data berupa wawancara yang dilakukan untuk mendapatkan lebih banyak informasi tentang objek penelitian dan kuesioner dengan membuat daftar pertanyaan berdasarkan standar yang termuat dalam *framework* COBIT 2019 tentang tingkat kematangan keamanan layanan jaringan. Responden yang dipilih sejumlah 45 orang yaitu 3 orang pihak IT, 17 Dosen dan 25 mahasiswa.

Pembahasan akan menjelaskan hasil dari penelitian yang sudah dilakukan berdasarkan objek yang diteliti lalu akan mendapatkan rekomendasi. Rekomendasi yang dapat berikan untuk meningkatkan kualitas tingkat kematangan keamanan layanan jaringan di instansi tersebut. Berikut disajikan pada Tabel 1. Kuesioner Pihak IT sebanyak 38 pertanyaan seperti dalam standar yang ada, dan Tabel 2 Kuesioner Untuk Pengguna (Dosen dan Mahasiswa).

Tabel 1. Kuesioner Pihak IT Kampus

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

No	Pernyataan	1	2	3	4	5
	DSS05.01 Melindungi dari perangkat lunak berbahaya					
1	Menyaring lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (mis, spyware, email phishing).					
2	Melakukan pelatihan berkala tentang malware di email dan penggunaan internet.					
3	Melatih pengguna untuk tidak membuka, tetapi melaporkan, email yang mencurigakan dan untuk tidak menginstal perangkat lunak yang dibagikan atau tidak disetujui.					
4	Mendistribusikan semua perangkat lunak perlindungan secara terpusat (tingkat versi dan patch) menggunakan konfigurasi terpusat dan manajemen perubahan TI.					
5	Meninjau dan evaluasi informasi secara berkala tentang potensi ancaman baru (misalnya, meninjau saran keamanan produk dan layanan vendor).					

Tabel 2. Kuesioner Kuesioner Untuk Pengguna (Dosen dan Mahasiswa)

No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
	DSS05.01 Melindungi dari perangkat lunak berbahaya					
1.	Selalu memperhatikan arus informasi masuk seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta.					
2.	Memberikan pelatihan berkala tentang perangkat lunak di email dan penggunaan internet.					
3.	Pelatihan tidak membuka, tetapi melaporkan, email yang mencurigakan dan untuk tidak menginstal perangkat lunak yang dibagikan atau tidak disetujui.					

Tabel yang disajikan Tabel 1 dan Tabel 2 merupakan bagian kecil dari tabel kuesioare yang ada 35 pertanyaan. Pertanyaan tersebut mengacu pada standar Cobit 2019 yang di kombinasi dengan skala *Maturity Level*.

B. Validasi DSS05 Dengan Aspek Keamanan

Validasi ini merupakan analisis DSS05 pada framework COBIT 2019 dengan parameter keamanan yaitu Kerahasiaan *(Confidentiality)*, Intergritas *(Integrity)*, dan Ketersediaan *(Availability)*. DSS05.01 yaitu melindungi dari perangkat lunak berbahaya menyatakan bahwa validasi keamanan bersifat kerahasiaan, DSS05.02 mengolah keamanan jaringan dan konektivitas menyatakan bahwa validasi keamanan bersifat kerahasiaan, DSS05.03 kelola keamanan titik akhir menyatakan bahwa validasi keamanan bersifat kerahasiaan dan intergritas, DSS05.04 kelola identitas pengguna dan akses logis menyatakan bahwa validasi keamanan bersifat kerahasiaan dan ketersediaan, DSS05.05 mengelola akses fisik ke asset dan IT menyatakan bahwa validasi keamanan bersifat intergritas dan ketersediaan, DSS05.06 kelola dokumen sensitive dan perangkat keluaran menyatakan bahwa validasi keamanan bersifat intergritas, DSS05.07 kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan sepeti pada Tabel 3.

Tabel 3. Aspek Keamanan

No	Kode DSS	C	I	A

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

1	DSS05.01	✓		
2	DSS05.02	✓		
3	DSS05.03	✓	✓	
4	DSS05.04	✓		✓
5	DSS05.05		✓	✓
6	DSS05.06		✓	✓
7	DSS05.07		✓	

C. Pengolahan Data *Maturity Level*

Pengolahan data berupa data yang telah diperoleh kemudian dikumpulkan, bersifat kuantitatif dengan assessment secara langsung kepada pihak yang terkait menggunakan checklist dengan skala likert. Setelah didapatkan total hasil setiap sub domain DSS05 lalu akan dihitung menggunakan indeks kematangan yang akan mengetahui *maturity level* saat ini dan menganalisis *maturity level gap* dengan menghitung *maturity level* saat ini dengan target yang diinginkan.

Salah satu alat pengukur dari kinerja suatu system teknologi informasi adalah model kematangan *(maturity level)*, jenis kematangan digunakan untuk mengontrol proses-proses teknologi informasi dengan metode penilaian dengan tujuan agar organisasi dapat mengetahui tingkat kematangan teknologi informasi saat ini danorganisasi dapat terus menerus selaras dan berusaha meningkatkan levelnya sampai tingkat tertinggi agar aspek governance terhadap teknologi informasi berjalan dengan lancar (Syaputra, 2020), seperti pada gambar 6.

Gambar 6. Skala *Maturity Level*

Berdasarkan gambar 6 maka:

1. Level 0: Non-existent: Tidak terdapat proses terkait sama sekali.
2. Level 1: Initial/Ad hoc: Tahap dimana manajemen sadar akan pentingnya diperhatikan proses terkait, tetapi implementasi yang terjadi masih bersifat reaktif, sesuai dengan kebutuhan mendadak yang ada dan tidak terorganisir.
3. Level 2: Repeatable but intuitive: Tahap dimana manajemen telah memiliki pola untuk mengelola proses terkait berdasarkan pengalaman yang berulang yang pernah dilakukan sebelum-sebelumnya. Namun, pola tersebut belum terstandarisasi.
4. Level 3: Defined process: Tahap dimana manajemen telah berhasil menciptakan dan mengkomunikasikan standar buku pengelolaan proses terkait walaupun belum dilakukan secara terintegrasi.
5. Level 4: Managed and measurable: Tahap dimana kegiatan dan standar yang ada telah diterapkan secara formal dan terintegrasi. Serta terdapat pula indikator sebagai pengukur kemajuan kinerja secara kuantitatif bagi pihak manajemen.
6. Level 5: Optimised: Tahap dimana manajemen telah berkomitmen terhadap proses yang ada agar dapat menjadi sebuah best practice yang selalu dikembangkan.

D. Pembahasan

Kuesioner yang telah disebarkan dimana sesuai dengan standar *framework* COBIT 2019 dan diberikan penilaian dengan *skala likert* dimana dalam kuesioner ini terdapat 5 penilaian seperti pada Tabel 4.

Tabel 4. Penilaian Kuesioner

Nilai	Keterangan
1	Sangat tidak setuju
2	Tidak setuju
3	Ragu-ragu
4	Setuju
5	Sangat setuju

Penilaian kuesioner pada Tabel 4, di kombinasikan dengan standar COBIT 2019, standar yang digunakan adalah *sub-domain* DSS05 dimana *sub domain* ini kusus untuk melakukan penilaian terkait kematangan kemanan layanan jaringan. Dalam standar ini terdapat 35 pernyataan yang berhubungan dengan standar keamanan COBIT 2019 Domain DSS05 dengan jumlah 45 responden (meliputi pihak IT 3 responden, Dosen 17 responden dan Mahasiswa 25 responden). Berikut paparan hasil kuesioner yang didapatkan disajikan dalam bentuk Tabel 5.

Tabel 5. Hasil Penilaian Kuesioner

Responden	DSS05.01	Jumlah

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

	1	2	3	4	5	
1	5	4	5	3	5	22
2	3	5	3	5	4	20
3	4	5	4	5	3	21
4	3	5	3	5	4	20
6	4	3	4	4	5	20

Data sebayak 3 responden IT, Dosen 17 responden dan Mahasiswa 25 responden hanya di sajikan dalam lampiran di tabel 4 hanya bagian dari data yang ada.

Analisis dan interpretasi data wawancara dan kuesioner terhadap tingkat kematangan keamanan layanan jaringan dapat digunakan sebagai temuan penelitian, berdasarkan perhitungan tingkat kematangan atau *maturity level*, dapat dilihat *gap* dan dapat menentukan nilai yang diharapkan yang akan dibuat.

Tabel 6. Nilai kriteria maturity level

Level	Kriteria	Keterangan
1	0,0 – 1,50	*Initial*
2	0,51 – 2,50	*Managed and measurable*
3	2.51 – 3,50	*Defined process*
4	3,51 – 4,50	*Managed and measurable*
5	4,51 – 5.00	*Optimised*

Hasil dari kuesioner yang telah di berikan terhadap responden dan telah di isi oleh responden. Selanjutnya akan dihitung indeks kematangan sebagai berikut:

$$IK = \frac{\sum nj}{\sum nk} \quad (1)$$

Keterangan:
IK = Indeks Kematangan
$\sum nj$ = Jumlah nilai jawaban
$\sum nj$ = Total nilai Kuesioner

Tabel 7. Hasil Indeks / Maturity Level

DSS05	Jumlah Jawaban	Jumlah Pertanyaan	*Indeks / Maturity Level saat ini*
01	826	5	3,67
02	810	5	3,6
03	820	5	3,64
04	799	5	3,55
05	762	5	3,38
06	725	5	3,22
07	782	5	3,47

Dari perhitungan indeks kematangan terhadap data kuesioner didapatkan hasil seperti tabel 7.

Dari data tabel 7 akan dibandingkan antara maturity level saat ini dengan *maturity* target kemudian akan didapatkan *maturity GAP* seperti pada gambar 7.

Gambar 7. Skala Maturity Level

GAP maturity level kemudian dapat dilakukan analisis sehingga ditetapkan *Maturity Level* setiap *sub domain* seperti pada table 8.

Tabel 8. *Maturity Level sub domain DSS05*

Level	*Sub Domain DSS05*	*Maturity Level*
4	*DSS05.01*	*Manage and Measurable*
3	*DSS05.02*	*Defined Process*
4	*DSS05.03*	*Manage and Measurable*
4	*DSS05.04*	*Manage and Measurable*
3	*DSS05.05*	*Defined Process*
3	*DSS05.06*	*Defined Process*
3	*DSS05.07*	*Defined Process*

Selanjutnya tingkat keamanan dapat ditetapkan dengan tingkatan maturity level keseluruhan aktifitas yang dilakukan dalam DSS05 sebagai berikut :

$$Maturity\ level\ DSS05 = \frac{maturity\ level}{banyak\ proses}$$

$$= \frac{(DSS05.01)+(DSS05.02)+(DSS05.03)+(DSS05.04)+DSS05.05)+DSS05.06)+(DSS05.07)}{Banyak\ Proses}$$

$$= \frac{(3{,}69)+(3{,}6)+(3{,}64)+(3{,}55)+(3{,}38)+(3{,}22)+(3{,}47)}{7}$$

$$= 3{,}50$$

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

KESIMPULAN

Penelitian ini menujukan kualitas keamanan layanan jaringan yang ada di kampus telah memenuhi standar keamanan yang diukur mengenai analisis DSS05 pada *framework* COBIT 2019 dengan parameter keamanan yaitu Kerahasiaan, intergritas dan ketersediaan. Tingkat kematangan keamanan layanan jaringan menggunakan *framework* COBIT 2019 dengan *maturity level* di kampus dengan nilai ketercapaian 3,50 menunjukkan *maturity level* pada *defined.* Level ini berarti dinyatakan institusi telah menjalankan proses yang sudah didefinisikan dan semua tim paham bagaimana proses seharusnya berjalan. Menggunakan standar organisasi dan menyesuaikan untuk mengatasi karakteristik proyek dan pekerjaan. Berfokus pada pencapaian tujuan proyek dan kinerja.

UCAPAN TERIMA KASIH

Kami ucapkan terimakasih atas pendanan yang diberikan oleh Kementerian Riset dan Teknologi – BRIN dalam Program Penelitian Kompetitif Nasional Penelitian Dosen Pemula. Kontrak Induk pada tanggal 11 Juni 2024, Nomor Kontrak Induk: 109/E5/PG.02.00.PL/2024.

REFERENSI

Budhy, E., & Hendra. (2021). Peningkatan Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta Melalui Klasifikasi Serangan Cyber Dalam Menunjang WFH. *Seminar Nasional Sains Dan Teknologi*, *November*, 1–6. jurnal.umj.ac.id/index.php/semnastek%0Ap

Hadari Nawawi, J. H., & Barat, K. (n.d.). *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*.

Handoyo, E., & Aprillya, M. R. (n.d.). *Handoyo, Penilaian resiko keamanan siber kampus menggunakan NIST cybersecurity framework 1.1 dengan Peringkat PEGI 1 Penilaian Resiko Keamanan Siber Kampus Menggunakan NIST Cybersecurity Framework 1.1 Dengan Peringkat PEGI*.

Handoyo, E., & Izza Eka Nigrum. (2024). Penilaian risiko keamanan siber kampus menggunakan framework cybersecurity NIST 1.1. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(3), 677–685. https://doi.org/10.37859/coscitech.v4i3.5628

Haster, A. P., & Hartomo, K. D. (2022). Analisis Tingkat Kematangan Smart City Kabupaten Lombok Utara Menggunakan COBIT 2019. *Jurnal Media Informatika Budidarma*, *6*(3), 1459. https://doi.org/10.30865/mib.v6i3.4344

Ilmiah, J., & Grafis, K. (2023). *Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 Pada Val*. *16*(1), 196–208. https://doi.org/10.51903/pixel.v16i1.1247

Isnaini, K. N., & Suhartono, D. (2022). Evaluation of Basic Principles of Information Security at University Using COBIT 5. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *21*(2), 317–326. https://doi.org/10.30812/matrik.v21i2.1311

Lim, M. V., & Fianty, M. I. (n.d.). Enhancing Information Technology Governance: A Comprehensive Evaluation Of The 2019 COBIT Framework In The Retail Industry. In *International Journal of Science*. http://ijstm.inarah.co.id

Niqotaini, Z., Zaidiah, A., & Isnainiyah, I. N. (2024). Evaluasi Penerimaan Situs Web Fakultas Ilmu Komputer Menggunakan Tam Dan Eucs. *JIKA (Jurnal Informatika)*, *8*(3), 350. https://doi.org/10.31000/jika.v8i3.11935

Nursanjaya. (2019). *Eksistensi pendidikan tinggi di indonesia: idealisme atau bisnis?* (Vol. 2, Issue 1).

Riadi, I., Riyadi Yanto, I. T., & Handoyo, E. (2020). Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI). *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 263–270.

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

https://doi.org/10.22219/kinetik.v5i4.1083

Riadi, I., Yanto, I. T. R., & Handoyo, E. (2020). Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI. *IOP Conference Series: Materials Science and Engineering*, *821*(1). https://doi.org/10.1088/1757-899X/821/1/012003

Saputra, M. A., & Redo, R. (2021). Penerapan Framework Cobit 2019 Untuk Perancangan Tata Kelola Teknologi Informasi Pada Perguruan Tinggi. In *Journal of Science and Social Research* (Issue 3). http://jurnal.goretanpena.com/index.php/JSSR

Setyadi, R., & Priyatiningsih, E. (2021). *Maturity Level of ITSM Analysis Using ITIL V3 Framework in State Electricity Enterprise Purwokerto* (Vol. 9, Issue 1).

Sopandi, A., Hannan, A. R., & Khotimah, H. (2024). Perancangan Aplikasi Mobile Menggunakan Framework Flutter Pada Sistem Informasi Akademik. *JIKA (Jurnal Informatika)*, *8*(3), 304. https://doi.org/10.31000/jika.v8i3.11402

Umar, R., Riadi, I., & Handoyo, E. (2019). Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI). *Scientific Journal of Informatics*, *6*(2), 193–202.

Wattimury, G., & Faza, A. (2023). COBIT 2019 Implementation for Enhancing IT Governance in Educational Institutions. In *Jurnal Informatika Sunan Kalijaga)* (Vol. 8, Issue 3).

Copyright @ 2025 JIKA (Jurnal of Informatics)
Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License